

Guida di Websense Manager

Websense[®] Web Security Websense Web Filter ©1996–2009, Websense Inc. Tutti i diritti riservati. 10240 Sorrento Valley Rd., San Diego, CA 92121, USA Pubblicato nel 2009 Stampato negli Stati Uniti e in Irlanda.

I prodotti e le metodologie descritti nel presente documento sono tutelati dai brevetti statunitensi numero 5.983.270, 6.606.659, 6.947.985, 7.185.015, 7.194.464 e RE40.187. Altri brevetti in corso di registrazione.

Questo documento non può essere, in tutto o in parte, copiato, fotocopiato, riprodotto, tradotto o trasferito su un supporto elettronico o convertito in un formato elettronicamente leggibile senza previa autorizzazione scritta di Websense, Inc.

Websense ha posto il massimo impegno per assicurare l'accuratezza delle informazioni contenute in questo manuale. Tuttavia Websense Inc. non offre garanzie riguardo alla documentazione fornita né riconosce alcuna garanzia implicita di commerciabilità e idoneità a uno scopo particolare. Websense Inc. non si assume alcuna responsabilità riguardo ad eventuali errori o danni accidentali o consequenziali in relazione alla distribuzione, alle prestazioni o all'uso di questo manuale o degli esempi qui contenuti. Le informazioni riportate in questa documentazione sono soggette a modifica senza obbligo di preavviso.

Marchi di fabbrica

Websense è un marchio registrato di Websense, Inc, negli Stati Uniti e in alcuni mercati internazionali. Websense è il detentore di numerosi altri marchi di fabbrica non registrati negli Stati Uniti e in altri paesi. Tutti gli altri marchi di fabbrica sono di proprietà dei rispettivi detentori.

Microsoft, Windows, Windows NT, Windows Server e Active Directory sono marchi registrati o marchi di fabbrica di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Sun, Sun Java System e tutti i marchi di fabbrica e i logo basati su Sun Java System sono marchi di fabbrica o marchi registrati di Sun Microsystems, Inc. negli Stati Uniti e in altri paesi.

Mozilla e Firefox sono marchi registrati di Mozilla Foundation negli Stati Uniti e/o in altri paesi.

eDirectory e Novell Directory Services sono marchi registrati di Novell, Inc. negli Stati Uniti e in altri paesi.

Adobe, Acrobat e Acrobat Reader sono marchi registrati o marchi di fabbrica di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

Pentium è un marchio registrato di Intel Corporation.

Red Hat è un marchio registrato di Red Hat, Inc. negli Stati Uniti e in altri paesi. Linux è un marchio di fabbrica di Linus Torvalds negli Stati Uniti e in altri paesi.

Il prodotto include software distribuito da Apache Software Foundation (http://www.apache.org).

Copyright (c) 2000. The Apache Software Foundation. Tutti i diritti riservati.

Altri nomi di prodotti menzionati in questo manuale potrebbero essere marchi di fabbrica o marchi registrati nonché proprietà esclusiva delle rispettive aziende.

Sommario

Argomento 1	Guida introduttiva	15
	Panoramica	16
	Utilizzo di Websense Manager	17
	Accesso a Websense Manager	18
	Navigazione in Websense Manager	20
	Revisione, salvataggio e annullamento delle modifiche	21
	Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte	22
	Personalizzazione della pagina Oggi.	24
	Cronologia: ultimi 30 giorni	25
	Tempi e ampiezza di banda risparmiati	27
	Personalizzazione della pagina Cronologia.	27
	Sottoscrizioni	28
	Gestione di un account tramite il portale MyWebsense	29
	Attivazione di Websense Web Protection Services TM	30
	Configurazione delle informazioni relative all'account	31
	Websense Master Database	32
	Aggiornamenti del database in tempo reale	33
	Real-Time Security Updates TM	33
	Configurazione dei download del database	34
	Prova della configurazione della rete	35
	Assistenza tecnica di Websense	36
Argomento 2	Filtri per l'uso di Internet	37
	Filtri di categoria e di protocollo	38
	Categorie speciali	40
	Classi di rischio	41
	Gruppi di protocolli per la sicurezza	44
	Allegati dei programmi di messaggistica immediata	44
	Azioni di filtraggio	44
	Utilizzo del tempo assegnato per limitare l'accesso a Internet	46
	Accesso con password.	47
	Search Filtering	47
	Gestione dei filtri	48
	Creazione di un filtro di categoria	49
	Modifica di un filtro di categoria	50
	Creazione di un filtro di protocollo	52

	Modifica di un filtro di protocollo	. 53
	Filtri di categoria e di protocollo definiti da Websense	. 55
	Modelli dei filtri di categoria e di protocollo	. 55
	Configurazione delle impostazioni di filtraggio di Websense	. 57
Argomento 3	Client	. 61
	Gestione dei client	. 62
	Gestione di computer e reti	. 63
	Gestione di utenti e gruppi	. 64
	Servizi di directory	. 65
	NT Directory / Active Directory di Windows (Mixed Mode)	. 65
	Active Directory di Windows (modalità nativa)	. 65
	eDirectory di Novell e Directory di Java System di Sun	. 67
	Impostazioni directory avanzate	. 67
	Gestione di gruppi LDAP personalizzati	. 68
	Aggiunta o modifica di un gruppo LDAP personalizzato	. 69
	Aggiunta di un client	. 70
	Ricerca nel service di directory	. 71
	Modifiche delle impostazioni per i client	. 72
	Spostamento dei client a ruoli diversi	. 72
Argomento 4	Criteri di filtraggio dell'uso di Internet	. 75
	Criterio Predefinito	. 76
	Gestione dei criteri	. 77
	Creazione di un criterio	. 78
	Modifica di un criterio.	. 79
	Assegnazione dei criteri ai client	. 81
	Ordine di filtraggio	. 82
	Filtraggio di un sito	. 83
Argomento 5	Pagine di blocco	. 87
	Messaggi di blocco dei protocolli	. 88
	Gestione delle pagine di blocco	. 89
	Personalizzazione dei messaggi di blocco	. 90
	Modifica delle dimensioni del frame del messaggio	. 91
	Modifica del logo visualizzato nella pagina di blocco	. 91
	Utilizzo delle variabili del contenuto di una pagina di blocco	. 92
		. 93
		. 94
	Uso di una pagina di blocco alternativa in un altro computer	. 94
Argomento 6	Utilizzo dei report per valutare i criteri di filtraggio	. 97
	Panoramica sulla creazione dei report	. 98
	Che cos'è il tempo di navigazione in Internet?	. 99

	Report di presentazione 100	,
	Conia di un report di presentazione	
	Definizione del filtro per report	
	Selezione dei client de includere in un report	
	Selezione delle categorie da includere in un report	
	Selezione dei protocolli da includere in un report	
	Selezione delle azioni da includere in un report 107	
	Impostazione delle opzioni per i report 108	
	Conferma della definizione dei filtri di report	
	Gestione dei Preferiti	
	Generazione dei report di presentazione	
	Pianificazione dei report di presentazione	
	Impostazione della pianificazione 113	
	Selezione dei report da pianificare	
	Selezione dell'intervallo di date	
	Selezione delle opzioni di output.	
	Visualizzazione dell'elenco dei processi pianificati	
	Visualizzazione di Cronologia processo	
	Report investigativi	
	Report di riepilogo 121	
	Report di riepilogo multi-livello 126	
	Report dettagliati flessibili 127	
	Colonne dei report dettagliati flessibili	
	Report Dettagli attività utente	
	Dettaglio giornaliero attività utente	
	Dettaglio mensile attività utente	
	Mappatura delle categorie	
	Report standard	
	Report investigativi preferiti	
	Salvataggio di un report come Preferito	
	Modifica di un report Preferito	
	Pianificazione dei report investigativi 141	
	Gestione dei processi pianificati per i report investigativi 144	
	Report casi atinici	
	Output su file 145	
	Stampa dai raport investigativi	
	A accesse all'attività utanta	
Argomento 7	Analisi del contenuto con le opzioni di Tempo reale 149	
	Download del database	1
	Opzioni di scansione	
	Categorizzazione del contenuto e scansione per l'identificazione di minacce 152	
	Scansione dei file 153	
	Eliminazione di un contenuto	

	Perfezionamento della scansione	156
	Creazione di report sull'attività di scansione in tempo reale	158
	Metodo di registrazione delle scansioni in tempo reale	159
Argomento 8	Filtro per i client remoti	161
	Modalità di funzionamento di Remote Filtering	162
	Internamente alla rete	163
	Esternamente alla rete	164
	Identificazione degli utenti remoti	165
	Comunicazione con il server non riuscita	166
	Virtual Private Network (VPN).	167
	Configurazione delle impostazioni di Remote Filtering	168
Argomento 9	Perfezionamento dei criteri di filtraggio	171
	Restrizione dell'accesso degli utenti a un elenco definito di siti Internet .	172
	Filtri per restrizioni di accesso e priorità di un filtro	172
	Creazione di un filtro per restrizioni di accesso	174
	Modifica di un filtro per restrizioni di accesso	174
	Aggiunta di siti dalla pagina Modifica criterio	176
	Copia di filtri e criteri nei ruoli	177
	Definizione dei Componenti filtro	178
	Gestione delle categorie	179
	Modifica delle categorie e dei loro attributi	179
	Revisione di tutti gli attributi personalizzati delle categorie	181
	Modifiche globali ai filtri di categoria	181
	Assegnazione di un nuovo nome a una categoria personalizzata	182
	Eiltre hegete su persole chique	182
	Definizione di perele chiave	184
	Ridefinizione di un filtro per specifici siti	186
	Definizione di URL non filtrati	187
	URL ricategorizzati	188
	Gestione dei protocolli	189
	Filtri di protocollo	189
	Modifica dei protocolli personalizzati.	190
	Aggiunta o modifica degli identificatori dei protocolli	191
	Assegnazione di un nuovo nome a un protocollo personalizzato Modifiche globali ai filtri di protocollo	192 192
	Creazione di un protocollo personalizzato	193
	Aggiunta a un protocollo definito da Websense	195
	Uso di Bandwidth Optimizer per la gestione della larghezza di banda	195
	Configurazione delle restrizioni predefinite di Bandwidth Optimizer .	196
	Gestione del traffico in base al tipo di file	197
	Gestione dei tipi di file	199

	Aggiunta di tipi di file predefiniti	. 200
	Aggiunta di estensioni di file a un tipo di file	. 200
	Uso delle espressioni regolari	. 200
	Uso della Casella degli strumenti per verificare il comportamento dei filtri	. 201
	Categoria degli URL	. 202
	Verifica criterio	. 202
	Verifica filtri	. 203
	Accesso URL	. 203
	Verifica utente	. 203
	Identificazione di un utente per verificare criteri o filtri	. 204
Argomento 10	Identificazione utente	. 205
	Identificazione trasparente	. 205
	Identificazione trasparente di utenti remoti.	. 206
	Autenticazione manuale	. 207
	Configurazione dei metodi di identificazione utente trasparente	. 208
	Impostazione delle regole di autenticazione per specifici computer .	.210
	Definizione delle eccezioni delle impostazioni	
	di identificazione utente	.210
	Verifica delle eccezioni delle impostazioni di identificazione utente .	.211
	Autenticazione manuale sicura	. 213
	Generazione di chiavi e di certificati	. 214
	Accettazione del certificato dall'interno del browser	. 215
	del computer client	. 215
	DC Agent	. 217
	Configurazione di DC Agent	. 218
	Logon Agent.	. 221
	Configurazione di Logon Agent	. 221
	RADIUS Agent	. 223
	Gestione del traffico RADIUS	. 224
	Configurazione dell'ambiente RADIUS	. 225
	Configurazione di RADIUS Agent	. 226
	Configurazione del client RADIUS	. 227
	Configurazione del server RADIUS	. 228
	eDirectory Agent	. 229
	Considerazioni speciali sulla configurazione	. 230
	Configurazione di eDirectory Agent	. 231
	Aggiunta di una replica del server eDirectory	. 232
	Configurazione di eDirectory Agent per usare LDAP.	. 233
	Auvazione di query complete nel server eDirectory	. 234
	Configurazione di molteplici agenti	. 233
	Configurazione di diverse impostazioni per un'istanza di agente.	. 237

	Parametri del file INI	238
	Configurazione di un agente affinché ignori determinati nomi utente.	239
Argomento 11	Amministrazione con delega	241
	Introduzione ai ruoli amministrativi	242
	Introduzione alle funzioni di amministratore	243
	Super Administrator	243
	Amministratori con delega	245
	Amministratori in molteplici ruoli	246
	Concetti di base sui ruoli amministrativi	247
	Notifica agli Amministratori	250
	Operazioni degli amministratori con delega	251
	Visualizzazione dell'account utente	251
	Visualizzazione della definizione del proprio ruolo	252
	Aggiunta di client alla pagina Client	252
	Applicazione di criteri ai client	253
	Generazione di report	255
	Attivazione dell'accesso a Websense Manager	255
	Account di directory	255
	Account utenti Websense	257
	Aggiunta di un account utente di Websense	258
	Modifica della password utente di Websense	258
	Uso dell'amministrazione con delega	259
	Aggiunta di ruoli	260
	Modifica dei ruoli	261
	Aggiunta di amministratori	264
	Aggiunta di client gestiti	266
	Gestione dei conflitti di ruolo	268
	Considerazioni speciali	268
	Molteplici amministratori in accesso a Websense Manager	270
	Definizione delle restrizioni di filtraggio per tutti i ruoli	271
	Creazione di un Blocco filtro	272
	Blocco delle categorie	272
		273
Argomento 12	Amministrazione del server Websense	275
	Componenti dei prodotti Websense	276
	Componenti per il filtraggio	277
	Componenti dei report.	280
	Componenti dell'identificazione utenti	281
	Funzionamento di Policy Database	282
	Gestione di Policy Server	282
	Aggiunta e modifica delle istanze di Policy Server	283

	Ambiente con molteplici Policy Server	. 284
	Modifica dell'indirizzo IP del Policy Server.	. 285
	Gestione di Filtering Service	. 287
	Revisione dei dati di Filtering Service	. 287
	Verifica dello stato di download del Master Database	. 288
	Ripresa del download del Master Database	. 288
	Visualizzazione ed esportazione del registro di controllo	. 289
	Chiusura e riavvio dei servizi di Websense	. 290
	Avvisi su schermo	. 292
	Prevenzione di un numero eccessivo di avvisi	. 292
	Configurazione delle opzioni generali degli avvisi	. 293
	Configurazione degli avvisi del sistema	. 295
	Configurazione degli avvisi di utilizzo di una categoria	. 296
	Aggiunta di avvisi di utilizzo di una categoria	. 296
	Configurazione degli avvisi di utilizzo di un protocollo	. 297
	Aggiunta degli avvisi di utilizzo protocollo	. 298
	Revisione dello stato del sistema in uso	299
	Esecuzione di backup e ripristino dei dati Websense.	. 300
	Pianificazione del backup	. 302
	Esecuzione immediata dei backup	. 303
	Manutenzione dei file di backup	304
	Ripristino dei dati Websense	. 305
	Cancellazione della pianificazione dei backup	. 306
	Opzioni di comando	306
Argomento 13	Amministrazione della creazione dei report	. 309
	Pianificazione della configurazione	. 310
	Gestione dell'accesso ai Reporting Tools	. 310
	Configurazione di base	. 311
	Assegnazione delle categorie alle classi di rischio	. 312
	Configurazione delle preferenze per la creazione dei report	. 314
	Configurazione di Filtering Service per la registrazione	. 314
	Utilità Configurazione di Log Server	. 316
	Configurazione delle connessioni di LogServer	. 317
	Configurazione delle opzioni del database Log Server	. 318
	Configurazione della connessione con il database	. 320
	Configurazione dei file cache di registro	321
	Configurazione delle opzioni di consolidamento	. 322
	Configurazione di WebCatcher	. 324
	Autenticazione di WebCatcher	327
	Autenticazione di WebCatcher Chiusura e riavvio di Log Server	327

	Processi del database	329
	Amministrazione del database di registrazione	330
	Impostazioni dell'amministrazione del database di registrazione	330
	Configurazione opzioni di rollover	331
	Configurazione della registrazione di URL completi	333
	Configurazione delle opzioni sui tempi di navigazione in Internet	. 334
	di registrazione	335
	Configurazione della creazione delle partizioni	555
	del database di registrazione	338
	Configurazione delle partizioni disponibili	339
	Visualizzazione dei registri di errore	340
	Configurazione dei report investigativi	341
	Collegamento con il database e impostazioni predefinite dei repor	t342
	Opzioni di visualizzazione e di output	344
	Attività utente	346
Argomento 14	Configurazione della rete	349
	Configurazione dell'hardware	350
	Configurazione di Network Agent	351
	Configurazione delle impostazioni globali	352
	Configurazione delle impostazioni locali	353
	Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC)	355
	Configurazione delle impostazioni di monitoraggio	
	per una scheda di interfaccia di rete (NIC)	356
	Aggiunta o modifica degli indirizzi IP	357
	Verifica della configurazione di Network Agent	358
Argomento 15	Diagnostica e risoluzione problemi	361
	Problemi di installazione e di sottoscrizione	361
	Lo stato Websense mostra un problema di sottoscrizione	361
	Dopo l'aggiornamento, mancano degli utenti in Websense Manager .	. 362
	Problemi con il Master Database	363
	Il database dei filtri iniziale è in uso	363
	Il Master Database risale a più di 1 settimana fa	363
	Il download del Master Database non può venire completato	364
	Chiave di sottoscrizione	364
	Accesso a Internet	365
	Spazio su disco insufficiente	365 366
	Memoria insufficiente	367
	Applicazione delle restrizioni	368
	Il download del Master Database non avviene ai tempi previsti	368
	Come contattare il Supporto tecnico per problemi di download del database	. 368

Problemi di filtro	369
Filtering Service non è in esecuzione	369
User Service non è disponibile	370
Siti erroneamente categorizzati come Tecnologia informatica	371
Le parole chiave non vengono bloccate	371
Gli URL personalizzati o con un filtro per restrizioni	
di accesso, non vengono filtrati come previsto.	372
Un utente non può accedere a un protocollo	
o un'applicazione come previsto	372
Una richiesta FTP non viene bloccata come previsto	372
Il software Websense non applica i criteri previsti per utenti o gruppi.	. 373
Gli utenti remoti non vengono filtrati dal criterio corretto	373
Problemi con Network Agent.	373
Network Agent non è stato installato	373
Network Agent non è in esecuzione	374
Network Agent non sta monitorando le schede NIC.	374
Network Agent non può comunicare con Filtering Service	375
Aggiornamento dell'indirizzo IP o delle informazioni	
sull'identificatore interno (UID) di Filtering Service	375
Problemi di identificazione utenti	376
Diagnostica/risoluzione problemi di DC Agent	377
Gli utenti vengono erroneamente filtrati dal criterio Predefinito	377
Modifica manuale delle autorizzazioni di DC Agent e User Service	:s378
Diagnostica/risoluzione problemi di Logon Agent	379
Oggetti Criteri di gruppo (Group Policy Objects)	379
User Service in esecuzione su Linux	380
NetBIOS	380
Problemi di profilo utente	381
Diagnostica/risoluzione problemi di eDirectory Agent	381
Attivazione della diagnostica di eDirectory Agent	382
eDirectory Agent calcola erroneamente le connessioni	
con il server eDirectory	383
Esecuzione di eDirectory Agent in modalità console	384
Diagnostica/risoluzione problemi di RADIUS Agent.	384
Esecuzione di RADIUS Agent in modalità console	385
Agli utenti remoti non viene richiesta l'autenticazione manuale	386
Gli utenti remoti non vengono filtrati correttamente	386
Problemi dei messaggi di blocco	386
Non è stata visualizzata una pagina di blocco per	
un determinato tipo di file bloccato	387
Gli utenti ricevono un errore di browser anziché	207
una pagina di blocco.	387
Viene visualizzata una pagina bianca vuota anziché una pagina di blocco	. 388

I messaggi di blocco del protocollo non vengono visualizzati come previsto	88
Viene visualizzato un messaggio di blocco del protocollo	
anziche una pagina di blocco	;9
Problemi di registro, di messaggi di stato e di avvisi di errore 38	;9
Dove posso trovare i messaggi di errore dei componenti Websense?38	;9
Avvisi di errore di integrità Websense	0
Vengono generati due record di registro per una singola richiesta. 39	1
Problemi di Policy Server e Policy Database	1
Password dimenticata	1
Non posso collegarmi a Policy Server	2
Impossibile avviare il servizio Websense Policy Database 39	2
Problemi di amministrazione con delega 39	13
I client gestiti non possono venire eliminati da un ruolo 39	13
Un errore di accesso segnala che un altro utente	
è collegato al mio computer	13
Alcuni utenti non possono accedere a un sito	
dell'elenco URL non filtrati	3
I siti ricategorizzati vengono filtrati in base alla categoria errata 39	14 14
Impossibile creare un protocollo personalizzato	<u>,</u> 4
Problemi di creazione report)4
Log Server non è in esecuzione	95
Nessun Log Server è stato installato per un'istanza di Policy Server 39	<i>)</i> 6
Il database di registrazione non è stato creato)7
Il database di registrazione non è disponibile)7
Dimensioni del database di registrazione	98
Log Server non registra i dati nel database di registrazione 39	19 10
Aggiornamento del collegamento con il Log Server	19
Configurazione delle autorizzazioni per l'utente relativamente	0
Log Server non può stabilire la connessione con il servizio di directory/	01
L'ati dei report sui tempi di navigazione in Internet sono alterati)1
I a larghezza di banda è superiore al previsto 40)1
Alcune richieste di protocollo non vengono registrate 40	12
Tutti i report sono vuoti 40	12
Partizioni del database 40	12
Processo di SQL Server Agent)2
Configurazione di Log Server)3
Nelle pagine Oggi e Cronologia non viene visualizzato alcun grafico . 40)4
Impossibile accedere ad alcune funzioni di creazione report 40)4
L'esportazione in Microsoft Excel causa la perdita di alcuni dati del report 40)4
Salvataggio di un'esportazione in HTML dei report di presentazione 40)4
Problemi di ricerca all'interno dei report investigativi)5

Problemi generali dei report investigativi	405
Strumenti di diagnostica e risoluzione problemi	406
Finestra di dialogo Servizi di Windows	406
Visualizzatore eventi di Windows	406
File di registro di Websense	407

Guida introduttiva

Il software Websense consente agli amministratori di rete di tutti i settori, dal commercio all'industria, all'istruzione, al governo ed ad altri ancora, di regolare e di monitorare il traffico Internet di rete. Con il software Websense si può ottenere:

- Massima riduzione dei tempi di fermo dei dipendenti che accedono a siti Internet considerati problematici, inappropriati o non correlati al lavoro svolto.
- Massima riduzione delle risorse di rete e del rischio di azioni legali dovute ad accessi inappropriati.
- Aggiunta di un ulteriore livello di protezione della rete contro potenziali spyware, malfare, hacking e altri tipi di intrusione.

Da qui, si possono ottenere informazioni sugli argomenti seguenti:

Configurazione di base di Websense		Implementazione dei filtri Internet
·	Utilizzo di Websense Manager, pagina 17	• <i>Filtri di categoria e di protocollo</i> , pagina 38
·	Sottoscrizioni, pagina 28	 Aggiunta di un client, pagina 70
·	Websense Master Database, pagina 32	Gestione dei criteri, pagina 77
٠	<i>Verifica della configurazione di Network Agent</i> , pagina 358	Assegnazione dei criteri ai client, pagina 81

Si può anche imparare a:

Valutare la configurazione	Specificare ulteriori criteri di filtraggio
Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte, pagina 22	 Creazione di una categoria personalizzata, pagina 182
Cronologia: ultimi 30 giorni, pagina 25	• <i>Ridefinizione di un filtro per specifici siti</i> , pagina 186
• <i>Report di presentazione</i> , pagina 100	• <i>Restrizione dell'accesso degli utenti a un elenco definito di siti Internet</i> , pagina 172
<i>Report investigativi</i> , pagina 119	• Filtro basato su parole chiave, pagina 184
 Uso della Casella degli strumenti per verificare il comportamento dei filtri, pagina 201 	Gestione del traffico in base al tipo di file, pagina 197
	 Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195

Panoramica

Il software Websense funziona in congiunzione con alcuni dispositivi di integrazione quali i server proxy, firewall, router e caching, ed offre sia il motore sia gli strumenti di configurazione necessari allo sviluppo, al monitoraggio e all'applicazione dei criteri di accesso ad Internet.

Una serie di componenti di Websense (descritti nella sezione *Componenti dei prodotti Websense*, pagina 276) dispone di funzioni di filtraggio degli accessi a Internet, di identificazione utente, avvertenze, generazione di report e funzioni di diagnostica/ risoluzione problemi.

Per una descrizione generale delle nuove funzioni incluse in questa versione del software Websense, consultare le <u>Note di rilascio</u>, disponibili nel <u>Portale di supporto</u> <u>di Websense</u>.

Una volta completata l'installazione, il software Websense applica il criterio **Predefinito** per monitorare l'uso di Internet senza bloccare alcuna richiesta. Questo criterio gestisce l'accesso ad Internet di tutti i client della rete fino a quando non si definiscono i propri criteri e questi non vengono assegnati ai client. Anche dopo aver creato impostazioni di filtraggio personalizzate, il criterio predefinito viene applicato se a un determinato client non sono stati assegnati altri criteri. Per ulteriori informazioni, vedere *Criterio Predefinito*, pagina 76.

Le procedure di creazione dei filtri, di aggiunta di client, definizione di criteri e applicazione ai client dei criteri definiti sono descritte nelle sezioni:

- Filtri per l'uso di Internet, pagina 37
- Client, pagina 61
- Criteri di filtraggio dell'uso di Internet, pagina 75

Websense Manager, uno strumento browser-based, costituisce l'interfaccia grafica centrale da usare per la definizione della configurazione, della gestione dei criteri e delle funzioni di generazione dei report del software Websense. Per ulteriori informazioni, vedere *Utilizzo di Websense Manager*, pagina 17.

È possibile definire diversi livelli di accesso a Websense Manager per consentire a determinati amministratori di gestire soltanto un gruppo specifico di client o di consentire a singoli utenti di generare report sul proprio uso di Internet. Per ulteriori informazioni, vedere *Amministrazione con delega*, pagina 241.

Utilizzo di Websense Manager

Argomenti correlati:

- Accesso a Websense Manager, pagina 18
- Navigazione in Websense Manager, pagina 20
- Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte, pagina 22
- Cronologia: ultimi 30 giorni, pagina 25

Websense Manager è l'interfaccia centrale di configurazione da usare per la personalizzazione dei filtri, il monitoraggio dell'uso di Internet, la creazione dei report sull'uso di Internet e la gestione della configurazione e delle impostazioni del software Websense. Questo strumento Web-based supporta due browser per la sua esecuzione:

- Microsoft Internet Explorer 7
- Mozilla Firefox 2

Sebbene sia possibile lanciare Websense Manager da altri browser, l'uso di uno dei due browser supportati garantisce funzionalità complete e una visualizzazione adeguata delle schermate dell'applicazione.

Per lanciare Websense Manager, eseguire una delle operazioni seguenti:

- Nei computer dotati del sistema operativo Windows:
 - Andare a Start > Programmi > Websensee selezionare quindi Websense Manager.
 - Fare doppio clic sull'icona di Websense Manager.
- Aprire un browser supportato su un computer collegato in rete ed inserire quanto segue:

https://<Indirizzo IP>:9443/mng

Nel campo *<Indirizzo IP* > inserire l'indirizzo IP del computer in cui è installato Websense Manager.

Se non è possibile collegarsi a Websense Manager dalla porta predefinita, consultare il file **tomcat.log** archiviato nel computer in cui è installato Websense Manager (situato per impostazione predefinita nel percorso C:**Programmi\Websense\tomcat\logs**\ oppure nella directory /opt/Websense/tomcat/logs/) per verificare la porta.

S si sta usando la porta corretta e non si riesce a stabilire il collegamento con Websense Manager da una computer remoto, verificare che il firewall in uso permetta la comunicazione con quella porta.

Il collegamento SSL viene utilizzato per garantire una comunicazione browser-based sicura con Websense Manager. Questo collegamento utilizza un certificato di sicurezza rilasciato da Websense, Inc. Poiché i browser supportati non riconoscono Websense, Inc. come un Organismo di certificazione standard, verrà visualizzato un errore di certificazione la prima volta che si lancia Websense Manager da un nuovo browser. Per evitare la visualizzazione di questo messaggio d'errore, si può installare o accettare permanentemente il certificato dall'interno del browser. Per istruzioni, consultare la <u>Knowledge Base di Websense</u>.

Dopo che il certificato di sicurezza è stato accettato, la pagina di accesso a Websense Manager viene visualizzata nella finestra del browser (vedere *Accesso a Websense Manager*).

Accesso a Websense Manager

Argomenti correlati:

- Utilizzo di Websense Manager
- Navigazione in Websense Manager, pagina 20
- Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte, pagina 22
- Cronologia: ultimi 30 giorni, pagina 25

Una volta completata l'installazione, il primo utente che accede a Websense Manager deve disporre di un accesso amministrativo completo. Il nome utente è **WebsenseAdministrator** e non può essere modificato. La password del WebsenseAdministrator viene configurata durante la procedura di installazione.

Per accedere, lanciare prima di tutto Websense Manager (vedere *Utilizzo di Websense Manager*). Dalla pagina di accesso, procedere come segue:

1. Selezionare il **Policy Server** da gestire.

Se il proprio ambiente informatico dispone soltanto di un Policy Server, questo sarà selezionato per predefinizione.

- 2. Selezionare un Tipo account:
 - Per un accesso tramite l'uso di un account utente di Websense, quale un account di WebsenseAdministrator, fare clic su Account Websense (predefinizione).
 - Per un accesso tramite l'uso delle proprie credenziali di rete, fare clic su Account di rete.
- 3. Inserire un Nome utente e una Password, e fare quindi clic su Inizia sessione.

L'accesso a Websense Manager è stato completato.

- Al primo accesso a Websense Manager, verrà offerta la possibilità di lanciare le Esercitazioni di riferimento rapido. Si consiglia agli utenti che usano per la prima volta il software Websense o agli utenti che usano per la prima volta questa nuova versione del software Websense, di completare le Esercitazioni di riferimento rapido.
- Se si sta utilizzando Amministrazione con delega e si sono creati ruoli amministrativi, potrebbe venire visualizzato un messaggio che richiede di

selezionare un ruolo da gestire. Per ulteriori informazioni, vedere *Amministrazione con delega*, pagina 241.

Ogni sessione di Websense Manager viene automaticamente chiusa 30 minuti dopo aver eseguito l'ultima azione tramite l'interfaccia utente (clic da un pagina all'altra, inserimento dati, inserimento di modifiche nella cache, salvataggio di modifiche). Cinque minuti prima del termine automatico della sessione, viene visualizzato un messaggio di avvertenza.

- Se esistono modifiche non inserite nella cache o modifiche nella cache in attesa di salvataggio, tali modifiche verranno perse alla chiusura di una sessione.
 Ricordarsi di fare clic su OK per l'inserimento nella cache e fare clic su Salva tutto per salvare e implementare le modifiche apportate.
- Se Websense Manager è aperto in molteplici schede della stessa finestra del browser, tutte queste istanze condivideranno la medesima sessione. Un timeout applicato alla sessione di una scheda, verrà automaticamente applicato anche a tutte le altre schede.
- Se Websense Manager è aperto in molteplici finestre del browser di un computer, tutte queste istanze condivideranno la medesima sessione se:
 - si sta usando Microsoft Internet Explorer e si usa Ctrl-N per aprire una nuova istanza di Websense Manager.
 - si sta usando Mozilla Firefox.

Un timeout applicato ad una finestra aperta, verrà automaticamente applicato anche a tutte le altre finestre.

• Se si lanciano molteplici finestre di Internet Explorer, una indipendente dall'altra, e queste vengono usate per un accesso a Websense Manager da parte di vari amministratori, queste finestre **non** condivideranno la stessa sessione. Un timeout applicato a una finestra, non verrà applicato alle altre.

Se si chiude il browser senza scollegarsi da Websense Manager, o se il computer remoto dal quale si è acceduto a Websense Manager si chiude inaspettatamente, il proprio diritto di accesso potrebbe venire temporaneamente bloccato. Entro 2 minuti, il software Websense rileverà questo problema e chiuderà la sessione interrotta consentendo all'utente di accedere nuovamente al software.

Navigazione in Websense Manager

L'interfaccia di Websense Manager è suddivisa in 4 aree distinte:

- 1. Intestazione di Websense
- 2. Riquadro di navigazione di sinistra
- 3. Riquadro dei collegamenti di destra
- 4. Riquadro del contenuto

WebSecurity	1 Policy Server	192.168.247.53 💌 Ruolo: Super Administrator	Termina sessione
	Oggiu integrità, cicurenza e vicultati a partire e	dalla mozzanotto 2 Guida V	
The state the state of the stat	Oggi: integrita, sicarezza e risalitat a partire i Download del database 1 Personalizza	Anna Mitezzanotte	
Stato			Salva tutto
Oggi >>>	Riepilogo avviso di integrità 👔	Risultati del giorno 👔	
Cronologia 2	🔊 Nessun problema rilevato	Bloccate: Contatori:	Operazioni comuni
Avvisi <u></u>		Applicazioni 🕒 Richieste: 0	👘 Esegui rapporto
Registro di controllo		dannose: 0	💑 Crea criterio 🛛 3
Creazione rapporti		e Bloccate: 0	
Rapporti di		🗙 Riservato 📀 RTSU: 4 🕦	
presentazione Desentazione		o agii aduld:	😥 Sblocca URL
Rapporti investigativi		00401	🕖 Suggerisci nuova
Gestione criteri	4		categoria
Client	Carico del filtro attuale	(i	Casella degli strumenti
Criteri	100		Categoria LIRI
Filtri	80		
Componenti filtro	60		Verifica criterio 🛛 🗸 🗸
Amministrazione con delega	40		Verifica filtri 🛛 🗸
Blocco filtro	20		Accesso LIRI
		6, 6, 6, 6, 6	
	051 051 061 081 SV	1510 1810 2110 2A10	Verifica utente 🔍 🗸
	Dischi principali por la sicurozza in baso 🔅	Categorio principali in bace allo	Portale di supporto
	alle richieste	richieste	
			•

L' intestazione di Websense visualizza:

- Il Policy Server a cui si è collegati (vedere *Gestione di Policy Server*, pagina 282)
- Il Ruolo amministrativo corrente (vedere Introduzione ai ruoli amministrativi, pagina 242)
- Un pulsante Disconnetti da usare per uscire dalla sessione amministrativa corrente

Il contenuto visualizzato in Websense Manager varia in base ai privilegi assegnati all'utente collegato in sessione. Un utente a cui sono stati assegnati soltanto privilegi di creazione dei report, non potrà accedere alle impostazioni di configurazione o agli strumenti di amministrazione dei criteri. Per ulteriori informazioni, vedere *Amministrazione con delega*, pagina 241.

Questa sezione descrive le opzioni rese disponibili a WebsenseAdministrator e agli altri utenti con privilegi di Super Administrator.

Il riquadro di navigazione di sinistra contiene due schede: Principale e Impostazioni. Utilizzare la scheda Principale per accedere alle funzioni di stato, di creazione dei report e gestione dei criteri. Utilizzare la scheda Impostazioni per gestire il proprio account Websense e per eseguire attività di amministrazione generale del sistema.

Il **riquadro dei collegamenti di destra** contiene dei collegamenti a strumenti utili e ad attività amministrative svolte di frequente. In questo riquadro è anche possibile rivedere e salvare le modifiche apportate in Websense Manager.

 L'area superiore del riquadro di navigazione indica se esistono modifiche memorizzate nella cache, in attesa di essere salvate. Se si sta lavorando in Websense Manager, la barra Modifiche indica se esiste o meno una Sospensione delle modifiche.

Nella maggior parte dei casi, quando si esegue un'attività in Websense Manager e si fa clic su **OK**, le modifiche vengono inserite nella cache. (Occorre a volte fare clic su OK sia in una pagina secondaria che in una pagina principale per inserire le modifiche nella cache.)

Una volta inserite le modifiche nella cache, fare clic su **Salva tutto** per salvare e implementare le modifiche. Per visualizzare le modifiche memorizzate nella cache (vedere *Revisione, salvataggio e annullamento delle modifiche*, pagina 21), fare clic sul pulsante **Visualizza modifiche in sospeso**. Questo è il pulsante più piccolo, a sinistra di Salva tutto.

- **Operazioni comuni** offre collegamenti ad attività amministrative svolte di frequente. Fare clic su una voce dell'elenco per portarsi automaticamente alla pagina in cui eseguire l'attività.
- La Casella degli strumenti contiene strumenti di ricerca rapida da utilizzare per verificare le impostazioni di filtraggio definite. Per ulteriori informazioni, vedere Uso della Casella degli strumenti per verificare il comportamento dei filtri, pagina 201.

Revisione, salvataggio e annullamento delle modifiche

Se si esegue un'attività in Websense Manager e si fa clic su **OK**, le modifiche apportate vengono inserite nella cache. Usare la pagina **Visualizza modifiche in sospeso** per rivedere le modifiche memorizzate nella cache.

Importante

Evitare di fare clic due o tre volte sul pulsante OK. Un clic rapido e ripetuto sullo stesso pulsante potrebbe causare problemi di visualizzazione, in Mozilla Firefox, che si possono risolvere soltanto chiudendo il browser e riaprendolo.

Le modifiche apportate a una singola area o funzionalità vengono raggruppate sotto un'unica voce nell'elenco della cache. Ad esempio, se si aggiungono 6 client e se ne eliminano 2, l'elenco della cache indica soltanto che si sono apportate modifiche ai client. Le modifiche apportate a una pagina delle Impostazioni, d'altro canto, potrebbero generare molteplici voci nell'elenco della cache. Questo si verifica se si utilizza un'unica pagina delle Impostazioni per configurare molteplici funzioni del software Websense.

- Per salvare tutte le modifiche memorizzate nella cache, fare clic su Salva tutte le modifiche.
- Per annullare tutte le modifiche memorizzate nella cache, fare clic su Annulla tutte le modifiche.

Dopo aver selezionato Salva tutte le modifiche o Annulla tutte le modiche, la barra Modifiche, situata nel riquadro dei collegamenti di destra, viene aggiornata e si viene riportati automaticamente all'ultima pagina selezionata. Le funzioni Salva tutte le modifiche o Annulla tutte le modifiche non possono venire annullate.

Utilizzare il Registro di controllo per rivedere in dettaglio le modifiche apportate in Websense Manager. Per ulteriori informazioni, vedere *Visualizzazione ed esportazione del registro di controllo*, pagina 289.

Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte

Argomenti correlati:

- Navigazione in Websense Manager, pagina 20
- Cronologia: ultimi 30 giorni, pagina 25
- Personalizzazione della pagina Oggi, pagina 24
- *Avvisi su schermo*, pagina 292]

La pagina **Stato > Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte** è la prima pagina visualizzata quando si accede a Websense Manager. Presenta la stato corrente del software di filtraggio ed illustra graficamente l'attività di filtraggio degli accessi ad Internet, fino a un massimo di 24 ore, con inizio alle 00:01 del mattino in base all'ora indicata dal computer in cui è installato il database di registrazione.

Nell'area superiore della pagina, due sezioni riepilogative offrono una rapida panoramica dello stato corrente.

 Riepilogo avviso di integrità visualizza lo stato del software Websense. Se viene visualizzato un messaggio di errore o di avvertenza, fare clic sul messaggio di avvertenza per aprire la pagina Avvisi ed accedere ad informazioni più dettagliate (vedere *Revisione dello stato del sistema in uso*, pagina 299).

Le informazioni contenute in Riepilogo avviso di integrità vengono aggiornate ogni 30 secondi.

 In Risultati del giorno, si possono vedere esempi di come il filtraggio applicato da Websense abbia protetto la rete nel corso della giornata, oltre al numero totale di richieste di accesso ad Internet, gestite dal software, e al numero totale di altre attività importanti completate. Sotto le informazioni di riepilogo, fino a un massimo di 4 grafici offrono informazioni sull'attività di filtraggio. Questi grafici sono a disposizione dei Super Administrator e degli amministratori con delega autorizzati a visualizzare i report contenuti nella pagina Oggi. Vedere *Modifica dei ruoli*, pagina 261.

Le informazioni contenute in questi grafici vengono aggiornate ogni 2 minuti. Per visualizzare tutti i grafici, scorrere verso il basso, se necessario.

Nome del grafico	Descrizione
Carico del filtro attuale	Visualizza, in intervalli di 10 minuti, il numero di accessi ad Internet filtrati ed elaborati nel database di registrazione.
Rischi principali per la sicurezza in base alle richieste	Visualizza le categorie di Rischi principali per la sicurezza che hanno ricevuto più richieste durante la giornata ed aiuta a determinare se i criteri di filtraggio offrono il grado di protezione desiderato per la rete.
Categorie principali in base alle richieste	Visualizza le categorie che hanno registrato il più alto numero di accessi durante la giornata. Offre una panoramica di alto livello su potenziali problemi relativi a sicurezza, larghezza di banda o produttività.
Applicazione di criteri in base alla classe di rischio	Visualizza il numero di richieste, per ogni classe di rischio, che sono state autorizzate o bloccate nel corso della giornata (vedere <i>Classi di rischio</i> , pagina 41). Consente di valutare se i criteri applicati attualmente sono efficaci o se è necessario apportare modifiche.
Protocolli principali in base alla larghezza di banda	Consente di determinare quali siano i protocolli che hanno registrato il massimo uso della larghezza di banda su rete nel corso della giornata. Si possono utilizzare queste informazioni per valutare l'adeguatezza della larghezza di banda e la necessità di modifica dei criteri stabiliti.
Computer con richieste di siti a rischio per la sicurezza	Consente di verificare quali computer hanno acceduto a siti con un alto Rischio di sicurezza. Potrebbe essere utile controllare questi computer per verificare che non siano infettati da virus o spyware.
Utenti bloccati principali	Consente di identificare gli utenti che hanno richiesto, nel corso della giornata, il più alto numero di accesso a siti bloccati e di verificare la conformità con gli standard d'uso di Internet definiti dalla propria organizzazione.
Siti non categorizzati principali	Consente di verificare i siti non categorizzati dal Websense Master Database che hanno registrato il più alto numero di accessi nel corso della giornata. Andare a Operazioni comuni > Ricategorizza URL per assegnare un sito ad una determinata categoria per il relativo filtraggio.

Fare clic su qualsiasi grafico per aprire un report investigativo dettagliato.

Sopra la pagina sono disponibili tre pulsanti:

• **Download del database** disponibile soltanto per i Super Administrator, apre la pagina per visualizzare lo stato del Master Database (vedere *Verifica dello stato di download del Master Database*, pagina 288).

- **Personalizza**, disponibile soltanto per i Super Administrator, apre la pagina in cui si possono modificare i chart che devono apparire nella pagina (vedere *Verifica dello stato di download del Master Database*, pagina 288).
- Stampa, disponibile per tutti gli amministratori, apre una finestra secondaria con una versione stampabile dei grafici visualizzati nella pagina Oggi. Utilizzare le opzioni offerte dal browser per stampare questa pagina che non includono tutte le opzioni di navigazione disponibili nella finestra principale di Websense Manager.

Sotto i grafici delle attività e dei filtri Internet, il **Riepilogo di Filtering Service** illustra lo stato di ciascun Filtering Service associato al Policy Server in uso. Fare clic sull'indirizzo IP del computer in cui è installato Filtering Service per visualizzare ulteriori informazioni su quell'istanza di Filtering Service.

Per motivi di sicurezza, ciascuna sessione di Websense Manager termina dopo 30 minuti di inattività. È possibile tuttavia scegliere di continuare a monitorare i dati di filtraggio e di avviso. Selezionare **Continua a monitorare lo stato relativo alle pagine Oggi, Cronologia e Avvisi senza interruzioni**, nell'area inferiore della pagina Oggi. Le informazioni contenute in queste 3 pagine vengono regolarmente aggiornate fino a quando non si chiude il browser o non si naviga a un'altra pagina di Websense Manager.

Importante

Se si attiva l'opzione di monitoraggio e si resta nelle pagine Oggi, Cronologia e Avvisi per più di 30 minuti, il tentativo di navigare a un'altra pagina di Websense Manager riporterà automaticamente alla pagina di accesso.

Se si attiva questa opzione, ricordarsi di salvare le modifiche memorizzate nella cache prima che il periodo di timeout di 30 minuti scada.

Personalizzazione della pagina Oggi

Argomenti correlati:

- Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte, pagina 22
- Personalizzazione della pagina Cronologia, pagina 27

Utilizzare la pagina **Oggi > Personalizza** per selezionare fino a un massimo di 4 grafici da visualizzare nella pagina Stato > Oggi. Soltanto i Super Administrator (incluso il WebsenseAdministrator) che possiedono permessi completi di gestione dei criteri, possono personalizzare la pagina Oggi.

I grafici selezionati vengono visualizzati nella pagina Oggi per tutti i Super Administrator e per gli amministratori con delega che possiedono il permesso di visualizzazione dei grafici nella pagina Oggi. Vedere *Modifica dei ruoli*, pagina 261. Alcuni grafici visualizzano informazioni potenzialmente confidenziali, come ad esempio il nome degli utenti e gli indirizzi IP. Accertarsi che tutti i grafici selezionati siano appropriati per gli amministratori autorizzati alla loro visualizzazione.

Per selezionare i grafici, contrassegnarli o eliminare il contrassegno di selezione accanto ai loro rispettivi nomi. Una volta terminata la selezione, fare clic su **OK** per ritornare alla pagina Oggi e visualizzare i grafici. Per ritornare alla pagina Oggi senza apportare modifiche, fare clic su **Annulla**.

Per una breve descrizione delle informazioni visualizzate in ciascun grafico, vedere *Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte*, pagina 22.

Cronologia: ultimi 30 giorni

Argomenti correlati:

- Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte, pagina 22
- Navigazione in Websense Manager, pagina 20
- Personalizzazione della pagina Cronologia, pagina 27

Usare la pagina **Stato > Cronologia: Ultimi 30 giorni** per ottenere una panoramica dell'attività di filtraggio svolta nei 30 giorni precedenti. I grafici contenuti nella pagina vengono aggiornati tutti i giorni alle ore 00.01 del mattino al fine di incorporare i dati del giorno precedente, in base all'ora del computer in cui è stato installato il database di registrazione.

Il periodo di tempo esatto rappresentato dai grafici e dalle tabelle di riepilogo dipende dai tempi di esecuzione del filtraggio del software Websense. Durante il primo mese di installazione del software Websense, la pagina raccoglie i dati relativi al numero di giorni successivi all'installazione. Dopo il primo mese, i report contengono i dati di 30 giorni precedenti alla data attuale.

L'opzione **Stime dei risultati**, disponibile nell'area superiore della pagina, calcola una stima del risparmio realizzato su tempi ed uso della larghezza di banda oltre a visualizzare un riepilogo delle richieste bloccate in base a categorie di particolare importanza per molte organizzazioni.

Portare il mouse sopra **Tempo** o **Larghezza di banda** (nella sezione Risparmiati) per una spiegazione sul calcolo di generazione della stima (vedere *Tempi e ampiezza di banda risparmiati*, pagina 27). È possibile fare clic su **Personalizza** per modificare il modo in cui vengono calcolati i valori.

L'area **Richieste bloccate** illustra in dettaglio come il software Websense abbia protetto la rete tramite la visualizzazione di un elenco di categorie di particolare interesse per molte organizzazioni che riporta il numero totale di richieste bloccate per ciascuna categoria, nell'arco di un determinato periodo di tempo. A seconda dei permessi di creazione dei report assegnati ad un determinato ruolo, gli amministratori con delega potrebbero non essere in grado di accedere ai grafici descritti nella tabella sottostante. Vedere *Modifica dei ruoli*, pagina 261.

La pagina include fino a un massimo di 4 grafici con informazioni importanti sui filtraggi. Per visualizzare tutti i grafici, scorrere verso il basso. Le informazioni contenute in questi grafici vengono aggiornate una volta al giorno. Fare clic su qualsiasi grafico per aprire un report investigativo più dettagliato.

Nome del grafico	Descrizione
Attività in Internet in base alle richieste	Visualizza il numero di richieste di accesso a Internet filtrate ed elaborate ogni giorno nel database di registrazione.
Rischi principali per la sicurezza in base alle richieste	Visualizza le categorie del Rischio di sicurezza a cui si è acceduto recentemente ed aiuta a determinare se i criteri di filtraggio offrono il grado di protezione desiderato per la rete.
Categorie principali in base alle richieste	Visualizza le categorie con il più alto numero di accessi. Offre una panoramica di alto livello su problemi potenziali relativi alla sicurezza, larghezza di banda o produttività.
Siti non categorizzati principali	Consente di verificare i siti non categorizzati dal Websense Master Database che hanno registrato il più alto numero di accessi. Andare a Operazioni comuni > Ricategorizza URL per assegnare un sito ad una determinata categoria con relativo filtraggio.
Protocolli principali in base alla larghezza di banda	Consente di determinare quali siano i protocolli che, recentemente, hanno registrato il massimo uso della larghezza di banda su rete. Si possono utilizzare queste informazioni per valutare l'adeguatezza della larghezza di banda e la necessità di modifica dei criteri stabiliti.
Applicazione di criteri in base alla classe di rischio	Visualizza il numero di richieste, per ogni classe di rischio, che sono state recentemente autorizzate o bloccate (vedere <i>Classi di rischio</i> , pagina 41). Consente di valutare se i criteri applicati attualmente sono efficaci o se è necessario apportare modifiche.
Utenti bloccati principali	Visualizza le richieste di accesso a Internet più bloccate. Consente di verificare la conformità agli standard d'uso di Internet definiti dalla propria organizzazione.
Riepilogo applicazione criteri	Offre una panoramica delle richieste recenti di accesso a siti rientranti nella classe Rischio di sicurezza, che sono state accordate o bloccate, nonché richieste recenti di accesso ad altri siti che sono state bloccate. Consente di identificare gli aspetti del filtraggio che necessitano di una valutazione più approfondita.

Sopra la pagina vengono visualizzati due pulsanti:

 Personalizza, disponibile per i Super Administrator soltanto, apre una pagina in cui è possibile modificare i grafici che devono venire visualizzati in quella pagina nonché di modificare il metodo di calcolo delle stime di risparmio (vedere *Personalizzazione della pagina Cronologia*, pagina 27). Stampa, disponibile per tutti gli amministratori, apre una finestra secondaria con una versione stampabile dei grafici visualizzati nella pagina Cronologia. Utilizzare le opzioni offerte dal browser per stampare questa pagina che non dispone di tutte le opzioni di navigazione disponibili nella finestra principale di Websense Manager.

Tempi e ampiezza di banda risparmiati

Oltre alla maggiore sicurezza fornita dai filtri di Websense, questa funzione aiuta a minimizzare i tempi e la larghezza di banda usati da un'attività in Internet considerata non produttiva.

La sezione Risparmiate dell'area Stime dei risultati visualizza una stima dei risparmi relativi a tempi e larghezza di banda. Questi valori vengono calcolati come segue:

- Tempo risparmiato: moltiplicare il tempo usato normalmente per ogni visita per il numero di siti bloccati. Inizialmente, il software Websense utilizza un valore predefinito come numero medio di secondi che un utente passa normalmente nella visita di un sito Web richiesto. Il valore relativo ai siti bloccati rappresenta il numero totale di richieste bloccate durante un determinato periodo di tempo definito nella pagina Cronologia.
- Larghezza di banda risparmiata: moltiplicare la larghezza di banda usata normalmente per ogni visita per il numero di siti bloccati. Inizialmente, il software Websense utilizza un valore predefinito come numero medio di byte che un utente consuma normalmente nella visita di un sito Web di dimensioni medie. Il valore relativo ai siti bloccati rappresenta il numero totale di richieste bloccate durante un determinato periodo di tempo definito nella pagina Cronologia.

Vedere *Personalizzazione della pagina Cronologia*, pagina 27 per informazioni su come modificare i valori usati in questi calcoli in base all'uso effettivo di un'organizzazione.

Personalizzazione della pagina Cronologia

Argomenti correlati:

- Cronologia: ultimi 30 giorni, pagina 25
- Personalizzazione della pagina Oggi, pagina 24

Utilizzare la pagina **Cronologia > Personalizza** per determinare i grafici da visualizzare nella pagina Stato > Cronologia e per determinare come vanno calcolati i risparmi relativi a tempi e larghezza di banda.

Inserire il contrassegno di selezione accanto al nome dei grafici, fino a un massimo di 4, da visualizzare nella pagina Cronologia. Per una breve descrizione di ciascun grafico, vedere *Cronologia: ultimi 30 giorni*, pagina 25. Soltanto i Super Administrator (incluso il WebsenseAdministrator) che possiedono permessi completi

di gestione dei criteri, possono personalizzare la visualizzazione dei grafici della pagina Cronologia.

Alcuni grafici visualizzano informazioni potenzialmente confidenziali, come ad esempio il nome degli utenti. Accertarsi che tutti i grafici selezionati siano appropriati per gli amministratori autorizzati alla loro visualizzazione.

Sia i Super Administrator che gli amministratori con delega possono personalizzare il modo in cui vengono calcolati i risparmi relativi a tempi e larghezza di banda. Gli amministratori con delega possono accedere a questi campi facendo clic sul link **Personalizza** nel pop-up con la descrizione dei calcoli relativi al risparmio di tempi e larghezza di banda.

Inserire le nuove misurazioni di tempi e larghezza di banda medi al fine di utilizzarli come base per i calcoli:

Opzione	Descrizione
Media dei secondi risparmiati per ogni pagina bloccata	Inserire il numero medio di secondi, in base ai calcoli di stima dell'organizzazione, che l'utente passa nella visita di una singola pagina.
	Il software Websense moltiplica questo valore per il numero di pagine bloccate al fine di determinare i risparmi di tempo che vengono riportati nella pagina Cronologia.
Media della larghezza di banda risparmiata [in KB] per ciascuna pagina bloccata	Inserire una valore medio, in kilobyte (KB) per le pagine visualizzate. Il software Websense moltiplica questo valore per il numero di pagine bloccate al fine di determinare i risparmi relativi alla larghezza di banda che vengono riportati nella pagina Cronologia.

Una volta completate le modifiche, fare clic su **OK** per ritornare alla pagina Cronologia e visualizzare i nuovi grafici con le stime relative a tempi e larghezza di banda. Per ritornare alla pagina Cronologia senza apportare modifiche, fare clic su **Annulla**.

Sottoscrizioni

Le sottoscrizioni di Websense vengono rilasciate in base ad ogni client del software. Il client è un utente o un computer collegato in rete.

Quando si acquista una sottoscrizione, viene rilasciata una chiave di sottoscrizione, inviata tramite e-mail. Ogni chiave è valida per un'unica installazione del Websense Policy Server. Se si installano molteplici Policy Server, occorre avere una chiave specifica per ognuno di essi.

Prima di poter applicare i filtri, occorre immettere una chiave di sottoscrizione valida (vedere *Configurazione delle informazioni relative all'account*, pagina 31). Questo

consente di scaricare il Master Database (vedere *Websense Master Database*, pagina 32), che consente di applicare i filtri di Websense ai client.

Dopo aver completato il download del database, Websense Manager visualizza il numero di client inclusi nella chiave di sottoscrizione.

Il software Websense mantiene una tabella delle sottoscrizioni per i client che vengono filtrati ogni giorno. La tabella delle sottoscrizioni viene azzerata ogni notte. La prima volta che un client invia una richiesta di accesso a Internet dopo l'azzeramento della tabella, il suo indirizzo IP viene inserito nella tabella.

Quando il numero di client elencati nella tabella ha raggiunto il numero massimo di sottoscrizioni, i clienti non ancora inclusi nell'elenco che inviano una richiesta di accesso a Internet, vengono considerati in eccedenza rispetto al numero di client autorizzati. In questo caso, il client che supera il numero massimo di sottoscrizioni viene interamente bloccato da qualsiasi accesso a Internet oppure gli viene concesso un accesso non filtrato, in base alla configurazione definita. Analogamente, quando una sottoscrizione scade, tutti i client vengono interamente bloccati o possono accedere senza applicazione di filtri, a seconda delle impostazioni definite.

Per configurare l'attività di filtraggio da applicare dopo il superamento o la prossima scadenza di una sottoscrizione, vedere *Configurazione delle informazioni relative all'account*, pagina 31.

Per configurare l'invio da parte del software Websense di una e-mail di avviso del superamento o del prossimo raggiungimento dei limiti massimi consentiti da una sottoscrizione, vedere *Configurazione degli avvisi del sistema*, pagina 295.

Il numero di categorie filtrate dipende dalla sottoscrizione Websense. Il software Websense filtra tutti i siti di tutte le categorie attivate in base al proprio acquisto.

Gestione di un account tramite il portale MyWebsense

Websense, Inc., dispone di un portale riservato ai clienti, all'indirizzo <u>www.mywebsense.com</u>, che offre l'accesso ad aggiornamenti del prodotto, patch correttivi, ultime novità relative ai prodotti, versioni di prova e risorse di assistenza al cliente per il software Websense.

Quando si crea un account, viene visualizzato un messaggio che richiede l'inserimento delle chiavi di sottoscrizione di Websense. Ciò aiuta a garantire l'accesso ad informazioni, avvertenze e patch correttivi attinenti al prodotto e alla versione di Websense in uso.

Una volta aperto un account in MyWebsense, se in qualsiasi momento successivo non fosse possibile accedere a Websense Manager, a causa ad esempio della perdita della password di WebsenseAdministrator, sarà sufficiente fare clic su **Password dimenticata** nella pagina di accesso a Websense Manager. Viene visualizzato un messaggio che richiede di accedere a MyWebsense. Verranno qui fornite le istruzioni necessarie alla generazione e attivazione di una nuova password.



Importante

Qualora si richieda una nuova password, la chiave di sottoscrizione selezionata nel portale MyWebsense deve corrispondere alla chiave inserita nella pagina Account di Websense Manager.

Molteplici membri della propria organizzazione possono creare dei dati di accesso a MyWebsense in base alla stessa chiave di sottoscrizione.

Per accedere al portale MyWebsense da Websense Manager, andare a Guida > MyWebsense.

Attivazione di Websense Web Protection Services™

Le sottoscrizioni a Websense Web Security includono l'accesso a Websense Web Protection Services: SiteWatcher[™], BrandWatcher[™] e ThreatWatcher[™]. Questi servizi, una volta attivati, contribuiscono alla protezione dei siti Web, dei marchi e dei server Web della propria organizzazione.

Servizio	Descrizione
SiteWatcher	Avverte quando i siti Web dell'organizzazione sono stati infettati da un codice dannoso consentendo quindi un intervento immediato per la protezione di clienti acquisiti, clienti potenziali e partner che potrebbero visitare il sito.
BrandWatcher	 Avverte quando i siti Web o i marchi dell'organizzazione sono stati mirati da attacchi di phishing (frodi)o da attacchi ai codici di accesso. Include tecnologie di sicurezza nell'uso di Internet, generazione di dettagli su eventuali attacchi e altre informazioni relative alla sicurezza in modo che si possa intervenire, notificare i clienti e ridurre al minimo qualsiasi potenziale impatto sulle pubbliche relazioni dell'organizzazione.
ThreatWatcher	 Offre una prospettiva del server Web dell'organizzazione dal punto di vista dell'hacker, esegue una scansione per identificare aree vulnerabili e minacce potenziali. Segnala i livelli di rischio ed offre raccomandazioni tramite un portale Web-based. Aiuta a prevenire attacchi nocivi a carico dei server Web prima che vengano attuati.

Accedere al portale MyWebsense per attivare Websense Protection Services. Una volta attivato ThreatWatcher, accedere a MyWebsense per visualizzare eventuali report su minacce dirette ai server Web.

Configurazione delle informazioni relative all'account

Argomenti correlati:

- Sottoscrizioni, pagina 28
- Configurazione dei download del database, pagina 34
- Gestione dei protocolli, pagina 189

Utilizzare la pagina **Impostazioni** > **Account** per inserire e visualizzare informazioni relative alla sottoscrizione e per modificare la password di WebsenseAdministrator utilizzata per accedere a Websense Manager. WebsenseAdministrator è l'account amministrativo master predefinito che viene utilizzato per gestire il software Websense.

Da qui si può anche attivare il software Websense per inviare dati sull'uso del protocollo a Websense, Inc. in forma anonima. Queste informazioni possono venire utilizzate per aggiornare il Websense Master Database che raccoglie oltre 36 milioni di siti Internet e oltre 100 definizioni di protocollo (per ulteriori informazioni, vedere *Websense Master Database*, pagina 32).

1. Una volta installato il software Websense, o in qualsiasi momento si riceva una nuova chiave di sottoscrizione, inserire la chiave nel campo **Chiave di sottoscrizione**.

Una volta inserita una nuova chiave di sottoscrizione e dopo aver fatto clic su OK, viene scaricato automaticamente un Master Database.

2. Una volta completato lo scaricamento del primo Master Database, vengono visualizzate le informazioni seguenti:

Scadenza chiave	La data di scadenza della chiave di sottoscrizione. Una volta raggiunta tale scadenza, occorre rinnovare la sottoscrizione per poter continuare a scaricare il Master Database e applicare i filtri necessari alla rete.
Utenti di rete con sottoscrizione	Numero degli utenti di rete a cui si possono applicare i filtri.
Utenti remoti con sottoscrizione	Numero di utenti esterni alla rete a cui si possono applicare i filtri (richiede la funzione facoltativa Remote Filtering).

- 3. Selezionare **Blocca utenti alla scadenza o al superamento della sottoscrizione** per:
 - Bloccare tutti gli accessi a Internet da parte degli utenti alla scadenza della sottoscrizione.
 - Bloccare tutti gli accessi a Internet da parte degli utenti che superano il numero massimo consentito di utenti con sottoscrizione.

Se questa opzione non è selezionata, gli utenti avranno diritto di accesso non filtrato al verificarsi di queste condizioni.

- 4. Per modificare la password di WebsenseAdministrator, inserire prima la password in uso e quindi inserire e confermare la nuova password.
 - La password deve contenere da 4 a 25 caratteri. Rispetta maiuscole e minuscole e può includere lettere, numeri, caratteri speciali e spazi.
 - Si consiglia di creare una password difficilmente identificabile per l'accesso all'account del WebsenseAdminsitrator. Questa password deve contenere almeno 8 caratteri tra cui una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale.
- 5. Selezionare **Invia i dati relativi a protocollo e categoria a Websense, Inc.** affinché il software Websense raccolga i dati d'uso delle categorie e protocolli definiti per Websense e li invii in forma anonima a Websense, Inc.

Questi dati relativi all'uso aiutano Websense, Inc, a migliorare continuamente le funzioni di filtraggio offerte dal software Websense.

Websense Master Database

Argomenti correlati:

- Aggiornamenti del database in tempo reale, pagina 33
- ◆ *Real-Time Security Updates*[™], pagina 33
- Filtri di categoria e di protocollo, pagina 38
- Gestione di Filtering Service, pagina 287
- Verifica dello stato di download del Master Database, pagina 288
- Ripresa del download del Master Database, pagina 288

The Websense Master Database include le categorie e le definizioni di protocollo che costituiscono la base dei filtri da applicare ai contenuti di Internet (vedere *Filtri di categoria e di protocollo*, pagina 38).

- Le **Categorie** vengono utilizzate per raggruppare i siti Web (identificati da URL e indirizzi IP) con contenuto simile.
- Le definizioni dei **Protocolli** raggruppano vari protocolli di comunicazione su Internet, utilizzati per scopi analoghi come ad esempio trasferimento di file o invio di messaggi istantanei.

Una versione limitata del database dei filtri viene installata durante l'installazione del software Websense, ma si consiglia di scaricare l'intero Master Database non appena possibile per poter usufruire delle funzioni di filtraggio completo dei contenuti Internet. Per scaricare il Master Database per la prima volta, inserire la chiave di sottoscrizione nella pagina **Impostazioni** > **Account** (vedere *Configurazione delle informazioni relative all'account*, pagina 31).

Se il software Websense deve passare attraverso un server proxy per eseguire il download, utilizzare anche la pagina **Impostazioni > Download del Database** per configurare le impostazioni del server proxy (vedere *Configurazione dei download del database*, pagina 34).

La procedura di scaricamento dell'intero database potrebbe richiedere diversi minuti o più di un'ora, a seconda della velocità del collegamento con Internet, della larghezza di banda, della memoria disponibile e dello spazio disponibile sul disco fisso.

Dopo lo scaricamento iniziale, il software Websense scarica le modifiche apportate al database in base alla frequenza e ai tempi stabliti dall'organizzazione (vedere *Configurazione dei download del database*, pagina 34). Poiché il Master Database viene aggiornato frequentemente, l'impostazione predefinita prevede scaricamenti giornalieri del database.

Se il Master Database non viene aggiornato oltre a 14 giorni consecutivi, il software non applica più i filtri alle richieste di accesso a Internet.

Per avviare il download del database in qualsiasi momento, o per verificare lo stato dell'ultimo download del database, la data dell'ultimo download o il numero di versione del database corrente, andare a **Stato > Oggi** e fare clic su **Download del database**.

Aggiornamenti del database in tempo reale

Oltre ai download pianificati, il software Websense esegue aggiornamenti di emergenza del database, in base a specifiche necessità. È possibile, ad esempio, usare un aggiornamento in tempo reale per ricategorizzare un sito che era stato erroneamente categorizzato. Questi aggiornamenti garantiscono che i siti e i protocolli vengano correttamente filtrati.

Il software Websense controlla ad ogni ora la disponibilità di aggiornamenti del database.

Gli aggiornamenti più recenti sono inclusi in un elenco della pagina **Stato > Avvisi** (vedere *Revisione dello stato del sistema in uso*, pagina 299).

Real-Time Security Updates™

Oltre a ricevere gli aggiornamenti standard del database in tempo reale, gli utenti di Websense Web Security possono attivare una funzione di aggiornamento di sicurezza in tempo reale per ricevere aggiornamenti del Master Database attinenti alla sicurezza, non appena vengono pubblicati da Websense, Inc.

Real-Time Security Updates aggiunge un ulteriore livello di protezione contro potenziali minacce alla sicurezza, provenienti da Internet. L'installazione di questi aggiornamenti, non appena disponibili, riduce la vulnerabilità a nuovi attacchi phishing (frodi), a rogue applications e a codici dannosi che attaccano siti o applicazioni Web di uso frequente.

Filtering Service controlla ogni 5 minuti la disponibilità di aggiornamenti relativi alla sicurezza, ma poiché questi aggiornamenti vengono inviati soltanto in presenza di

minacce alla sicurezza, le modifiche effettive sono occasionali e intendono non interferire con l'attività di rete normale.

Utilizzare la pagina **Impostazioni > Download del database** per attivare aggiornamenti di sicurezza in tempo reale (vedere *Configurazione dei download del database*, pagina 34).

Configurazione dei download del database

Argomenti correlati:

- Configurazione delle informazioni relative all'account, pagina 31
- Websense Master Database, pagina 32
- Verifica dello stato di download del Master Database, pagina 288

Utilizzare la pagina **Impostazioni > Download del database** per definire la pianificazione dei tempi di scaricamento automatico del Master Database. Consente inoltre di specificare la presenza di un server proxy o di un firewall che il software Websense deve attraversare per scaricare il database.

1. Selezionare Giorni in cui eseguire il download per i download automatici.

Occorre scaricare i Master Database almeno una volta ogni 14 giorni affinché il software Websense continui ad applicare i filtri necessari senza interruzioni superflue. Se si deselezionano tutti i giorni definiti per il download, il software Websense cerca di eseguire automaticamente un download 7 giorni dopo l'ultimo aggiornamento.



2. Selezionare il tempo di inizio (**Da**) e il tempo di fine (**A**) per l'**Intervallo temporale del download**. Se non si seleziona un tempo specifico, il download del database avverrà tra le ore 21.00 e le ore 6.00 del mattino.

Il software Websense seleziona un'ora a caso in questo intervallo di tempo, per contattare il server del Master Database. Per configurare le avvertenze da visualizzare in caso di un download non riuscito, vedere *Configurazione degli avvisi del sistema*, pagina 295.

Nota

Dopo aver scaricato il Master Database o averlo aggiornato, l'uso della CPU potrebbe raggiungere il 90% durante il caricamento del database nella memoria locale. (Websense Web Security) Selezionare Abilita gli aggiornamenti di sicurezza in tempo reale affinché il software Websense controlli ogni 5 minuti la disponibilità di aggiornamenti di sicurezza del Master Database. Se un aggiornamento di sicurezza è disponibile, questo viene immediatamente scaricato.

Gli aggiornamenti di sicurezza in tempo reale proteggono la rete da vulnerabilità verso nuovi attacchi phishing (frodi), rogue applications e codici dannosi che attaccano siti o applicazioni Web di uso comune.

4. Selezionare **Utilizza server proxy o firewall** se il software Websense deve accedere a Internet passando da un server proxy o un firewall (al di fuori dei prodotti di integrazione con cui il software Websense comunica) per scaricare il Master Database. Procedere quindi con la configurazione seguente:

IP o nome del	Inserire l'indirizzo IP o il nome del computer che
server	funge da host per il server proxy o il firewall.
Porta	Inserire il numero della porta che il download del database deve attraversare (il numero predefinito è 8080).

5. Se il server proxy o il firewall configurati al punto 4 necessitano di un'autenticazione per raggiungere Internet, selezionare **Utilizza autenticazione** ed inserire quindi il **Nome utente** e la **Password** che il software Websense deve usare per accedere a Internet.



Nota

Se si è selezionata l'opzione Utilizza autenticazione, il server proxy o il firewall devono venire configurati in modo da accettare un semplice testo o un'autenticazione generica che consenta i download del Master Database.

Per impostazione predefinita, il nome utente e la password vengono codificati in modo da corrispondere al set di caratteri definiti per il computer locale che funge da Policy Server. Questa codifica può venire configurata manualmente tramite le pagine **Impostazioni > Servizi di directory** (vedere *Impostazioni directory avanzate*, pagina 67).

Prova della configurazione della rete

Per poter applicare i filtri alle richieste di accesso a Internet, il software Websense deve essere in grado di rilevare il traffico Internet diretto a, o proveniente da, i dispositivi collegati in rete. Utilizzare Strumento di rilevazione del traffico di rete per accertare che questa comunicazione con Internet sia visibile al software di applicazione dei filtri. Per informazioni, vedere *Verifica della configurazione di Network Agent*, pagina 358.

Se il Rilevatore traffico di rete non è in grado di vedere tutti i segmenti della rete, fare riferimento a *Configurazione della rete*, pagina 349 per istruzioni di configurazione.

Assistenza tecnica di Websense

Websense, Inc., investe il massimo impegno per garantire la soddisfazione del cliente. Andare al sito Websense Technical Support in qualsiasi momento per accedere alle informazioni più recenti sulla versione corrente e per accedere alla Knowledge Base o alla documentazione del prodotto, oppure per inviare una richiesta di assistenza tecnica.

www.websense.com/SupportPortal/

I tempi di risposta per le richieste di assistenza inviate online durante l'orario di lavoro si aggirano sulle 4 ore. Le risposte a richieste di assistenza inviate fuori orario di lavoro vengono evase il giorno lavorativo successivo.

È anche disponibile un'assistenza telefonica. Per ottenere rapidamente una risposta a richieste telefoniche, occorre disporre di quanto segue:

- Chiave di sottoscrizione rilasciata da Websense
- Accesso a Websense Manager
- Accesso al computer su cui sono installati Filtering Service e Log Server, e al server con il database (Microsoft SQL Server o MSDE)
- Permesso di accesso al database di registrazione di Websense
- Familiarità con l'architettura di rete o accesso a persone che possiedono tale familiarità
- Specifiche dei computer su cui sono in esecuzione Filtering Service e Websense Manager
- Un elenco delle altre applicazioni in esecuzione su un computer con Filtering Service

Per problemi gravi, potrebbero venire richieste ulteriori informazioni.

Il servizio di assistenza telefonica standard è disponibile negli orari di lavoro normali da lunedì a venerdì, ai numeri seguenti:

- San Diego, California, USA: +1 858.458.2940
- Londra, Inghilterra: +44 (0) 1932 796244

Per informazioni sugli orari di lavoro e su altre opzioni di assistenza al cliente, visitare il sito di assistenza tecnica riportato sopra.

I clienti residenti in Giappone possono contattare il distributore autorizzato di zona per ottenere il servizio di assistenza più rapido.
Filtri per l'uso di Internet

Argomenti correlati:

- Filtri di categoria e di protocollo, pagina 38
- *Gestione dei filtri*, pagina 48
- Configurazione delle impostazioni di filtraggio di Websense, pagina 57
- Criteri di filtraggio dell'uso di Internet, pagina 75
- Perfezionamento dei criteri di filtraggio, pagina 171

I criteri vengono definiti per regolare l'accesso a Internet da parte degli utenti. I criteri costituiscono una pianificazione che informa il software Websense come e quando deve filtrare l'accesso ai siti Web e alle applicazioni in Internet. I criteri consistono negli elementi di base seguenti:

- Filtri di categoria, utilizzati per applicare azioni (autorizzazione, blocco) a varie categorie di siti Web
- **Filtri di protocollo**, utilizzati per applicare azioni alle applicazioni disponibili in Internet e ai protocolli non-HTTP
- Una pianificazione che determina quando il filtro va applicato

Il filtraggio basato sui criteri consente di assegnare ai client (utenti, gruppi e computer collegati in rete) vari livelli di accesso a Internet. Occorre prima di tutto creare dei filtri che definiscano in modo preciso le restrizioni relative all'accesso a Internet e quindi usare questi filtri per costruire i criteri applicabili.

Alla prima installazione, il software Websense crea un criterio **Predefinito** e lo utilizza per iniziare a monitorare le richieste di accesso a Internet dopo aver immesso la chiave di sottoscrizione (vedere *Criterio Predefinito*, pagina 76). Inizialmente, il criterio Predefinito concede un permesso di accesso a tutte le richieste.



Se si aggiorna da una versione precedente del software Websense, le impostazioni dei criteri definiti vengono preservate. A seguito dell'aggiornamento, si consiglia di rivalutare tali criteri per confermarne o meno la validità. Per applicare a determinati client restrizioni di filtraggio diverse, occorre definire per prima cosa i filtri di categoria. Si può definire:

- Un filtro di categoria che blocca l'accesso a tutti i siti Web ad eccezione di quelli che fanno parte delle categorie Business ed economia, Istruzione, Notizie e media.
- Un secondo filtro di categoria che concede l'accesso a tutti i siti Web ad eccezione di quelli che costituiscono un rischio per la sicurezza e quelli con contenuto riservato ad un pubblico adulto.
- Un terzo filtro di categoria che monitora l'accesso a siti Web, senza tuttavia bloccarlo (vedere *Creazione di un filtro di categoria*, pagina 49).

Questi filtri di categoria possono essere accompagnati da:

- Un filtro di protocollo che blocca l'accesso alla messaggistica immediata e ai siti di Chat, allo scambio di file Peer-to-Peer, a Elusione via Proxy e ai gruppi di protocollo per uno streaming multimediale.
- Un secondo filtro di protocollo che accetta tutti i protocolli non-HTTP ad eccezione di quelli associati a elusione via Proxy.
- Un terzo filtro di protocollo che accetta tutti i protocolli non-HTTP (vedere *Creazione di un filtro di protocollo*, pagina 52).

Una volta definito un set di filtri conforme alle regole definite per l'accesso a Internet della propria organizzazione, si può aggiungerlo ai criteri e quindi applicarlo ai client (vedere *Criteri di filtraggio dell'uso di Internet*, pagina 75).

Filtri di categoria e di protocollo

Il Websense Master Database organizza i siti Web simili (identificati da URL e indirizzi IP) in varie **categorie**. Ciascuna categoria ha un nome descrittivo, come ad esempio, Materiale riservato ad un pubblico adulto, Gioco d'azzardo, o Scambio di file Peer-To-Peer. È anche possibile creare categorie personalizzate al fine di raggruppare siti di particolare interesse per l'organizzazione (vedere *Creazione di una categoria personalizzata*, pagina 182). Le categorie del Master Database e le categorie definite dall'utente costituiscono la base dei filtri di accesso a Internet.

Websense Inc. non formula giudizi di valore sulle categorie o sui siti inclusi nel Master Database. Le categorie vengono definite allo scopo di creare raggruppamenti utili di siti problematici per i clienti dotati di una sottoscrizione. Non intendono caratterizzare un sito o un gruppo di siti o le persone o gruppi di interesse che li costituiscono, e non vanno intesi come tali. Similarmente, le etichette apposte alle categorie di Websense sono basate su principi di praticità e non intendono in alcun modo comunicare un'opinione o un giudizio, di approvazione o disapprovazione, nei riguardi del contenuto o dei siti che vengono in tal modo classificati.

Un elenco aggiornato delle categorie incluse nel Master Database è disponibile a:

www.websense.com/global/en/ProductsServices/MasterDatabase/ URLCategories.php Per suggerire l'aggiunta di un sito al Master Database, fare clic su **Suggerisci nuova** categoria nel riquadro dei collegamenti di destra di Websense Manager, oppure andare a:

www.websense.com/SupportPortal/SiteLookup.aspx

Dopo aver acceduto al portale MyWebsense, si accede automaticamente allo strumento Site Lookup e Category Suggestion.

Se si crea un **filtro di categoria** in Websense Manager, occorre scegliere le categorie da bloccare e quelle da autorizzare.

Oltre a raccogliere le categorie di URL, il Websense Master Database include i gruppi di protocolli utilizzati per la gestione del traffico Internet non-HTTP. Ciascun gruppo di protocolli definisce tipi simili di protocolli Internet (come ad esempio FTP o IRC) e di applicazioni (come AOL Instant Messenger o BitTorrent). Le definizioni vengono verificate e aggiornate frequentemente se non ogni notte.

Come per le categorie, è anche possibile definire dei protocolli personalizzati da usare nei filtri di accesso a Internet.

L'elenco aggiornato dei protocolli inclusi nel Master Database è disponibile a:

www.websense.com/global/en/ProductsServices/MasterDatabase/ ProtocolCategories.php

Se si crea un **filtro di protocollo** in Websense Manager, occorre scegliere i protocolli da bloccare e quelli da autorizzare.

Nota
Occorre aver installato Network Agent per attivare i filtri di protocollo.

Alcuni protocolli definiti da Websense consentono di bloccare il traffico in uscita verso Internet, destinato ad un server esterno, ad esempio un server di messaggistica immediata specifico. Soltanto i protocolli definiti da Websense con numeri di porta assegnati dinamicamente possono venire bloccati come traffico in uscita.

Nuove categorie e protocolli

Se si aggiungono nuove categorie e nuovi protocolli al Master Database, a ciascuno di essi viene assegnata un'azione di filtraggio predefinita, come ad esempio **Autorizza** o **Blocca** (vedere *Azioni di filtraggio*, pagina 44).

- L'azione predefinita viene applicata a tutti i filtri di categoria e di protocollo attivi (vedere *Gestione dei filtri*, pagina 48). Per modificare il modo in cui determinate categorie o protocolli vengono filtrati, occorre modificare i filtri attivi.
- L'azione predefinita si basa sul feedback ricevuto relativamente all'idoneità, o all'attinenza o meno di un sito al business aziendale

Si può configurare il software Websense per generare un'avvertenza di sistema e segnalare all'utente che una nuova categoria o un nuovo protocollo sono stati aggiunti al Master Database. Per ulteriori informazioni, vedere *Avvisi su schermo*, pagina 292.

Categorie speciali

Il Master Database contiene categorie speciali che agevolano la gestione di particolari tipi di uso di Internet. Le categorie seguenti sono disponibili in tutte le edizioni del software Websense:

◆ La categoria Eventi speciali viene utilizzata per classificare i siti considerati di argomento ad intenso interesse in modo da agevolare la gestione dell'aumento di traffico Internet in concomitanza con eventi speciali. Ad esempio, la Coppa del mondo potrebbe venire inserita nella categoria Sport, ma spostata nella categoria Eventi speciali mentre sono in corso le finali.

Gi aggiornamenti della categoria Eventi speciali vengono aggiunti al Master Database durante i download pianificati. I siti vengono aggiunti a questa categoria per un breve periodo di tempo, dopodiché vengono spostati in un'altra categoria o eliminati dal Master Database.

- La categoria **Produttività** è incentrata sulla prevenzione di comportamenti che causano perdite di tempo.
 - Pubblicità
 - Download di freeware e software
 - Messaggistica immediata
 - Attività di Borsa online
 - Guadagna navigando
- La categoria Larghezza di banda è incentrata sul risparmio dell'uso della larghezza di banda.
 - Radio e TV in Internet
 - Telefonia in Internet
 - Scambio di file Peer-to-Peer
 - Archiviazione e backup su rete di materiale personale
 - Streaming media

Websense Web Security include altre categorie relative alla sicurezza:

- Websense Security Filtering (nota anche come Sicurezza) incentrata sui siti Internet che contengono codici malevoli e che possono aggirare programmi di rilevazione di virus. I siti inclusi in questa categoria vengono bloccati per predefinizione.
 - Bot network
 - Keyloggging
 - Siti web pericolosi
 - Phishing e altri tipi di frodi
 - Software potenzialmente indesiderati
 - Spyware

- Protezione estesa è incentrata soprattutto sui siti Web potenzialmente pericolosi. I siti inclusi nelle sottocategorie Esposizione elevata e Nuove minacce vengono bloccati per predefinizione.
 - Esposizione elevata include siti che camuffano la loro vera natura o identità o che includono elementi indicativi di un intento maligno latente.
 - **Nuove minacce** include siti che fungono da host per lo sfruttamento di codici, sia noti che potenziali.
 - La categoria **Contenuto potenzialmente dannoso** include siti che contengono, con molta probabilità, materiale di scarsa o di nessuna utilità.

Il gruppo Protezione estesa filtra l'accesso a siti Web potenzialmente pericolosi in base alla loro *reputazione*. La reputazione del sito deriva da segni premonitori di attività potenzialmente dannose. Un attaccante può mirare a un URL contenente, ad esempio, un errore ortografico comune, e che potrebbe altrimenti essere un URL legittimo. Questo tipo di sito può venire utilizzato per distribuire malware a determinati utenti prima che i filtri tradizionali possano venire aggiornati classificando questi siti come pericolosi.

Quando la funzione di ricerca di Websense, rivolta alla sicurezza, rileva una minaccia potenziale, questa viene aggiunta alla categoria Protezione estesa fino a quando Websense non è certo al 100% della categorizzazione definitiva del sito.

Classi di rischio

Argomenti correlati:

- Assegnazione delle categorie alle classi di rischio, pagina 312
- Report di presentazione, pagina 100
- *Report investigativi*, pagina 119

Websense Master Database raggruppa le categorie in **classi di rischio**. Le classi di rischio suggeriscono diversi tipi, o diversi livelli di vulnerabilità posti da siti compresi in un gruppo di categorie.

Le classi di rischio vengono utilizzate primariamente nella generazione dei report. Le pagine Oggi e Cronologia includono grafici che illustrano l'attività svolta in Internet in base alla classe di rischio ed è quindi possibile generare report di presentazione o report investigativi organizzati in base alla classe di rischio.

Le classi di rischio possono anche essere utili nella creazione di filtri di categoria. Ad esempio, il filtro di categoria Sicurezza di base blocca tutte le categorie incluse per predefinizione nella classe Rischio di sicurezza. I raggruppamenti in base alla classe di rischio possono venire utilizzati come linee guida quando si creano filtri di categoria personalizzati, in quanto possono aiutare a decidere se una determinata categoria debba venire autorizzata, bloccata o se debbano venire ad essa assegnate una o più restrizioni.

Il software Websense include 5 classi di rischio, elencate qui di seguito. Per predefinizione, il software Websense raggruppa le categorie qui di seguito in ciascuna classe di rischio.

- Una categoria può essere inserita in molteplici classi di rischio o può non venire assegnata ad alcuna classe di rischio.
- I raggruppamenti possono venire periodicamente modificati nel Master Database.

Responsabilità legale

Materiale riservato ad adulti (inclusi contenuti per adulti, biancheria intima e costumi da bagno, nudità e sesso)

Larghezza di banda > Scambio file Peer-to-Peer

Gioco d'azzardo

Illegale o contestabile

Materiale IT > Hacking (Pirateria informatica) e Elusione via Proxy

Materiale militare ed estremista

Razzismo e odio

Cattivo gusto

Violenza

Armi

Perdita di larghezza di banda

Larghezza di banda (tra cui Radio e TV in Internet, Telefonia in Internet, Scambio di file Peer-to-Peer, Archiviazione e backup su rete di materiale personale e Streaming media)

Intrattenimento > Servizi di download MP3 e audio

Produttività > Pubblicità e Download di Freeware *e* di software

Utilizzo aziendale

Business e economia (inclusi dati e servizi finanziari)

Istruzione > Materiale scolastico e Materiale di riferimento

Governo (incluso materiale di argomento militare)

Tecnologia informatica – IT (tra cui Sicurezza informatica, Motori di ricerca e portali, e siti di traduzione URL)

Viaggi e turismo

Veicoli

Rischio sicurezza

Larghezza di banda > Scambio file Peer-to-Peer

Protezione estesa (tra cui Esposizione elevata, Nuove minacce e Contenuto potenzialmente dannoso) [*Websense Web Security*]

Tecnologia informatica > Hacking (pirateria informatica) e Elusione via Proxy

Rischio sicurezza

Produttività > Download di freeware e software

Sicurezza (tra cui Reti Bot, Keylogging, siti Web dannosi, Phishing [falsificazione di pagine Web] e altre frodi, software potenzialmente indesiderati e Spyware [programmi spia])

Perdita di produttività

Aborti (tra cui materiale Pro-choice [Diritto di scelta] *e* Pro-Life [Diritto alla vita])

Materiale per adulti > Educazione sessuale

Gruppi di sostegno

Larghezza di banda > Radio e TV in Internet, Scambio di file Peer-to-Peer e Streaming media

Droghe (tra cui Abuso di droga, marijuana, farmaci prescrittibili, additivi / composti non regolati)

Istruzione (tra cui Istituti culturali e Istituti scolastici)

Intrattenimento (tra cui Servizi di download MP3 e audio)

Gioco d'azzardo

Giochi

Governo > Gruppi politici

Salute

Tecnologia informatica - IT > Web Hosting

Comunicazione in Internet (tra cui E-mail in generale, E-mail organizzata, messaggistica e Web Chat)

Ricerca di lavoro

Notizie e media (tra cui pubblicazioni alternative)

Produttività (tra cui download di Freeware e Software, Messaggistica immediata, Forum e Bacheche, Attività di Borsa e Guadagna navigando)

Religione (tra cui religioni non tradizionali, occultismo, folclore *e* religioni tradizionali)

Acquisti in linea (tra cui Vendite all'asta via Internet e Immobiliari)

Organismi sociali (tra cui organizzazioni professionali e di lavoratori, servizi ed organizzazioni filantropiche, organizzazioni sociali ed affiliazioni)

Vita sociale e stili di vita (tra cui alcool e tabacco, interessi gay, lesbici o bisessuali, hobby, servizi di incontri, ristoranti e conviti, comunità virtuali e siti personali)

Eventi speciali

Sport (tra cui Caccia sportiva e Club di tiro)

Viaggi e turismo

Veicoli

I Super Administrator possono modificare le categorie assegnate a ciascuna classe di rischio tramite la pagina **Impostazioni > Classe di rischio** (vedere *Assegnazione delle categorie alle classi di rischio*, pagina 312)

Gruppi di protocolli per la sicurezza

Oltre alle categorie Sicurezza e Protezione estesa, Websense Web Security include due protocolli finalizzati ad aiutare nella rilevazione e nella protezione contro spyware e codici o contenuti malevoli trasmessi tramite Internet.

- Il gruppo di protocolli **Traffico dannoso** include il protocollo **Reti bot** finalizzato al blocco del traffico di tipo "comando e controllo" generato da un bot nel tentativo di collegarsi con una botnet a scopo di attacco.
- Il gruppo di protocolli **Traffico dannoso Solo monitoraggio** viene utilizzato per identificare il traffico che potrebbe essere associato a un software dannoso.
 - Worm provenienti da e-mail monitora il traffico SMPT in uscita che potrebbe essere generato da un attacco di worm via e-mail.
 - Altro traffico dannoso monitora il traffico in entrata e in uscita che si sospetta abbia connessioni con applicazioni dannose.

Il gruppo di protocolli Traffico dannoso viene bloccato per impostazione predefinita e può venire configurato nell'ambito dei propri filtri di protocollo (vedere *Modifica di un filtro di protocollo*, pagina 53). I protocolli Traffico dannoso – Solo monitoraggio possono venire registrati a scopo di generazione di report ma non sarà possibile applicare alcuna azione di filtraggio.

Allegati dei programmi di messaggistica immediata

La funzione Allegati dei programmi di messaggistica immediata è facoltativa. Se si dispone di questa funzione, è possibile limitare lo scambio dei file con i client di messaggistica immediata (IM) tra cui AOL/ICQ, Microsoft (MSN) e Yahoo. Ciò consente di autorizzare il traffico IM e di bloccare il trasferimento di allegati inviati dai client IM.

Allegati dei programmi di messaggistica immediata è un gruppo di protocolli che include definizioni per molteplici client IM. Se si attiva la gestione di questi allegati, questi protocolli vengono visualizzati nell'elenco dei protocolli di tutti i filtri di protocollo attivi e nella pagina Modifica protocolli.

Il filtraggio degli allegati IM può essere applicato sia al traffico interno che esterno. Per consentire l'applicazione di un filtraggio interno, definire la parte della propria rete da monitorare usando le opzioni della pagina **Impostazioni** > **Network Agent** > **Globale** (vedere *Configurazione delle impostazioni globali*, pagina 352).

Azioni di filtraggio

I filtri di categoria e di protocollo assegnano un'**azione** ad ogni categoria e ad ogni protocollo. Il software di filtraggio Websense svolge queste azioni in risposta a una richiesta di accesso a Internet da parte di un client. Le azioni applicabili sia a categorie che a protocolli sono:

- Blocco della richiesta Gli utenti ricevono una pagina o un messaggio di blocco e non saranno in grado di accedere al sito o di usare un'applicazione disponibile in Internet.
- Autorizzazione della richiesta Gli utenti possono accedere al sito o possono usare l'applicazione disponibile in Internet.
- Valutazione dell'uso della Larghezza di banda effettuata prima di bloccare o autorizzare la richiesta. Se si attiva questa azione, e l'uso della larghezza di banda raggiunge una determinata soglia, le successive richieste di accesso a Internet relative a una determinata categoria o protocollo verranno bloccate. Vedere Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195.

Sono disponibili altre azioni che possono tuttavia venire applicate soltanto alle categorie.



Nota

Le opzioni Conferma e Assegna non possono venire utilizzate se i singoli client (utenti, gruppi e computer) sono gestiti da Policy Server.

Le informazioni sui tempi, associate a queste funzioni, non vengono condivise dai Policy Server e i client a cui si riferiscono possono ricevere un permesso di accesso a Internet più o meno limitato rispetto alla loro richiesta.

 Conferma — Gli utenti ricevono una pagina di blocco che chiede loro di confermare che l'accesso al sito è motivato da obiettivi di lavoro. Se un utente fa clic su Continua, gli verrà concesso di accedere al sito.

Facendo clic su Continua si avvia un timer. Durante il periodo di tempo configurato (impostazione predefinita: 60 secondi), l'utente può visitare altri siti che fanno parte delle categorie incluse nell'opzione Conferma, senza che vengano visualizzate altre pagine di blocco. Al termine del periodo di tempo definito, la navigazione a qualsiasi altro sito incluso nell'opzione Conferma, comporta la visualizzazione della pagina di blocco.

È possibile modificare il periodo di tempo predefinito usando le opzioni della pagina **Impostazioni > Filtri**.

 Assegna — Gli utenti ricevono una pagina di blocco che richiede loro se intendono utilizzare un tempo assegnato per visualizzare il sito. Se un utente fa clic su Utilizza tempo assegnato, gli verrà concesso l'accesso al sito.

Se si fa clic su Utilizza tempo assegnato, vengono avviati due timer: un timer per la sessione assegnata e un timer per l'allocazione totale assegnata.

- Se l'utente richiede l'assegnazione di altri siti durante una **sessione** con un tempo predefinito (10 minuti), potrà visitare questi siti senza ricevere altre pagine di blocco.
- **Tempo** assegnato totale viene allocato giornalmente. Una volta raggiunto il massimo uso, ogni client dovrà attendere fino al giorno successivo prima di poter accedere ai siti inclusi nelle categorie assegnate. L'allocazione predefinita e assegnata giornalmente (impostazione predefinita: 60 minuti), va impostata

nella pagina **Impostazioni > Filtri**. L'allocazione può anche venire assegnata individualmente a determinati client. Per ulteriori informazioni, vedere *Utilizzo del tempo assegnato per limitare l'accesso a Internet*, pagina 46.

- Blocca per parole chiave—Se si definiscono parole chiave e si attiva di blocco in base a parole chiave, agli utenti che richiedono l'accesso a un sito il cui URL contiene una parola chiave bloccata non potranno accedere al sito richiesto. Vedere *Filtro basato su parole chiave*, pagina 184.
- Blocca per tipi di file Se la funzione di blocco in base al tipo di file è attiva, gli utenti che tentano di scaricare un file il cui tipo è bloccato, ricevono una pagina di blocco e il file non potrà essere scaricato. Vedere *Gestione del traffico in base al tipo di file*, pagina 197.

Utilizzo del tempo assegnato per limitare l'accesso a Internet

Se un utente fa clic su Utilizza tempo assegnato, gli verrà concesso l'accesso ai siti di qualsiasi categoria assegnata fino al termine della sessione assegnata. Il tempo di sessione assegnato e predefinito (configurato tramite la pagina **Impostazioni > Filtri**) è di 10 minuti.

Nota

L'opzione Assegna non può venire utilizzata se i singoli client sono gestiti da molteplici Policy Server.

Le informazioni sui tempi, associate a questa funzione, non vengono condivise dai Policy Server e i client a cui si riferiscono potrebbero ricevere un permesso di accesso a Internet più o meno limitato del previsto.

Al termine della sessione assegnata, la richiesta di un sito assegnato genera la visualizzazione di un altro messaggio di blocco dell'assegnazione. Gli utenti che non hanno consumato la loro allocazione giornaliera, possono avviare una nuova sessione assegnata.

Una volta configurato il tempo assegnato, il software Websense utilizza un elenco prioritario per determinare la risposta da dare quando un utente richiede l'accesso a un sito che fa parte di una categoria assegnata. Il software cerca il tempo assegnato che era stato configurato per:

- 1. l'utente
- 2. il computer o il client collegato in rete
- 3. i gruppi a cui appartiene l'utente

Se un utente fa parte di diversi gruppi, il software Websense assegna un tempo in base all'impostazione di **Utilizzare blocchi più restrittivi** della pagina **Impostazioni > Filtri** (vedere *Configurazione delle impostazioni di filtraggio di Websense*, pagina 57).

4. Tempo assegnato predefinito

Gli applets, come ad esempio gli applet Java o Flash, potrebbero non rispondere come previsto alle restrizioni del tempo assegnato. Anche se si accede ad un applet da un sito con restrizioni di tempo assegnato, l'applet in esecuzione nel browser può continuare la sua esecuzione oltre il tempo assegnato per la sessione.

Ciò è dovuto al fatto che questi applet vengono scaricati completamente nel computer client e vengono eseguiti come vere e proprie applicazioni, senza necessità di comunicare con il server host d'origine. Se tuttavia l'utente fa clic sul pulsante Aggiorna, il software Websense rileva la comunicazione in corso con il server host e blocca la richiesta in base alla restrizioni definite per l'assegnazione applicata.

Accesso con password

La funzione di Accesso con password consente agli utenti in possesso di una password valida di accedere ai siti bloccati dal software Websense. È possibile assegnare un accesso con password a singoli client (utenti, gruppi, computer o reti).

Se l'opzione dell'accesso con password è attiva, i messaggi di blocco di Websense includono un campo per la password. I client che inseriscono una password valida possono accedere ai siti bloccati per un periodo di tempo limitato.



Nota

L'opzione dell'accesso con password non può venire utilizzata se i singoli client sono gestiti da molteplici Policy Server.

Le informazioni sui tempi, associate a questa funzione, non vengono condivise dai Policy Server e i client a cui si riferiscono possono ricevere un permesso di accesso a Internet più o meno limitato rispetto alla loro richiesta.

L'opzione dell'accesso con password viene attivata utilizzando la pagina Impostazioni > Filtri (vedere *Configurazione delle impostazioni di filtraggio di Websense*, pagina 57).

L'accesso con password può venire assegnato a specifici client utilizzando la pagina **Gestione criteri > Clients** (vedere *Aggiunta di un client*, pagina 70 or *Modifiche delle impostazioni per i client*, pagina 72).

Search Filtering

Search Filtering è una funzione offerta da alcuni motori di ricerca che aiutano a limitare il numero di risultati di ricerca inappropriati che vengono visualizzati dall'utente.

I risultati dei motori di ricerca di Internet includono normalmente immagini miniatura associate ai siti che soddisfano i criteri di ricerca definiti. Se queste immagini miniatura sono associate a siti bloccati, il software Websense impedisce agli utenti di accedere al sito completo ma non impedisce al motore di ricerca di visualizzarne l'immagine.

Se si attiva Search Filtering, il software Websense attiva una funzione di motore di ricerca che impedisce la visualizzazione, nei risultati della ricerca, delle immagini miniatura associate ai siti bloccati. L'attivazione di Search Filtering viene applicata al filtraggio effettuato sia sui client locali che remoti.

Websense, Inc., mantiene un database dei motori di ricerca che dispongono della funzione Search Filtering. Se un motore di ricerca viene aggiunto o eliminato dal database, viene visualizzato un messaggio di avvertenza (vedere *Avvisi su schermo*, pagina 292).

Search Filtering viene attivato tramite la pagina **Impostazioni > Filtri**. Per ulteriori informazioni, vedere *Configurazione delle impostazioni di filtraggio di Websense*, pagina 57.

Gestione dei filtri

Argomenti correlati:

- Filtri di categoria e di protocollo, pagina 38
- Criteri di filtraggio dell'uso di Internet, pagina 75
- Creazione di un filtro di categoria, pagina 49
- *Creazione di un filtro di protocollo*, pagina 52
- Creazione di un filtro per restrizioni di accesso, pagina 174

Utilizzare la pagina **Gestione criteri > Filtri** di Websense Manager per visualizzare, creare e modificare i filtri di categoria e di protocollo insieme ad altri strumenti di filtraggio.

La pagina Filtri è suddivisa in 3 sezioni principali:

- I Filtri di categoria determinano le categorie da bloccare o da autorizzare.
- I Filtri di protocollo determinano i protocolli non-HTTP da bloccare o da autorizzare.

Occorre aver installato Network Agent per attivare i filtri di protocollo.

 I Filtri per restrizione di accesso definiscono un elenco di siti Web ad accesso ristretto (vedere *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172).

I filtro di categoria, protocollo e per accesso limitato costituiscono la piattaforma per la definizione dei **criteri**. Ciascun criterio è composto da almeno un filtro di categoria o un filtro per accesso ristretto, e di un filtro di protocollo, applicati a determinati client in base a una pianificazione specifica.

- Per valutare o modificare un filtro di categoria, di protocolla o per accesso limitato, fare clic sul nome del filtro. Per ulteriori informazioni, vedere:
 - *Modifica di un filtro di categoria*, pagina 50
 - Modifica di un filtro di protocollo, pagina 53
 - Modifica di un filtro per restrizioni di accesso, pagina 174
- Per creare un nuovo filtro di categoria, di protocollo o per accesso limitato, fare clic su Aggiungi. Per ulteriori informazioni, vedere:
 - Creazione di un filtro di categoria, pagina 49
 - *Creazione di un filtro di protocollo*, pagina 52
 - Creazione di un filtro per restrizioni di accesso, pagina 174

Per duplicare un filtro esistente, contrassegnare la casella di controllo adiacente al nome del filtro e fare quindi clic su **Copia**. Alla copia viene assegnato il nome del filtro originale più un numero univoco che la contraddistingue, e viene quindi aggiunta all'elenco dei filtri. La copia può venire modificata esattamente come qualsiasi altro filtro.

Se si sono creati ruoli di amministrazione con delega (vedere *Amministrazione con delega*, pagina 241), i Super Administrator possono copiare i filtri da loro creati in altri ruoli in modo che possano venire usati dagli amministratori con delega.

Per copiare dei filtri in un altro ruolo, contrassegnare la casella di controllo adiacente al nome del filtro e fare quindi clic su **Copia nel ruolo**. Per ulteriori informazioni, vedere *Copia di filtri e criteri nei ruoli*, pagina 177.

Creazione di un filtro di categoria

Argomenti correlati:

- Gestione dei filtri, pagina 48
- Modifica di un filtro di categoria, pagina 50

Utilizzare la pagina **Gestione criteri > Filtri > Aggiungi filtro di categoria** pr creare un nuovo filtro di categoria. È possibile usare un modello predefinito oppure fare una copia di un filtro di categoria esistente ed usarlo come base per la definizione del nuovo filtro.

1. Inserire un **Nome filtro** univoco. Il nome deve contenere da 1 a 50 caratteri e non può includere i caratteri seguenti:

* < > { } ~ ! \$ % & @ # . " | \setminus & + = ? / ; : ,

I nomi assegnati ai filtri possono includere spazi, trattini e apostrofi.

2. Inserire una breve **Descrizione** del filtro. Questa descrizione deve apparire accanto al nome del filtro nella sezione Filtri di categoria della pagina Filtri e deve specificare lo scopo del filtro.

Le restrizioni relative ai caratteri usati per il nome dei filtri sono anche applicabili alle descrizioni, con due eccezioni: le descrizioni possono includere punti (.) e virgole (,).

- 3. Selezionare una voce dal menu a discesa per indicare se si vuole usare un modello o la copia di un filtro esistente. Per ulteriori informazioni sui modelli, vedere *Modelli dei filtri di categoria e di protocollo*, pagina 55.
- 4. Per visualizzare e modificare il nuovo filtro, fare clic su **OK**. Il filtro viene aggiunto all'elenco **Filtri di categoria** della pagina Filtri.

Per personalizzare il filtro, fare clic sul nome del filtro e procedere quindi a *Modifica di un filtro di categoria*.

Modifica di un filtro di categoria

Argomenti correlati:

- Filtri di categoria e di protocollo, pagina 38
- Azioni di filtraggio, pagina 44
- Utilizzo del tempo assegnato per limitare l'accesso a Internet, pagina 46
- Accesso con password, pagina 47
- Gestione dei filtri, pagina 48

 \mathbf{P}

• *Gestione delle categorie*, pagina 179

Utilizzare la pagina **Gestione criteri > Filtri > Modifica filtro di categoria** per apportare modifiche ai filtri di categoria esistenti.

Importante

Quando si modifica un filtro di categoria, le modifiche incidono su tutti i criteri che prevedono l'applicazione del filtro.

Ciò non incide tuttavia sui criteri che prevedono l'applicazione di un filtro di categoria con lo stesso nome, ad un altro ruolo di amministrazione con delega.

Il nome e la descrizione del filtro vengono visualizzati nell'area superiore della pagina.

- Fare clic su **Rinomina** per modificare il nome del filtro.
- Per modificare la descrizione del filtro, digitare semplicemente la modifica nel campo **Descrizione**.

Il numero visualizzato accanto a **Criteri che utilizzano questo filtro** indica quanti criteri usano attualmente il filtro selezionato. Se il filtro di categoria è attivo, fare clic

su **Visualizza criteri** per visualizzare l'elenco dei criteri che prevedono l'applicazione del filtro.

L'area inferiore della pagina visualizza un elenco di categorie e le azioni correntemente applicate a ciascuna di esse.

- 1. Selezionare una voce dall'elenco **Categorie** per visualizzare informazioni su una categoria o per modificare l'azione di filtraggio associata alla categoria selezionata.
- 2. Prima di apportare modifiche all'azione applicata a una categoria, utilizzare la sezione **Dettagli categoria** per verificare eventuali attributi associati a quella categoria.
 - Per verificare eventuali URL ricategorizzati o non filtrati assegnati alla categoria, fare clic su Visualizza URL personalizzati in questa categoria. Vedere *Ridefinizione di un filtro per specifici siti*, pagina 186.
 - Per rivedere eventuali parole chiave assegnate alla categoria, fare clic su Visualizza parole chiave personalizzate in questa categoria. Vedere *Filtro* basato su parole chiave, pagina 184.
 - Per rivedere le espressioni regolari usate per definire gli URL o le parole chiave personalizzate per la categoria, fare clic su Visualizza espressioni regolari in questa categoria.
- 3. Utilizzare i pulsanti situati nell'area inferiore dell'elenco delle categorie per modificare l'azione applicata alla categoria selezionata. Per ulteriori informazioni sulle azioni disponibili, vedere *Azioni di filtraggio*, pagina 44.

Gli amministratori con delega non possono modificare l'azione associata alle categorie bloccate da un Super Administrator. Per ulteriori informazioni, vedere *Definizione delle restrizioni di filtraggio per tutti i ruoli*, pagina 271.

- 4. Utilizzare le caselle di controllo a destra dell'elenco delle categorie per applicare azioni di filtraggio alla categoria selezionata:
 - Per modificare il modo in cui le parole chiave vengono utilizzate nel filtraggio della categoria selezionata, selezionare o deselezionate Blocca per parole chiave. *Filtro basato su parole chiave*, pagina 184
 - Per determinare se gli utenti possono accedere ad alcuni tipi di file dai siti inclusi nella categoria selezionata, selezionare o deselezionare Blocca per tipi di file. Vedere *Gestione del traffico in base al tipo di file*, pagina 197.

Se si è scelta l'opzione di bloccare alcuni tipi di file, selezionare i tipi di file da bloccare.

 Per specificare se l'accesso ai siti inclusi in una categoria sia limitato dal raggiungimento di determinate soglie nell'uso della larghezza di banda, selezionare o deselezionare Blocca con Bandwidth Optimizer. Vedere Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195.

Se si è scelto di bloccare l'accesso in base all'uso della larghezza di banda, specificare le soglie di restrizione all'uso.

5. Ripetere le operazioni descritte ai punti da 1 a 3 per modificare le azioni di filtraggio applicate alle altre categorie.

6. Dopo aver modificato il filtro, fare clic su **OK** per inserire le modifiche nella cache e ritornare alla pagina Filtri. Le modifiche non vengono implementare fino a quando non si fa clic su **Salva tutto**.

Per attivare un nuovo filtro di categoria, aggiungerlo a un criterio ed assegnare quindi questo criterio ai client. Vedere *Criteri di filtraggio dell'uso di Internet*, pagina 75.

Creazione di un filtro di protocollo

Argomenti correlati:

- Filtri di categoria e di protocollo, pagina 38
- Azioni di filtraggio, pagina 44
- Modifica di un filtro di protocollo, pagina 53
- *Gestione dei protocolli*, pagina 189

Utilizzare la pagina **Gestione criteri > Filtri > Aggiungi filtro di categoria** per creare un nuovo filtro di categoria. È possibile usare un modello predefinito oppure fare una copia di un filtro di protocollo esistente ed usarlo come base per la definizione del nuovo filtro.

1. Inserire un **Nome filtro** univoco. Il nome deve contenere da 1 a 50 caratteri e non può includere i caratteri seguenti:

* < > { } ~ ! \$ % & @ # . " | \setminus & + = ? / ; : ,

I nomi assegnati ai filtri possono includere spazi, trattini e apostrofi.

2. Inserire una breve **Descrizione** del filtro. Questa descrizione deve apparire accanto al nome del filtro nella sezione Filtri di protocollo della pagina Filtri e deve specificare lo scopo del filtro.

Le restrizioni relative ai caratteri usati per il nome dei filtri è anche applicabile alle descrizioni, con due eccezioni: le descrizioni possono includere punti (.) e virgole (,).

- 3. Selezionare una voce dal menu a discesa per indicare se si vuole utilizzare un modello (vedere *Modelli dei filtri di categoria e di protocollo*, pagina 55) o fare una copia di un filtro esistente da usare come base per il nuovo filtro.
- 4. Per visualizzare e modificare il nuovo filtro, fare clic su **OK**. Il filtro viene aggiunto all'elenco **Filtri di protocollo** della pagina Filtri.

Per terminare la personalizzazione del nuovo filtro, fare clic su *Modifica di un filtro di protocollo*.

Modifica di un filtro di protocollo

Argomenti correlati:

- Filtri di categoria e di protocollo, pagina 38
- *Creazione di un filtro di protocollo*, pagina 52
- Azioni di filtraggio, pagina 44
- Gestione dei protocolli, pagina 189
- Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195

Utilizzare la pagina **Gestione criteri > Filtri > Modifica filtro di protocollo** per apportare modifiche ai filtri di protocollo esistenti.



Importante

Le modifiche apportate incidono su tutti i criteri di imposizione di questo filtro.

Ciò non incide tuttavia sui criteri che prevedono l'applicazione di un filtro di protocollo con lo stesso nome ad un altro ruolo di amministrazione con delega.

Il nome e la descrizione del filtro vengono visualizzati nell'area superiore della pagina.

- Fare clic su **Rinomina** per modificare il nome del filtro.
- Per modificare la descrizione del filtro, digitare semplicemente la modifica nel campo **Descrizione**.

Il numero visualizzato accanto a **Criteri che utilizzano questo filtro** indica quanti criteri usano attualmente il filtro selezionato. Se il filtro di protocollo è attivo, fare clic su **Visualizza criteri** per un elenco dei criteri di imposizione del filtro.

L'area inferiore della pagina visualizza un elenco di protocolli e le azioni correntemente applicate a ciascuno di essi.

Per modificare il modo in cui i protocolli vengono filtrati e registrati nel log:

1. Selezionare un protocollo dall'elenco **Protocolli**. Le azioni di filtraggio avanzate ed applicabili al protocollo selezionato vengono visualizzate a destra dell'elenco.

2. Utilizzare i pulsanti **Autorizza** e **Blocca**, situati nell'area inferiore dell'elenco dei protocolli, per modificare l'azione applicata al protocollo selezionato.



Nota

Il software Websense può bloccare le richieste basate su protocolli TCP, ma non le richieste basate su protocolli UDP.

Alcune applicazioni utilizzano sia messaggi basati sul protocollo TCP che UDP. Se una richiesta da un'applicazione su rete viene inviata via TCP e i dati vengono successivamente inviati via UDP, il software Websense blocca la richiesta TCP iniziale e blocca quindi il successivo traffico UDP.

Le richieste UDP potrebbero venire registrate nel log come bloccate anche se sono di fatto autorizzate.

Per applicare la stessa azione agli altri protocolli del gruppo di protocolli selezionato, fare clic su **Applica a gruppo**.

- 3. Per informazioni sull'uso del protocollo selezionato disponibile per l'invio di avvertenze o la creazione di report, selezionare la casella di controllo **Registra dati protocollo**.
- 4. Per imporre restrizioni sulla larghezza di banda relativamente all'uso di questo protocollo, fare clic su **Blocca con Bandwidth Optimizer** e fornire i valori di soglia definiti per l'uso della larghezza di banda. Per ulteriori informazioni, vedere *Uso di Bandwidth Optimizer per la gestione della larghezza di banda*, pagina 195.
- 5. Dopo aver modificato il filtro, fare clic su **OK** per inserire le modifiche nella cache e ritornare alla pagina Filtri. Le modifiche non vengono implementare fino a quando non si fa clic su **Salva tutto**.

Per attivare un nuovo filtro di protocollo, aggiungerlo a un criterio e assegnare quindi questo criterio ai client (vedere *Criteri di filtraggio dell'uso di Internet*, pagina 75).

Nota

È possibile creare criteri che inizino ad applicare un determinato filtro di protocollo in base a un tempo specifico. Se gli utenti iniziano una sessione basata su un determinato protocollo, prima che il relativo filtro entri in effetto, potranno continuare ad accedere a questo protocollo fino alla fine della sessione in corso, anche se il filtro lo blocca. Una volta che un utente chiude la sessione, le richieste successive per l'uso di quel protocollo verranno bloccate.

Filtri di categoria e di protocollo definiti da Websense

Il software Websense include diversi filtri d'esempio di categoria e di protocollo. È possibile usare questi filtri così come sono oppure modificarli in base a specifiche esigenze di filtraggio. Se non si ha necessità di usare i filtri predefiniti, molti di essi potranno venire eliminati.

I filtri di categoria predefiniti sono:

- Base
- Sicurezza di base
- Salva tutto
- Predefinito
- Solo monitoraggio
- Autorizza sempre

I filtri di categoria Blocca sempre e Autorizza sempre non vengono inclusi nell'elenco riportato nella pagina Filtri, sebbene possano venire aggiunti ai criteri. Questi filtri giocano un ruolo di filtraggio particolare e non possono venire eliminati o modificati. Quando una richiesta di accesso a Internet viene filtrata, il software Websense verifica per prima cosa se i filtri Blocca sempre e Autorizza sempre sono applicabili, prima di eseguire ulteriori controlli di filtraggio (vedere *Filtraggio di un sito*, pagina 83).

I filtri di protocollo predefiniti sono:

- Sicurezza di base
- Predefinito
- Solo monitoraggio
- Autorizza sempre

Il filtro di protocollo Autorizza sempre, come il suo filtro di categoria equivalente, non viene incluso nella pagina Filtri e non può quindi venire modificato o eliminato. Assume anche un grado di priorità quando si esegue il filtraggio.

I filtri di categoria e di protocollo predefiniti possono essere modificati ma non possono venire eliminati. In situazioni di aggiornamento, se ci sono aree scoperte nei criteri predefiniti, i filtri predefiniti vengono utilizzati per filtrare richieste per le quali non esistono criteri applicabili.

Modelli dei filtri di categoria e di protocollo

Se si crea un nuovo filtro di categoria o di protocollo, si può iniziare facendo una copia di un filtro disponibile nella pagina Filtri, selezionare un filtro esistente come un modello dalla pagina Aggiungi filtro, oppure usare un **modello** per filtri.

Il software Websense include 5 modelli di filtro di categoria.

- Solo monitoraggio e Autorizza sempre concede un permesso di accesso a tutte le categorie.
- Blocca sempre blocca tutte le categorie.

- Base blocca le categorie bloccate più di frequente e autorizza le altre.
- **Predefinito** applica alle categorie le azioni Blocca, Autorizza, Continua e Assegna.
- Ad esempio Sicurezza di base blocca soltanto le categorie predefinite nella classe Rischio di sicurezza (vedere *Classi di rischio*, pagina 41).

Il software Websense include 3 modelli di filtri di protocollo:

- Solo monitoraggio e Autorizza sempre concede un permesso di accesso a tutti i protocolli.
- Sicurezza di base blocca i protocolli Scambio di file Peer-to-Peer e Elusione via Proxy nonché i protocolli relativi ad allegati di messaggistica immediata (se inclusa come opzione) e di traffico dannoso (Websense Web Security).
- Predefinito blocca i protocolli relativi alla messaggistica e alle Chat, allo scambio di file Peer-to-Peer, a Elusione via Proxy nonché agli allegati della messaggistica (se acquistata come opzione) e quelli relativi a un traffico dannoso (Websense Web Security).

Sebbene sia possibile modificare o eliminare la maggior parte dei filtri di categoria e di protocollo, non è possibile modificare o eliminare i modelli. Analogamente, sebbene si possano creare tanti filtri personalizzati quanti necessari, non è possibile creare nuovi modelli.

Poiché i modelli non possono venire modificati, offrono un metodo costante di riferimento retrospettivo verso le azioni di filtraggio originali applicate ai filtri definiti da Websense. Ad esempio, i modelli del filtro di categoria e del filtro di protocollo Normale, applicano le stesse azioni previste dai filtri originali predefiniti di categoria e di protocollo. Ciò significa che è sempre possibile ripristinare la configurazione di filtraggio Websense originale tramite la creazione di filtri che utilizzano modelli predefiniti.

Per informazioni sull'uso di un modello per la creazione di un nuovo filtro, vedere *Creazione di un filtro di categoria*, pagina 49 o *Creazione di un filtro di protocollo*, pagina 52.

Configurazione delle impostazioni di filtraggio di Websense

Argomenti correlati:

- Filtri di categoria e di protocollo, pagina 38
- Client, pagina 61
- *Pagine di blocco*, pagina 87
- Azioni di filtraggio, pagina 44
- Accesso con password, pagina 47
- Ordine di filtraggio, pagina 82
- Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195
- Filtro basato su parole chiave, pagina 184

Utilizzare la pagina **Impostazioni > Filtri** per definire le impostazioni di base di una serie di funzioni di filtraggio.

In **Bandwidth Optimizer**, inserire le informazioni necessarie a filtrare l'uso di Internet in base alla larghezza di banda disponibile. Per ulteriori informazioni sul filtraggio basato sulla larghezza di banda, vedere *Uso di Bandwidth Optimizer per la gestione della larghezza di banda*, pagina 195.

- 1. Per specificare una Velocità di connessione a Internet, eseguire una delle operazioni seguenti:
 - Selezionare una velocità standard dal menu a discesa.
 - Inserire la velocità di rete in kilobit per secondo nell'apposito campo di testo.
- 2. Utilizzare il campo **Larghezza di banda predefinita per la rete** per inserire una soglia predefinita (valore percentuale del traffico di rete totale) da usare quando il filtraggio della larghezza di banda della rete è attivo.
- 3. Utilizzare il campo Larghezza di banda predefinita per ciascun protocollo per inserire una soglia predefinita da usare quando il filtraggio della larghezza di banda del protocollo è attivo.

Usare la sezione **Filtri generici** per determinare come filtrare gli utenti nel caso siano loro applicabili molteplici criteri, per specificare opzioni di ricerca di parole chiave e per definire l'accesso con password, la funzione di continua e di sessione assegnata.

 Per determinare come filtrare gli utenti nel caso siano loro applicabili molteplici criteri, selezionare o deselezionare Utilizza i criteri di gruppo più restrittivi (vedere Ordine di filtraggio, pagina 82).

- Se questa opzione è selezionata, vengono applicati i criteri con le impostazioni di filtraggio più restrittive. Ossia, se dei criteri applicabili bloccano l'accesso a una categoria ed altri lo permettono, la richiesta dell'utente per l'accesso a un sito di questa categoria viene bloccata.
- Se l'opzione non è stata selezionata, vengono applicate le impostazioni più permissive.
- 2. Selezionare una delle seguenti **Opzioni di ricerca per parole chiave** (vedere *Filtro basato su parole chiave*, pagina 184).

Solo CGI	Blocca i siti quando delle parole chiave appaiono nelle stringhe di query CGI (dopo il "?" di un indirizzo Web) Esempio: it. search.yahoo.com/search?p=test Il software Websense non cerca parole chiave prima di "?" quando questa opzione è selezionata.
Solo URL	Blocca i siti i cui URL includono le parole chiave. Se l'indirizzo richiesto contiene una stringa di query CGI, il software Websense cerca parole chiave fino a quando non incontra "?".
URL e CGI	Blocca i siti i cui indirizzi includono in un punto qualunque una parola chiave. Nel caso di una stringa di query CGI, il software Websense cerca parole chiave in una posizione sia precedente sia successiva a "?".
Disabilita blocco per parole chiave	Usare questa opzione con cautela. Disabilita blocco per parole chiave disattiva il blocco in base alle parole chiave anche se Blocca per parole chiave è selezionato in un filtro di categoria.

- 3. Inserire nel campo **Timeout accesso con password** il numero massimo di secondi (fino a 3600, impostazione predefinita: 60) che un utente può usare per un accesso ai siti di tutte le categorie dopo aver selezionato l'opzione di accesso con la password (vedere *Accesso con password*, pagina 47).
- 4. Inserire nel campo **Timeout continuo**, il numero massimo di secondi (fino a 3600, impostazione predefinita: 60) che un utente, dopo aver fatto clic su Continua, può usare per accedere ai siti di tutte le categorie soggette all'azione di Conferma (vedere *Azioni di filtraggio*, pagina 44).
- 5. Inserire nel campo **Lunghezza sessione assegnata** l'intervallo (fino a 60 minuti, impostazione predefinita: 10) durante il quale un utente può visitare dei siti che fanno parte di categorie limitate da un'assegnazione (vedere *Utilizzo del tempo assegnato per limitare l'accesso a Internet*, pagina 46).

Una sessione inizia quando l'utente fa clic sul pulsante Utilizza tempo assegnato.

6. Inserire **Tempo assegnato predefinito giornaliero** (fino a 240 minuti, impostazione predefinita: 60) per tutti gli utenti.

Per modificare l'assegnazione del tempo per singoli utenti, andare alla pagina **Criteri > Client**.

Mano a mano che si modifica la lunghezza della sessione e dei tempi assegnati, predefiniti e giornalieri, le **Sessioni assegnate predefinite giornaliere** vengono calcolate e visualizzate.

Utilizzare la sessione **Messaggi di blocco** per inserire l'URL o il percorso alle pagine HTML alternative di blocco create per il frame superiore dei messaggi di blocco browser-based (vedere *Creazione di messaggi di blocco alternativi*, pagina 94).

- Si possono usare pagine distinte per i vari protocolli. FTP, HTTP (tra cui HTTPS) e Gopher.
- Lasciare vuoti questi campi se si vuole utilizzare il messaggio di blocco predefinito dal software Websense o una versione personalizzata del messaggio (vedere *Personalizzazione dei messaggi di blocco*, pagina 90).

In **Filtri di ricerca**, selezionare **Abilita filtri di ricerca** affinché il software Websense attivi un'impostazione incorporata in alcuni motori di ricerca che impedisce la visualizzazione, nei risultati di una ricerca, di immagini miniatura e di altri espliciti contenuti associati a siti bloccati (vedere *Search Filtering*, pagina 47).

I motori di ricerca che supportano questa funzione sono indicati nell'area inferiore della sezione.

Una volta terminata la configurazione delle impostazioni di Filtri, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementare fino a quando non si fa clic su **Salva tutto**.

Client

È possibile personalizzare il modo in cui il software Websense filtra le richieste inoltrate da specifici utenti o computer aggiungendo questi ultimi ai **client** di Websense Manager. I client possono essere costituiti da:

- Computer Computer collegati in rete e definiti da un indirizzo IP specifico.
- Rete Gruppi di computer, definiti collettivamente come un range di indirizzi IP.
- Utenti Account di utenti, gruppi o domini in un servizio di directory supportato.

Inizialmente, il software Websense filtra tutti i client nello stesso modo, usando il criterio **Predefinito** (vedere *Criterio Predefinito*, pagina 76). Dopo aver aggiunto un client alla pagina Client di Websense Manager, è possibile assegnare a quel client un criterio di filtraggio specifico.

Nel caso in cui si possano applicare molteplici criteri , come ad esempio all'utente viene assegnato un criterio e al computer viene assegnato un altro criterio, il software Websense determina nel modo seguente il criterio da applicare:

- 1. Applica il criterio assegnato all'**utente** che ha inoltrato la richiesta. Se, al momento della richiesta, quel criterio non ha filtri attivi, utilizza il criterio applicabile successivo.
- 2. Se non esistono criteri specifici per l'utente o se i criteri non hanno filtri attivi al momento della richiesta, il software Websense cerca prima il criterio assegnato al **computer** oppure alla **rete** da cui è stata inoltrata la richiesta.
- 3. Se, al momento della richiesta, non esistono criteri specifici per il computer o per la rete o se i criteri non hanno filtri attivi, il software Websense cerca il criterio assegnato al **gruppo** a cui l'utente appartiene. Se l'utente appartiene a più di un gruppo, il software Websense considera tutti i criteri dei gruppi interessati (vedere *Ordine di filtraggio*, pagina 82).
- 4. Se non esiste un criterio assegnato ai gruppi interessati, il software Websense cerca il criterio assegnato al **dominio** dell'utente (OU).
- 5. Se non trova un criterio applicabile, oppure se, al momento della richiesta, il criterio non dispone di un filtro di categoria, applica il criterio **Predefinito** associato al ruolo a cui il client è stato assegnato.

Per ulteriori informazioni su come il software Websense applica i criteri di filtraggio ai client, vedere *Filtraggio di un sito*, pagina 83.

Gestione dei client

Argomenti correlati:

- *Client*, pagina 61
- Gestione di computer e reti, pagina 63
- Gestione di utenti e gruppi, pagina 64
- Aggiunta di un client, pagina 70
- Modifiche delle impostazioni per i client, pagina 72

Utilizzare la pagina **Gestione criteri** > **Client** per visualizzare le informazioni sui client esistenti, per aggiungere, modificare o eliminare i client, oppure per spostare i client a un ruolo di amministrazione con delega.

Se l'utente con funzioni di amministratore con delega vuole visualizzare i client nella pagina Client, deve aggiungerli all'elenco da lui gestito. Per istruzioni, vedere *Aggiunta di un client*, pagina 70,.

I client sono suddivisi in 3 gruppi:

- **Directory** che include utenti, gruppi e domini dal proprio servizio di directory (vedere *Gestione di utenti e gruppi*, pagina 64).
- Rete che include i range di indirizzi IP nell'ambito della rete filtrata che possono venire regolamentati da un unico criterio (vedere *Gestione di computer e reti*, pagina 63).
- **Computer** che include singoli computer della rete filtrata, identificati da un indirizzo IP (vedere *Gestione di computer e reti*, pagina 63).

Fare clic sul segno (+) accanto al tipo di client per visualizzare un elenco di client esistenti dello stesso tipo. Ciascun elenco di client include:

- Il nome, l'indirizzo IP o il range di indirizzi IP di quel client.
- Il **criterio** assegnato attualmente al client. Il criterio **Predefinito** viene utilizzato fino a quando non si assegna un altro criterio (vedere *Criteri di filtraggio dell'uso di Internet*, pagina 75).
- Se il client può usare l'**accesso password** che gli consente di visualizzare i siti bloccati (vedere *Accesso con password*, pagina 47).
- Se il client ha un **tempo assegnato** personalizzato che gli è stato allocato (vedere *Utilizzo del tempo assegnato per limitare l'accesso a Internet*, pagina 46).

Per trovare un client specifico, navigare lungo l'apposito nodo dell'albero.

Per modificare le impostazioni relative ai criteri, accesso con password, tempo assegnato e autenticazione, selezionare uno o più client dall'elenco e fare quindi clic su **Modifica**. Per ulteriori informazioni, vedere *Modifiche delle impostazioni per i client*, pagina 72,.

Per aggiungere un client o per applicare determinati criteri a un client gestito che non è incluso attualmente nella pagina dei Client, fare clic su **Aggiungi**. Per ulteriori informazioni, andare a *Aggiunta di un client*, pagina 70,.

Se si sono creati ruoli di amministrazione con delega (vedere *Amministrazione con delega*, pagina 241), i Super Administrator possono spostare i loro client ad altri ruoli. Selezionare, per prima cosa, la casella di controllo accanto alla voce del client da spostare e fare quindi clic su **Passa al ruolo**. Se un client viene spostato a un ruolo di amministratore con delega, i criteri e i filtri ad esso applicati vengono copiati nel ruolo. Per ulteriori informazioni, vedere *Spostamento dei client a ruoli diversi*, pagina 72,.

Se si è configurato il software Websense in modo che comunichi con un servizio di directory LDPA-based, il pulsante **Gestisci gruppi LDAP personalizzati** viene visualizzato nella barra degli strumenti, nell'area superiore della pagina. Fare clic su questo pulsante per aggiungere o per modificare i gruppi in base all'attributo LDAP (vedere *Gestione di gruppi LDAP personalizzati*, pagina 68).

Per eliminare un client da Websense Manager, selezionarlo e fare clic su Elimina.

Gestione di computer e reti

Argomenti correlati:

- *Gestione dei client*, pagina 62
- Gestione di utenti e gruppi, pagina 64
- Aggiunta di un client, pagina 70
- Assegnazione dei criteri ai client, pagina 81

In Websense Manager, il **computer** è rappresentato da un indirizzo IP (ad esempio, 10.201.3.1) associato a un computer filtrato. La **rete** è rappresentata da un range di indirizzi IP (ad esempio, 10.201.3.2 - 10.201.3.44) associato a un gruppo di computer filtrati.

È possibile assegnare dei criteri ai client costituiti da computer o reti come si farebbe con i client costituiti da utenti, gruppi o domini.

- Si può ad esempio assegnare ad un computer un criterio in base al quale gli utenti possono collegarsi senza dover inserire dati di accesso o possono accedere al computer tramite un account "ospite".
- Si può assegnare un criterio alla **rete** in modo che quel criterio di filtraggio venga applicato simultaneamente a diversi computer.

Se si assegna un criterio a un computer o a una rete, questo criterio verrà applicato indipendentemente dall'utente collegato al computer filtrato, **a meno che** non si sia assegnato un particolare criterio all'utente collegato. I criteri assegnati al computer o

alla rete hanno priorità rispetto a qualsiasi altro tipo di criteri **di gruppo** eventualmente applicati all'utente.

Gestione di utenti e gruppi

Argomenti correlati:

- *Gestione dei client*, pagina 62
- Servizi di directory, pagina 65
- Gestione di gruppi LDAP personalizzati, pagina 68
- Gestione di computer e reti, pagina 63
- *Aggiunta di un client*, pagina 70
- Assegnazione dei criteri ai client, pagina 81

Al fine di applicare criteri a singoli utenti e gruppi collegati in rete, occorre configurare il software Websense in modo che si possa accedere al servizio di directory per ottenere informazioni sugli oggetti di directory (utente, gruppo, dominio o unità organizzativa).

Il software Websense è in grado di comunicare con NT Directory / Active Directory di Windows (Mixed Mode) mentre comunica con Active Directory di Windows, eDirectory di Novell e Java System Directory di Sun con accesso tramite Lightweight Directory Access Protocol (LDAP)

Nota

Se si utilizza un servizio di directory LDAP-based, i nomi utenti duplicati non sono supportati. Verificare che lo stesso nome utente non appaia in molteplici domini.

Se si sta inoltre utilizzando Active Directory di Windows oppure Java System Directory di Sun, i nomi utenti senza password non sono supportati. Accertare che a tutti gli utenti sia stata assegnata una password.

User Service di Websense inoltra informazioni dal servizio di directory a Policy Server e a Filtering Service, da usare per l'applicazione dei criteri di filtraggio.

Websense, Inc., consiglia di installare iUser Service in un computer dotato del sistema operativo Windows (anche se può risiedere in un computer Linux). Normalmente questo è il computer in cui è installato Policy Server.

Per configurare il software Websense in modo che comunichi con il servizio di directory, vedere *Servizi di directory*.

Servizi di directory

Il servizio di directory è uno strumento che archivia informazioni sugli utenti e sulle risorse di una rete. Prima di poter aggiungere client (utenti, gruppi, domini o unità organizzative) a Websense Manager, occorre configurare il software Websense in modo che si possano reperire le informazioni necessarie dal servizio di directory.

Utilizzare la pagina **Impostazioni > Servizi di directory** per identificare il servizio di directory utilizzato nella rete. È possibile configurare le impostazioni per un solo tipo di servizio di directory per ogni Policy Service.

Selezionare prima di tutto un servizio di directory dall'elenco delle Directory. La selezione eseguita determina le impostazioni che verranno visualizzate nella pagina.

Per istruzioni sulla configurazione, andare alla sezione rilevante:

- NT Directory / Active Directory di Windows (Mixed Mode), pagina 65
- Active Directory di Windows (modalità nativa), pagina 65
- *eDirectory di Novell e Directory di Java System di Sun*, pagina 67

NT Directory / Active Directory di Windows (Mixed Mode)

Se il proprio servizio di directory è NT Directory o Active Directory di Windows (Mixed Mode), non è necessario eseguire un'ulteriore configurazione.

Nel caso raro in cui si utilizzi un altro servizio di directory, potrebbe essere necessario inserire ulteriori informazioni in questa schermata. Ciò si verifica soltanto se:

- si sta usando DC Agent ai fini di un'identificazione trasparente (vedere *DC Agent*, pagina 217)
- User Service è in esecuzione in un computer Linux

Se l'installazione usa questa configurazione, fornire le credenziali amministrative nell'elenco disponibile in NT Directory / Active Directory di Windows (Mixed Mode). Se l'installazione non utilizza questa configurazione, i campi delle credenziali amministrative appaiono inattivi.

Active Directory di Windows (modalità nativa)

Active Directory di Windows archivia le informazioni utente in uno o più *cataloghi globali*. Il catalogo globale consente ad individui ed applicazioni di trovare gli oggetti necessari (utenti, gruppi e così via) in un dominio Active Directory.

Affinché il software Websense possa comunicare con Active Directory in modalità nativa, occorre fornire informazioni sui server di catalogo globale collegati in rete.

- 1. Fare clic su **Aggiungi**, accanto all'elenco dei server di catalogo globale. Viene visualizzata la pagina Aggiungi server di catalogo globale.
- 2. Utilizzare il campo **IP o nome del server** per identificare il server di catalogo globale:

- se si dispone di molteplici server di catalogo globale configurati per il failover, inserire il nome di dominio DNS.
- se i server di catalogo globale non sono configurati per il failover, inserire l'indirizzo IP o il nome dell'host (se la risoluzione dei nomi è disattiva nella rete) del server da aggiungere.
- 3. Inserire la **Porta** che il software Websense deve utilizzare per comunicare con il catalogo globale (impostazione predefinita: **3268**).
- 4. A titolo facoltativo, inserire il **Contesto radice** che il software Websense deve utilizzare per cercare informazioni sull'utente. Se si inserisce un valore, questo deve costituire un contesto valido nel dominio.
 - Se si è specificata una porta di comunicazione 3260 o 3269, non è necessario inserire un contesto radice.
 - Se la porta specificata è 389 o 636, occorre inserire un contesto radice.
 - Se si lascia vuoto il campo Contesto radice, il software Websense inizia la ricerca a partire dal livello superiore del servizio di directory.

Nota

Evitare che lo stesso nome utente appaia in molteplici domini. Se il software Websense trova nomi di account duplicati per uno stesso utente, l'utente non potrà essere identificato in modo trasparente.

5. Specificare l'account amministrativo che il software Websense deve utilizzare per reperire, dal servizio di directory, le informazioni necessarie su nome utente e percorso. Questo account deve essere in grado di condurre una query dal servizio di directory, ma non deve necessariamente essere in grado di apportare modifiche al servizio di directory o essere un amministratore di dominio.

Selezionare **Nome distinto dai componenti** oppure **Nome distinto completo** per specificare come si vogliono inserire le informazioni di account.

 Se si è selezionato Nome distinto dai componenti, inserire Nome visualizzato, Password dell'account, Cartella account e Nome dominio DNS per l'account amministrativo. Utilizzare la forma di nome comune (cn) per il nome utente dell'account amministrativo, non usare l'ID utente (uid).

Nota

Il campo **Cartella account** non supporta valori con il tag di unità organizzativa (ou), (ad esempio, ou=Finanza). Se il proprio nome per l'account amministrativo contiene il tag "ou", inserire il nome distinto completo per l'account amministrativo.

- Se si è selezionato un Nome distinto completo, inserirlo come un'unica stringa nel campo Nome distinto utente (ad esempio, *cn=Admin, cn=Users, ou=InfoSystems, dc=company, dc=net*), e inserire quindi la Password definita per l'account.
- 6. Fare clic su OK.

- 7. Ripetere la procedura descritta sopra per ciascun server di catalogo globale.
- 8. Fare clic su **Impostazioni directory avanzate** e procedere quindi a *Impostazioni directory avanzate*, pagina 67.

eDirectory di Novell e Directory di Java System di Sun

Per reperire informazioni dal servizio di directory, il software Websense richiede il nome distinto completo, il contesto radice e la password di accesso agli account utente con privilegi amministrativi.

- 1. Inserire l'indirizzo IP del computer con il server directory nel campo IP del server.
- 2. Inserire il numero di **Porta** che il software Websense userà per comunicare con la directory. Il valore predefinito è 389.
- 3. Se la directory necessita di specifici privilegi amministrativi per un accesso di sola lettura, inserire il **Nome distinto amministratore** e la **Password**.
- 4. A titolo facoltativo, inserire il **Contesto radice** che il software Websense deve utilizzare per cercare informazioni sull'utente. Ad esempio, *o=domain.com*.

Se si riduce l'ambito del contesto, si ottiene una maggiore velocità ed efficienza di reperimento delle informazioni.



Nota

Evitare che lo stesso nome utente appaia in molteplici domini. Se il software Websense trova nomi di account duplicati per uno stesso utente, l'utente non potrà essere identificato.

5. Fare clic su **Impostazioni directory avanzate** e procedere quindi a *Impostazioni directory avanzate*, pagina 67.

Impostazioni directory avanzate

Argomenti correlati:

- Active Directory di Windows (modalità nativa), pagina 65
- eDirectory di Novell e Directory di Java System di Sun, pagina 67

Queste impostazioni possono venire utilizzate per definire:

- il metodo con cui il software Websense deve condurre la ricerca nel servizio directory per reperire le informazioni necessarie su utenti, gruppi e domini
- se il software Websense deve utilizzare un collegamento cifrato per comunicare con il servizio di directory
- quale set di caratteri deve usare il software Websense per codificare le informazioni LDAP

Configurare queste impostazioni come necessario, per ogni servizio di directory LDPA-based.

- 1. Se si utilizzano tipi di classe di oggetti personalizzati (nomi attributi) nel servizio di directory, selezionare **Utilizza filtri personalizzati**. Le stringhe predefinite del filtro vengono visualizzate nei campi Filtri.
- 2. Modificare le stringhe dei filtri esistenti, sostituendo i tipi di classe oggetti specifici della propria directory. Ad esempio, se la propria directory utilizza il tipo di classe oggetti **dept** anziché **ou** (unità organizzativa), inserire un nuovo valore nel campo Filtro di ricerca dominio.

Gli attributi sono sempre stringhe utilizzate nella ricerca all'interno del servizio di directory. I filtri personalizzati offrono le funzioni descritte qui di seguito.

- Filtro di ricerca utente determina come User Service deve cercare gli utenti.
- Filtro di ricerca gruppo determina come User Service deve cercare i gruppi.
- Filtro di ricerca dominio determina come User Service deve cercare i domini e le unità organizzative.
- Filtro di ricerca gruppo utente determina come User Service associa gli utenti ai gruppi.
- 3. Per garantire la comunicazione tra il software Websense e il servizio di directory, selezionare Utilizza SSL.
- 4. Per determinare il set di caratteri che il software Websense deve utilizzare per codificare le informazioni LDAP, selezionare **UTF-8** o **MBCS**.

MBCS, o set di caratteri multibyte, viene normalmente usato per codificare le lingue asiatiche, come ad esempio, cinese, giapponese e coreano.

5. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Gestione di gruppi LDAP personalizzati

Argomenti correlati:

- *Gestione di utenti e gruppi*, pagina 64
- Servizi di directory, pagina 65
- Aggiunta o modifica di un gruppo LDAP personalizzato, pagina 69

Utilizzare la pagina **Gestisci gruppi LDAP personalizzati** per gestire i gruppi personalizzati basati su attributi definiti nel proprio servizio di directory. Questa

opzione è disponibile soltanto se si è configurato il software Websense per la comunicazione con un servizio directory LDAP-based.



Importante

Se si aggiungono gruppi LDAP personalizzati a Websense Manager, le definizioni dei gruppi vengono archiviate nel Policy Server attivo e non incidono su altre istanze del Policy Server. Per aggiungere gruppi LDAP personalizzati a molteplici Policy Server, utilizzare Websense Manager per accedere ad ogni Policy Server ed inserire quindi le informazioni necessarie.

Se si aggiungono dei gruppi LDAP personalizzati e si modificano quindi i servizi di directory o si modifica il percorso del server di directory, i gruppi esistenti perdono la loro validità. Occorrerà aggiungere nuovamente i gruppi e quindi definire ciascuno di essi come un client.

- Per aggiungere un gruppo, fare clic su Aggiungi (vedere Aggiunta o modifica di un gruppo LDAP personalizzato, pagina 69).
- Per modificare una voce dell'elenco, fare clic sul nome del suo gruppo (vedere Aggiunta o modifica di un gruppo LDAP personalizzato).
- Per eliminare una voce, selezionarla e fare quindi clic su Elimina.

Una volta completate le modifiche dei gruppi LDAP personalizzati, fare clic su OK per inserire le modifiche nella cache e ritornare alla pagina precedente. Le modifiche non vengono implementate fino a quando non si fa clic su Salva tutto.

Aggiunta o modifica di un gruppo LDAP personalizzato

Utilizzare la pagina Aggiungi gruppo LDAP personalizzato per definire un gruppo in Websense Manager in base agli attributi definiti nel servizio di directory. Utilizzare la pagina Modifica gruppo LDAP personalizzato per apportare modifiche a una definizione esistente.

Importante

Se si aggiungono dei gruppi LDAP personalizzati e si modificano quindi i servizi di directory o si modifica il percorso del server di directory, i gruppi esistenti perdono la loro validità. Occorre aggiungere nuovamente i gruppi e quindi definire ciascuno di essi come un client.

1. Inserire o modificare il Nome gruppo. Utilizzare un nome descrittivo che indichi chiaramente lo scopo del gruppo LDAP.

I nomi dei gruppi rispettano maiuscole e minuscole e devono essere univoci.

2. Inserire o modificare la descrizione che definisce questo gruppo nel proprio servizio di directory. Ad esempio:

(WorkStatus=parttime)

In questo esempio, **WorkStatus** è un attributo utente che indica lo stato di impiego a tempo pieno e **partime** è un valore che indica che l'utente è un dipendente a metà tempo.

- 3. Fare clic su **OK** per ritornare alla pagina Gestisci gruppi LDAP personalizzati. La voce nuova o modificata viene visualizzata nell'elenco.
- 4. Aggiungere o modificare un'altra voce o fare clic su **OK** per inserire le modifiche nella cache e ritornare alla pagina precedente. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta di un client

Argomenti correlati:

- *Gestione dei client*, pagina 62
- Gestione di computer e reti, pagina 63
- Gestione di utenti e gruppi, pagina 64
- *Ricerca nel service di directory*, pagina 71
- Modifiche delle impostazioni per i client, pagina 72

Utilizzare la pagina **Gestione criteri > Client > Aggiungi client** per aggiungere a Websense Manager i client costituiti da utenti, gruppi, computer e reti in modo da poter assegnare loro un criterio.

Se ci si è collegati in base a un ruolo di amministratore con delega, è possibile aggiungere soltanto i client che appaiono nel proprio elenco di client gestiti. Durante la procedura di aggiunta alla pagina Client di client gestiti, occorre assegnare ad essi un criterio.

- 1. Identificare uno o più client:
 - Per aggiungere un client costituito da un utente, un gruppo o un dominio, navigare lungo l'albero della **Directory** per trovare le voci rilevanti nel proprio servizio di directory. Se si sta usando un servizio di directory LDAPbased, è anche possibile fare clic su **Cerca** per attivare uno strumento di ricerca da usare all'interno della directory (vedere *Ricerca nel service di directory*, pagina 71).
 - Per aggiungere un client costituito da un computer o da una rete, inserire un indirizzo IP o un range di indirizzi IP. Due definizioni qualsiasi di rete non possono sovrapporsi, ma un client rete può includere un indirizzo IP identificato separatamente come client computer. Nel caso di una sovrapposizione di questo tipo, i criteri assegnati al computer avranno priorità rispetto ai criteri assegnati alla rete.
- 2. Fare clic sul pulsante freccia (>) per aggiungere ciascun client all'elenco Client selezionati.

Per eliminare una voce dall'elenco Client selezionati, selezionare il client da eliminare e fare quindi clic su **Rimuovi**.

- 3. Selezionare il Criterio da assegnare a tutti i client dell'elenco Client selezionati.
- 4. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

I client vengono aggiunti all'apposito elenco della pagina **Gestione criteri > Client**. Per modificare il criterio assegnato a uno o più client o per configurare ulteriori impostazioni da applicare ai client, selezionare la voce di ogni client e fare clic su **Modifica**. Per ulteriori informazioni, vedere *Modifiche delle impostazioni per i client*, pagina 72,.

Ricerca nel service di directory

Se si è configurato il software Websense per una comunicazione con il servizio directory LDAP-based, è possibile utilizzare una funzione di ricerca per identificare gli utenti da aggiungere come client al Websense Manager. La ricerca è anche disponibile per aggiungere client gestiti e amministratori ai ruoli di amministratori con delega.

Per condurre una ricerca all'interno di un servizio di directory per il reperimento di informazioni su utenti, gruppi e unità organizzative:

- 1. Fare clic su Cerca.
- 2. Inserire il **Nome** di tutti o di una parte degli utenti, dei gruppi o delle unità organizzative.
- 3. Utilizzare l'elenco **Tipo** per indicare il tipo di voce di directory (utente, gruppo, OU o tutti) da trovare.

Se il servizio di directory è esteso, la selezione di **Tutti** potrebbe allungare i tempi della ricerca.

- 4. Navigare lungo l'albero di **Contesto di ricerca** per specificare la parte della directory in cui si vuole condurre la ricerca. Un contesto più ristretto rende la ricerca più rapida.
- 5. Fare clic su Vai.

Vengono visualizzati i risultati della ricerca.

- Selezionare una o più voci dei risultati della ricerca e fare quindi clic sulla freccia rivolta a destra (>) per aggiungere ciascuna selezione come client o come amministratore.
- 7. Fare clic su Nuova ricerca per inserire un altro set di criteri di ricerca.
- 8. Fare clic su Sfoglia per ritornare alla navigazione all'interno della directory.
- 9. Una volta terminate le modifiche, fare clic su **OK** per inserirle nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Modifiche delle impostazioni per i client

Usare la pagina **Gestione criteri > Client > Modifica client** per modificare le impostazioni dei criteri e dell'autenticazione relativi a uno o più client. Se si selezionano molteplici client prima di fare clic su Modifica, le modifiche di configurazione apportate alla pagina Modifica client vengono applicate a tutti i client selezionati.

- 1. Selezionare un **Criterio** da applicare ai client selezionati. Il criterio Predefinito regola i client fino a quando non vengono loro assegnati altri criteri.
- 2. Per consentire agli utenti di aggirare una pagina di blocco di Websense tramite l'inserimento di una password, fare clic su **Attivo** in Accedi con password e quindi inserire e confermare la password definita.

Per eliminare da un client i privilegi derivanti da un accesso con password, fare clic su **Disattivato**.

3. Per allocare un **Tempo assegnato** personalizzato ai client selezionati, fare clic su **Personalizzato** ed inserire quindi il tempo da assegnare.

Per ripristinare le impostazioni di tempo assegnato predefinite, fare clic su **Predefinito**.

4. Fare clic su **OK** per inserire nella cache le modifiche apportate e per ritornare alla pagina Client. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Le nuove impostazioni per i client vengono visualizzate come parte dell'elenco dei client nella pagina **Gestione criteri** > **Client**.

Spostamento dei client a ruoli diversi

I Super Administrators possono usare la pagina **Sposta client nel ruolo** per spostare uno o più client a un ruolo di amministrazione con delega. Una volta spostato, il client viene visualizzato nell'elenco Client gestiti e nella pagina Client del ruolo di destinazione.

- Il criterio applicato al client da un ruolo di Super Administrator e i filtri applicati in base a tale criterio, vengono copiati nel ruolo di amministratore con delega.
- Gli amministratori con delega possono modificare i criteri applicati ai client da loro gestiti.
- La restrizioni di Blocco filtro non incidono sui client gestiti dai Super Administrator, ma incidono sui client gestiti dai ruoli di amministratore con delega.
- Se un gruppo, un dominio o un'unità organizzativa vengono aggiunti a un ruolo come client gestiti, gli amministratori con delega assegnati a quel ruolo potranno assegnare criteri ai singoli utenti che fanno parte di quel gruppo, dominio o unità organizzativa.
- Se una rete (range di indirizzi IP) viene aggiunta ad un ruolo come client gestito, gli amministratori con delega assegnati a quel ruolo potranno assegnare criteri ai singoli computer collegati a questa rete.
- Lo stesso client non può venire spostato a molteplici ruoli.

Per spostare i client selezionati a un ruolo di amministratore con delega:

- 1. Utilizzare l'elenco a discesa **Seleziona ruolo** per selezionare un ruolo di destinazione.
- 2. Fare clic su OK.

Una finestra di dialogo pop-up indica che i client selezionati sono in corso di spostamento. La procedura di spostamento potrebbe richiedere qualche minuto.

3. Le modifiche non vengono implementate fino a quando non si fa clic su Salva tutto.

Se, durante la procedura di spostamento, gli amministratori con delega assegnati al ruolo selezionato sono collegati in sessione ed hanno accesso ai criteri, dovranno scollegarsi da Websense Manager e ricollegarsi ancora per poter visualizzare i nuovi client inseriti nel loro elenco di Client gestiti. 4

Criteri di filtraggio dell'uso di Internet

Argomenti correlati:

- Filtri per l'uso di Internet, pagina 37
- Client, pagina 61
- *Criterio Predefinito*, pagina 76
- Gestione dei criteri, pagina 77
- Ordine di filtraggio, pagina 82

I criteri regolano l'accesso degli utenti a Internet. I criteri sono costituiti da:

- Filtri di categoria, usati per l'applicazione di determinate azioni (quali autorizzazioni o blocchi) alle varie categorie di siti Web (vedere *Filtri di categoria e di protocollo*, pagina 38)
- Filtri per restrizioni di accesso, utilizzati per consentire l'accesso a un numero ristretto di siti Web (vedere *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172)
- Filtri di protocollo, usati per l'applicazione di azioni a protocolli Internet (vedere Filtri di categoria e di protocollo, pagina 38)
- La pianificazione dei tempi determina quando ciascun filtro di categoria, o filtro per restrizioni di accesso, e filtro di protocollo vanno applicati.

L'installazione del nuovo software Websense include 3 tipi di criteri predefiniti:

- Predefinito filtra l'accesso a Internet di tutti i client non soggetti ad altri criteri. Il software Websense inizia l'applicazione di questo criterio non appena si immette una chiave di sottoscrizione (vedere *Criterio Predefinito*, pagina 76).
- Illimitato consente un accesso illimitato a Internet. Questo criterio non viene applicato per predefinizione ai client.
- Esempio: Utente standard mostra come sia possibile applicare molteplici filtri di categoria e di protocollo in base a un criterio per fornire diversi gradi di restrizione di filtraggio in diversi periodi di tempo. Questo criterio è descritto nelle esercitazioni. Per nuovi utenti che spiegano il processo di modifica dei criteri e la loro applicazione ai client.

Utilizzare uno qualsiasi di questi criteri tale quale, modificarlo per soddisfare esigenze specifiche o creare i propri criteri personalizzati.

Criterio Predefinito

Argomenti correlati:

- Criteri di filtraggio dell'uso di Internet, pagina 75
- Gestione dei criteri, pagina 77
- Ordine di filtraggio, pagina 82

Se si installa il software Websense, il criterio Predefinito inizia a monitorare l'uso di Internet non appena si immette la chiave di sottoscrizione. Inizialmente, il criterio Predefinito concede un'autorizzazione a tutte le richieste.



Quando si aggiorna da una versione precedente del software Websense, le impostazioni dei criteri esistenti vengono conservate. A seguito dell'aggiornamento, si consiglia di rivalutare tali criteri per confermarne o meno la validità.

Durante la procedura di creazione e di applicazione di criteri di filtraggio personalizzati, il criterio Predefinito continua, per motivi di sicurezza, a filtrare gli accessi ad Internet per i client non ancora soggetti a specifici criteri.

Nel caso di una nuova installazione, il criterio Predefinito garantisce un filtraggio degli accessi ad Internet 24 ore al giorno, 7 giorni alla settimana (tramite l'applicazione di una combinazione di filtri di categoria o per restrizioni di accesso e, se applicabile, di filtri di protocollo).

Importante

Coloro che aggiornano da una versione precedente del software Websense, potrebbero disporre di un criterio Predefinito che non copre un periodo di tempo completo. Non si è tenuti a modificare il proprio criterio Predefinito. Se tuttavia, si decide, in un secondo tempo, di modificare tale criterio, il software Websense non consentirà di salvare le modifiche fino a quando tutti i periodi di tempo non sono stati coperti.

Modificare il criterio Predefinito, come necessario, per soddisfare specifiche esigenze aziendali. Il criterio Predefinito non può venire eliminato.

Gestione dei criteri

Argomenti correlati:

- Criteri di filtraggio dell'uso di Internet, pagina 75
- Creazione di un criterio
- Modifica di un criterio
- Filtri per l'uso di Internet
- Perfezionamento dei criteri di filtraggio

Usare la pagina **Gestione criteri** > **Criteri** per visualizzare le informazioni relative ai criteri esistenti. Questa pagina funge anche da punto di inizio per l'aggiunta, la modifica e l'eliminazione di criteri, per la loro copia nei ruoli di amministratori con delega (Super Administrator soltanto) nonché per la stampa di informazioni dettagliate sulla configurazione dei criteri definiti.

La pagina Criteri include un elenco dei criteri esistenti. Questo elenco include il nome e la descrizione di ogni criterio, nonché il numero dei client utente, rete e computer ai quali questi criteri sono stati assegnati.

- Per aggiungere un criterio, fare clic su **Aggiungi**. Per ulteriori informazioni al proposito, andare a *Creazione di un criterio*, pagina 78.
- Per modificare un criterio, fare clic sul suo nome nell'elenco. Per ulteriori informazioni, vedere *Modifica di un criterio*, pagina 79.
- Per visualizzare i client che vengono filtrati in base a determinati criteri, fare clic su un numero nella colonna Utenti, Reti o Computer. Le informazioni sul client vengono visualizzate nella finestra di dialogo popup.

Per stampare un elenco di criteri e di loro componenti, tra cui filtri, categorie e protocolli personalizzati, parole chiave, URL personalizzati e espressioni regolari, fare clic su **Stampa criteri su file**. Questa funzione crea un foglio Microsoft Excel con informazioni dettagliate sui criteri. Si intende con questo fornire un modo pratico, per il personale del reparto di risorse umane, per i manager e altro personale con funzioni direttive, di esaminare le informazioni ottenute tramite i criteri di filtraggio applicati.

Se si sono creati ruoli di amministrazione con delega (vedere *Amministrazione con delega*, pagina 241), i Super Administrator possono copiare i filtri da loro creati in altri ruoli in modo che possano venire usati dagli amministratori con delega. Vengono copiati anche i filtri applicati in base ai criteri definiti.



Poiché gli amministratori con delega sono soggetti al Blocco filtro, i filtri e i criteri di tipo Autorizza sempre non possono venire copiati nei ruoli. Per copiare dei criteri in un altro ruolo, contrassegnare la casella di controllo adiacente al nome del criterio e fare quindi clic su **Copia nel ruolo**. Per ulteriori informazioni, vedere *Copia di filtri e criteri nei ruoli*, pagina 177.

Creazione di un criterio

Argomenti correlati:

- Criteri di filtraggio dell'uso di Internet, pagina 75
- Gestione dei criteri, pagina 77
- Modifica di un criterio, pagina 79
- *Gestione dei filtri*, pagina 48
- *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172

Utilizzare la pagina **Gestione criteri > Criteri > Aggiungi criterio** per creare un nuovo criterio personalizzato.

1. Inserire un **Nome criterio** univoco. I nomi assegnati ai criteri devono contenere da 1 a 50 caratteri e non possono includere i caratteri seguenti:

* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

I nomi assegnati ai criteri possono includere spazi, trattini e apostrofi.

2. Inserire una breve **Descrizione** del criterio. La descrizione dovrebbe essere chiara e dettagliata per agevolare la gestione dei criteri a lungo termine.

Le restrizioni relative ai caratteri usati per i nomi dei criteri sono anche applicabili alle descrizioni, con due eccezioni: le descrizioni possono includere punti (.) e virgole (,).

3. Per utilizzare un criterio esistente come base per la creazione di un nuovo criterio, selezionare la casella di controllo **Basa su criterio esistente** e selezionare quindi il criterio rilevante dall'elenco a discesa.

Per creare un criterio da zero, lasciare questa casella deselezionata.

4. Fare clic su **OK** per inserire nella cache le modifiche apportate e per andare alla pagina Modifica criterio.

Usare la pagina Modifica criterio per completare la definizione dei nuovi criteri. Vedere *Modifica di un criterio*, pagina 79.

Modifica di un criterio

Argomenti correlati:

- Criteri di filtraggio dell'uso di Internet, pagina 75
- Gestione dei criteri, pagina 77
- Creazione di un criterio, pagina 78
- Gestione dei filtri, pagina 48
- *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172

Usare la pagina **Gestione criteri > Criteri > Modifica criterio** per apportare modifiche a un criterio esistente oppure per completare la definizione di un nuovo criterio.

Utilizzare l'area superiore della pagina per modificare il nome e la descrizione del criterio.

- Fare clic su **Rinomina** per modificare il nome del criterio.
- Per modificare la descrizione del criterio, digitare semplicemente la modifica nel campo **Descrizione**.

Sotto la descrizione del criterio, il campo **Client** riporta in un elenco quanti client di ogni tipo (utente, computer e rete) sono attualmente filtrati da questo criterio. Per visualizzare i client soggetti a questo criterio, fare clic sul link che corrisponde al tipo di client appropriato.

Per assegnare questo criterio ad altri client, fare clic su **Applica ai client** nella barra degli strumenti in alto nella pagina e quindi andare alla sezione *Assegnazione dei criteri ai client*, pagina 81.

Utilizzare l'area **Definizione criterio** per definire i filtri che questo criterio deve applicare in base a diversi tempi:

- 1. Per aggiungere un blocco temporale alla pianificazione, fare clic su Aggiungi.
- 2. Utilizzare le colonne **Inizio** e **Fine** della tabella Pianificazione per definire il periodo di tempo coperto da questo blocco temporale.

Per definire un filtraggio da applicare a un periodo di tempo che attraversa la mezzanotte (ad esempio, dalle 17 alle 8 del mattino), occorre aggiungere due blocchi temporali alla pianificazione: uno che copre l'arco di tempo dall'inizio del periodo in oggetto fino a mezzanotte e un altro che copre da mezzanotte alla fine del periodo in oggetto.

Il criterio dal nome **Esempio – Utente standard**, incluso nel software Websense, dimostra come definire un periodo di filtraggio che attraversa la mezzanotte.

- 3. Utilizzare la colonna **Giorni** per definire i giorni della settimana da includere in questo blocco temporale. Per selezionare i giorni da un elenco, fare clic sulla freccia rivolta verso il basso nell'area di destra della colonna. Una volta selezionati i giorni, fare clic sulla freccia rivolta verso l'alto.
- 4. Utilizzare la colonna **Filtro di accesso limitato** / **categoria** per selezionare un filtro da applicare durante questo blocco temporale.

Per aggiungere un nuovo filtro da applicare tramite questi criteri, selezionare **Crea filtro di categoria** o **Crea filtro per restrizioni di accesso**. Per ulteriori informazioni, vedere *Creazione di un filtro di categoria*, pagina 49 oppure *Creazione di un filtro per restrizioni di accesso*, pagina 174.

5. Utilizzare la colonna **Filtro di protocollo** per selezionare un filtro di protocollo da applicare a questo blocco temporale.

Per aggiungere un nuovo filtro da applicare tramite questo criterio, selezionare **Crea filtro di protocollo**. Per informazioni, vedere *Creazione di un filtro di protocollo*, pagina 52.

6. Ripetere le operazioni descritte dal punto 1 al punto 5 per aggiungere blocchi temporali alla pianificazione.

Se si seleziona un blocco temporale nella pianificazione, l'area inferiore della pagina Modifica criteri visualizza i filtri applicati durante quel blocco temporale. Ciascun elenco di filtri include:

- Il tipo di filtro (filtro di categoria, filtro per accesso limitato o filtro di protocollo)
- Il nome e la descrizione del filtro
- Il contenuto del filtro (categorie o protocolli con azioni ad essi applicate o un elenco di siti il cui accesso è autorizzato)
- Il numero di criteri applicati al filtro selezionato
- I pulsanti che possono venire utilizzati per modificare il filtro

Quando si modifica un filtro in questa pagina, le modifiche incidono su tutti i criteri applicati al filtro. Prima di modificare un filtro applicato tramite molteplici criteri, fare clic sul link **Criteri che utilizzano questo filtro** per verificare esattamente i criteri interessati.

Tipo di filtro	Pulsanti
filtro di categoria	• Utilizzare i pulsanti Autorizza, Blocca o Assegna durata per modificare l'azione applicata alle categorie selezionate (vedere <i>Azioni di filtraggio</i> , pagina 44).
	• Per modificare l'azione applicata a una categoria principale e a tutte le sottocategorie, modificare per prima cosa l'azione applicata alla categoria principale e fare quindi clic su Applica a sottocategorie .
	• Per attivare il blocco in base alle parole chiave o il blocco in base all'uso della larghezza di banda, fare clic su Avanzate .
filtro per accesso ristretto	 Utilizzare i pulsanti Aggiungi siti e Aggiungi espressioni per aggiungere al filtro gli URL, gli indirizzi IP o le espressioni regolari consentiti (vedere <i>Restrizione</i> <i>dell'accesso degli utenti a un elenco definito di siti</i> <i>Internet</i>, pagina 172). Per eliminare un sito dal filtro, selezionare la casella di controllo accanto all'URL, all'indirizzo IP o all'espressione e fare quindi clic su Elimina.
filtro protocolli	• Utilizzare i pulsanti Autorizza o Blocca per modificare l'azione applicata ai protocolli selezionati (vedere <i>Azioni di filtraggio</i> , pagina 44).
	 Per modificare l'azione applicata a tutti i protocolli di un gruppo di protocolli, modificare l'azione applicata a un protocollo qualsiasi del gruppo e fare quindi clic su Applica a sottocategorie.
	• Per registrare i dati del protocollo selezionato nel log, oppure per attivare il blocco in base alla larghezza di banda, fare clic su Avanzate .

I pulsanti visualizzati nell'area inferiore dell'elenco dei filtri, dipendono dal tipo di filtro:

Al termine della procedura di modifica dei criteri, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Assegnazione dei criteri ai client

Argomenti correlati:

- Criteri di filtraggio dell'uso di Internet, pagina 75
- Creazione di un criterio, pagina 78
- Modifica di un criterio, pagina 79
- *Client*, pagina 61
- *Aggiunta di un client*, pagina 70

Usare la pagina **Criteri > Modifica criterio > Applica criterio ai client** per assegnare i criteri selezionati ai client.

L'elenco Client elenca tutti i client costituiti da utenti, computer e reti disponibili nonché i criteri applicati attualmente ad ogni client.

Selezionare la casella di controllo accanto ad ogni client da filtrare in base al criterio selezionato, e fare quindi clic su **OK** per ritornare alla pagina Modifica criterio. Fare clic su **OK** per inserire le modifiche nella cache.

Fare clic su **Salva tutto** per indicare al software Websense di iniziare ad usare il nuovo criterio per filtrare le richieste inoltrate dai client selezionati.

Ordine di filtraggio

Il software Websense utilizza molteplici filtri, applicati ad un ordine specifico per determinare se autorizzare, bloccare o limitare l'accesso richiesto ai dati Internet

Per ciascuna richiesta ricevuta, il software Websense:

- 1. Verifica la validità della sottoscrizione accertandosi che non sia scaduta e che il numero di client sottoscritti non sia stato superato.
- 2. Determina il criterio da applicare, procedendo nell'ordine seguente:
 - a. Criterio assegnato all'utente.
 - b. Criterio assegnato all'indirizzo IP (computer o rete) del computer in uso.
 - c. Criterio assegnato ai gruppi a cui appartiene l'utente.
 - d. Criterio assegnato al dominio dell'utente.
 - e. Il criterio **Predefinito**.

Viene usato il primo criterio trovato dalla ricerca.

3. Filtra la richiesta in base alle restrizioni stabilite dal criterio.

In alcuni casi, un utente potrebbe appartenere a più di un gruppo o dominio, e nessun criterio per utenti, computer o rete è applicabile. In questi casi, il software Websense verifica i criteri assegnati a ciascun gruppo di appartenenza dell'utente.

- Se a tutti i gruppi sono stati applicati gli stessi criteri, il software Websense filtra la richiesta in base a questo criterio.
- Se a uno dei gruppi è stato applicato un criterio diverso, il software Websense filtra la richiesta in base all'opzione Utilizzare blocchi più restrittivi della pagina Impostazioni > Filtraggio.

Se si seleziona **Utilizzare blocchi più restrittivi** e uno qualsiasi dei criteri applicabili blocca l'accesso alla categoria richiesta, il software Websense blocca il sito.

Se questa opzione non è selezionata e uno qualsiasi dei criteri applicabili consente l'accesso alla categoria richiesta, il software Websense consente l'accesso al sito.

Se uno qualsiasi dei criteri applicabili prevede un filtro per restrizioni di accesso, l'opzione **Utilizzare blocchi più restrittivi** può esercitare effetti diversi da quelli previsti. Vedere *Filtri per restrizioni di accesso e priorità di un filtro*, pagina 172.

Filtraggio di un sito

Per determinare se l'accesso al sito richiesto debba venire bloccato o autorizzato, il software Websense valuta le restrizioni definite dai criteri, come descritto di seguito.



- 1. Determina quali **filtri di categoria** o **filtri per restrizioni di accesso** sono previsti dai criteri in relazione al giorno e all'ora correnti.
 - Se il filtro di categoria attivo è Autorizza sempre, l'accesso al sito è autorizzato.
 - Se il filtro di categoria attivo è **Blocca sempre**, l'accesso al sito è bloccato.
 - Se il filtro è **per restrizioni di accesso**, il software Websense verifica se il filtro contiene l'URL o l'indirizzo IP. In caso positivo, l'accesso al sito viene autorizzato. In caso negativo, l'accesso al sito viene bloccato.

• Se un altro filtro di categoria è applicabile, procedere al punto 2.

Nota

Il software Websense filtra gli URL a cui si è acceduto dalla cache di un motore di ricerca Internet analogamente a come filtra qualsiasi altro URL. Gli URL archiviati in questo modo vengono filtrati in base ai criteri attivi per quelle categorie di URL. I record di registro per gli URL memorizzati nella cache mostrano l'intero URL memorizzato, inclusi eventuali parametri del motore di ricerca.



- 2. Cerca una corrispondenza tra il sito e una voce dell'elenco URL non filtrati.
 - Se l'URL è incluso nell'elenco, autorizza l'accesso.
 - Se l'URL non è incluso nell'elenco, procede alle operazioni descritte al punto
 3.
- 3. Verifica il **filtro di protocollo** attivo e determina se esistono protocolli HTTP associati alla richiesta.
 - In caso positivo, applica le impostazioni del filtro di protocollo ai dati che potrebbero venire trasmessi.
 - In caso negativo, procede alle operazioni descritte al punto 4.
- 4. Cerca una corrispondenza tra il sito e una voce dell'elenco URL ricategorizzati.
 - Se trova una corrispondenza, identifica la categoria per il sito e procede alle operazioni descritte al punto 6.
 - Se non trova una corrispondenza, procede alle operazioni descritte al punto 5.
- 5. Cerca una corrispondenza tra il sito e una voce dell'elenco Master Database.
 - Se l'URL è incluso nel Master Database, identifica la categoria per il sito e procede alle operazioni descritte al punto 6.

 Se non trova una corrispondenza, categorizza il sito Miscellanea/Non categorizzato e procede alle operazioni descritte al punto 6.



- 6. Verifica il filtro di categoria attivo e identifica l'azione applicata alla categoria contenente il sito richiesto.
 - Se l'azione è **Blocca**, blocca l'accesso al sito.
 - Se viene applicata un'altra azione, procede alle operazioni descritte al punto 7.
- 7. Verifica le impostazioni di **Bandwidth Optimizer** nel filtro di categoria attivo (vedere *Uso di Bandwidth Optimizer per la gestione della larghezza di banda*, pagina 195).
 - Se l'uso della larghezza di banda supera i limiti configurati, blocca il sito.
 - Se l'uso corrente della larghezza di banda non supera i limiti specificati, o se nessuna azione relativa all'uso della larghezza di banda è applicabile, procede alle operazioni descritte al punto 8.
- 8. Verifica le restrizioni relative al **tipo di file** applicate alla categoria attiva (vedere *Gestione del traffico in base al tipo di file*, pagina 197).
 - Se il sito contiene file le cui estensioni sono bloccate, blocca l'accesso a questi file. Se il sito contiene un tipo di file bloccato, blocca l'accesso al sito.
 - Se il sito non contiene file le cui estensioni sono bloccate, procede alle operazioni descritte al punto 9.
- 9. Verifica la presenza di **parole chiave bloccate** nel percorso URL e CGI, se la funzione di blocco in base alla parole chiave è attiva (vedere *Filtro basato su parole chiave*, pagina 184).
 - Se trova una parola chiave bloccata, blocca l'accesso al sito.

 Se non trova una parola chiave bloccata, procede alle operazioni descritte al punto 10.



- 10. Gestisce il sito in base all'azione applicata alla categoria.
 - Autorizza Autorizza l'accesso al sito.
 - Limita in base al tempo assegnato Visualizza il messaggio di blocco con l'opzione di visualizzare il sito in base al tempo assegnato oppure ritorna alla pagina precedente.
 - **Conferma** Visualizza il messaggio di blocco con l'opzione di visualizzare il sito a scopo di lavoro.

Il software Websense procede fino a quando l'accesso al sito richiesto non viene bloccato o esplicitamente autorizzato. A quel punto, il software Websense non tenta più di applicare un filtro. Ad esempio, se un sito richiesto appartiene a una categoria bloccata e contiene una parola chiave bloccata, il software Websense blocca il sito a livello di categoria senza attendere l'applicazione del filtro in base alle parole chiave. Il Log Server registra quindi le richieste come bloccate a causa di una categoria bloccata, non a causa di una parola chiave.

Nota

Gli utenti con privilegi di accesso con password possono accedere a siti Internet indipendentemente dai motivi per i quali il sito era stato bloccato.

Pagine di blocco

Argomenti correlati:

- Messaggi di blocco dei protocolli, pagina 88
- *Gestione delle pagine di blocco*, pagina 89
- Creazione di messaggi di blocco alternativi, pagina 94
- Uso di una pagina di blocco alternativa in un altro computer, pagina 94

Quando il software Websense blocca un sito Web, visualizza una pagina di blocco nel browser del client. Se il sito è bloccato in quanto appartiene ad una categoria della classe Rischio sicurezza (vedere *Classi di rischio*, pagina 41), viene visualizzata una versione speciale della pagina di blocco.

Per impostazione predefinita, la pagina di blocco è costituita da 3 sezioni principali.

Contenuto bloccato dall'organizzazione 🛛 🚽		intestazione
Motivo: URL:	La seguente categoria Websense è soggetta a filtro: Contenuto per adulti. http://www.playboy.com/	frame superiore
Opzioni:	Fare clic su <u>ulteriori informazioni</u> per informazioni sul criterio di accesso. Fare clic su Indietro oppure utilizzare il pulsante Indietro del browser per tornare al pagina precedente. Indietro	frame inferiore

- L'intestazione indica che il sito è bloccato.
- Il **frame superiore** contiene un messaggio di blocco con l'URL richiesto e il motivo per cui l'URL è stato bloccato.
- Il **frame inferiore** include le opzioni disponibili all'utente, come ad esempio l'opzione di ritornare alla pagina precedente o di fare clic sul pulsante Continua o su Utilizza tempo assegnato per visualizzare il sito.

Le pagine di blocco vengono generate dai file HTML. I file delle pagine di blocco predefinite sono incluse nel software Websense. È possibile usare questi file predefiniti oppure creare le proprie versioni personalizzate.

- Personalizzare i file predefiniti per modificare il messaggio di blocco (vedere Gestione delle pagine di blocco, pagina 89).
- Configurare il software Websense in modo che possa utilizzare i messaggi di blocco (predefiniti o personalizzati) ospitati in un server Web remoto (vedere Uso di una pagina di blocco alternativa in un altro computer, pagina 94).

Messaggi di blocco dei protocolli

Argomenti correlati:

- *Gestione delle pagine di blocco*, pagina 89
- Creazione di messaggi di blocco alternativi, pagina 94
- Uso di una pagina di blocco alternativa in un altro computer, pagina 94

Se un utente o un'applicazione richiede un protocollo non-HTTP bloccato, il software Websense visualizza normalmente un messaggio di blocco del protocollo.

Se tuttavia un utente richiede, dall'interno di un browser, l'accesso a un sito FTP, HTTPS e Gopher bloccato, e la richiesta passa attraverso un proxy, viene visualizzata nel browser una pagina di blocco HTML-based.

Se un'applicazione richiede l'accesso a un protocollo bloccato, l'utente potrebbe ricevere un messaggio di errore dall'applicazione stessa con l'indicazione che la richiesta non può essere eseguita. Questi messaggi di errore dell'applicazione non sono generati dal software Websense.

La configurazione di alcuni sistemi potrebbe richiedere la visualizzazione dei messaggi di blocco dei protocolli nei computer dotati del sistema Windows:

- Per poter visualizzare il messaggio di blocco di un protocollo su un computer client dotato di Windows NT, XP o 200x, occorre aver attivato il servizio Windows Messenger. Per impostazione predefinita, questo servizio è disattivo. Si può usare la finestra di dialogo Servizi Windows per verificare se il servizio è in esecuzione in un determinato computer (vedere *Finestra di dialogo Servizi di Windows*, pagina 406).
- Per visualizzare i messaggi di blocco dei protocolli in un computer Windows 98, occorre avviare winpopup.exe, situato nella directory Windows. Eseguire l'applicazione dal prompt di comando oppure copiarla nella cartella di avvio in modo che vanga configurata per un lancio automatico.

I messaggi di blocco dei protocolli non vengono visualizzati nei computer Linux. Le pagine di blocco HTML vengono visualizzate indipendentemente dal sistema operativo in uso.

Se si è attivato il filtro di protocollo, il software Websense filtrerà le richieste di protocollo sia nel caso i messaggi di blocco dei protocolli siano o non siano stati configurati per una visualizzazione nei computer client.

Gestione delle pagine di blocco

Argomenti correlati:

- Messaggi di blocco dei protocolli, pagina 88
- Personalizzazione dei messaggi di blocco, pagina 90
- Creazione di messaggi di blocco alternativi, pagina 94
- Uso di una pagina di blocco alternativa in un altro computer, pagina 94

I file da utilizzare per creare le pagine di blocco di Websense sono memorizzati nella directory **Websense\BlockPages\en\Default**:

• **master.html** crea il frame contenente le informazioni per la pagina di blocco e utilizza uno dei file seguenti per visualizzare nel frame inferiore le opzioni disponibili.

Nome del file	Contenuto
blockFrame.html	Testo e pulsante (opzione Indietro) per i siti inclusi nelle categorie bloccate.
continueFrame.html	Testo e pulsanti per i siti inclusi nelle categorie alle quali è stata applicata l'azione Conferma .
quotaFrame.html	Testo e pulsanti per i siti inclusi nelle categorie alle quali è stata applicata l'azione Assegna durata .
moreInfo.html	Contenuto per la pagina visualizzata quando un utente fa clic sul link Ulteriori informazioni nella pagina di blocco.

• **block.html** contiene il testo per il frame superiore del messaggio di blocco che spiega che l'accesso è ristretto, indica il sito richiesto e descrive il motivo delle restrizioni di accesso.

Personalizzazione dei messaggi di blocco

Argomenti correlati:

- Modifica delle dimensioni del frame del messaggio, pagina 91
- Modifica del logo visualizzato nella pagina di blocco, pagina 91
- Utilizzo delle variabili del contenuto di una pagina di blocco, pagina 92
- Ripristino delle pagine di blocco predefinite, pagina 93

È possibile fare una copia dei file delle pagine di blocco predefinite e quindi usare questa copia per personalizzare il frame superiore della pagina di blocco che gli utenti ricevono.

- Aggiungere informazioni sui criteri relativi all'uso di Internet da parte della propria organizzazione.
- Offrire un metodo di contatto con il reparto delle risorse umane o con un amministratore di Websense riguardo ai criteri d'uso di Internet.
- 1. Navigare alla directory delle pagine di blocco di Websense:

<percorso di installazione>\BlockPages\en\Default

2. Copiare i file delle pagine di blocco nella directory delle pagine di blocco:

<percorso di installazione>\BlockPages\en\Custom

Nota

Non modificare i file dei messaggi di blocco originali nella directory BlockPages\en\Default. Copiarli nella directory BlockPages\en\Custom e quindi modificarne le copie.

3. Aprire i file in un programma di gestione del testo, come ad esempio Notepad o Vi.



Attenzione

Utilizzare un editor del testo per modificare i file dei messaggi di blocco. Alcuni programmi editor di HTML modificano il codice HTML e potrebbero con questo danneggiare i file e causare problemi di visualizzazione dei messaggi di blocco.

- Modificare il testo. I file contengono istruzioni su come inserire le modifiche.
 Non modificare i token (racchiusi tra i simboli \$* e *\$) o la struttura del codice HTML. I token consentono al software Websense di includere specifiche informazioni nei messaggi di blocco.
- 5. Salvare il file.
- 6. Riavviare Filtering Service (per le relative istruzioni, vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

Modifica delle dimensioni del frame del messaggio

In base al tipo di informazioni che si vuole includere nel messaggio di blocco, la larghezza del messaggio e l'altezza del frame superiore predefinite potrebbero non essere appropriate. Per modificare i parametri di queste dimensioni nel file **master.html**:

- 1. Copiare il file master.html dalla directory Websense\BlockPages\en\Default alla directory Websense\BlockPages\en\Custom.
- 2. Aprire i file in un programma di gestione del testo, come ad esempio Notepad o Vi (non usare un editor di testo HTML).
- 3. Per modificare la larghezza del frame del messaggio, modificare la riga seguente:

<div style="border: 1px solid #285EA6;width: 600px...">

Modificare il valore del parametro width (larghezza), come necessario.

4. Per consentire al frame superiore del messaggio di scorrere, in modo che l'utente possa visualizzare tutte le informazioni, modificare la riga seguente:

```
<iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
scrolling="no" style="width:100%; height: 6em;">
```

Sostituire il valore del parametro **scrolling (scorrimento)** con **auto** in modo da visualizzare una barra di scorrimento quando il testo del messaggio supera l'altezza del frame.

È anche possibile modificare il valore del parametro **height (altezza)** per cambiare l'altezza del frame.

- 5. Salvare e chiudere il file.
- 6. Riavviare Filtering Service per implementare le modifiche apportate (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

Modifica del logo visualizzato nella pagina di blocco

Il file **master.html** include anche il codice HTML utilizzato per visualizzare il logo di Websense nella pagina di blocco. Per visualizzare il logo della propria organizzazione:

- 1. Copiare i file di blocco dalla directory Websense\BlockPages\en\Default alla directory Websense\BlockPages\en\Custom, se non è stato ancora fatto.
- Copiare il file di immagine contenente il logo della propria organizzazione nello stesso percorso.
- 3. Aprire il file **master.html** in un programma di gestione del testo, come ad esempio Notepad o Vi (non usare un editor di testo HTML) e modificare la riga seguente per sostituire il logo di Websense con il proprio logo.

```
<img title="Websense" src="/en/Custom/wslogo_block_page.png" ...>
```

- Sostituire wslogo_block_page.png con il nome del file di immagine contenente il logo della propria organizzazione.
- Sostituire i valori del parametro **title** per riflettere il nome della propria organizzazione.

- 4. Salvare e chiudere il file.
- 5. Riavviare il Filtering Service per implementare le modifiche apportate (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

Utilizzo delle variabili del contenuto di una pagina di blocco

Le variabili di contenuto definiscono le informazioni visualizzate nelle pagine di blocco HTML. Le variabili seguenti sono incluse nel codice del messaggio di blocco predefinito.

Nome della variabile	Contenuto visualizzato
WS_DATE	Data corrente
WS_USERNAME	Nome dell'utente (senza il nome del dominio)
WS_USERDOMAIN	Nome del dominio dell'utente
WS_IPADDR	Indirizzo IP del computer che ha originato la richiesta
WS_WORKSTATION	Nome del computer bloccato (se il nome non è disponibile, viene visualizzato il suo indirizzo IP)

Per usare una variabile, inserire il nome della variabile racchiusa tra i simboli \$* *\$ del relativo tag HTML.

```
$*WS USERNAME*$
```

In questo esempio, WS USERNAME è la variabile.

Il codice del messaggio di blocco include altre variabili, come descritto qui di seguito. Alcune di queste variabili possono essere utili nella creazione di messaggi di blocco personalizzati. Si raccomanda tuttavia di **non** modificare le variabili visibili nei file dei messaggi di blocco definiti da Websense. Poiché Filtering Service utilizza queste variabili durante la gestione delle richieste bloccate, non è consentito modificarle.

Nome della variabile	Obiettivo
WS_URL	Visualizza l'URL richiesto
WS_BLOCKREASON	Visualizza il motivo del blocco del sito (ad es. l'azione di filtraggio applicata)
WS_ISSECURITY	Indica se il sito richiesto appartiene ad una delle categorie predefinite della classe Rischio sicurezza. Se TRUE, la pagina di blocco per la sicurezza viene visualizzata
WS_PWOVERRIDECGIDATA	Inserisce automaticamente nel campo del codice HTML della pagina di blocco le informazioni relative all'uso del pulsante Accedi con password

Nome della variabile	Obiettivo
WS_QUOTA_CGIDATA	Inserisce automaticamente nel campo del codice HTML della pagina di blocco le informazioni relative all'uso del pulsante Utilizza tempo assegnato
WS_PASSWORDOVERRID_BEGIN, WS_PASSWORDOVERRID_END	Utilizzata per l'attivazione della funzione di accesso con la password.
WS_MOREINFO	Visualizza informazioni dettagliate (dopo aver fatto clic sul link Ulteriori informazioni) sul motivo per cui l'accesso al sito è stato bloccato
WS_POLICYINFO	Indica i criteri applicabili al client che ha inoltrato la richiesta
WS_MOREINFOCGIDATA	Inoltra i dati a Filtering Service sull'uso del link Ulteriori informazioni
WS_QUOTATIME	Visualizza il tempo assegnato che è rimasto al client che ha inoltrato la richiesta
WS_QUOTAINTERVALTIME	Visualizza la durata della sessione assegnata e configurata per il client che ha inoltrato la richiesta
WS_QUOTABUTTONSTATE	Indica se il pulsante Utilizza tempo assegnato è stato attivato o disattivato in relazione a una particolare richiesta
WS_SESSIONID	Agisce come un identificatore interno associato a una richiesta
WS_TOPFRAMESIZE	Indica le dimensioni (in valore percentuale) dell'area superiore di una pagina di blocco inviata da un server di blocco personalizzato, se configurato
WS_BLOCKMESSAGE_PAGE	Indica il testo d'origine da usare per il frame superiore di una pagina di blocco
WS_CATEGORY	Visualizza la categoria dell'URL bloccato
WS_CATEGORYID	Rappresenta l'identificatore univoco definito per la categoria dell'URL richiesto

Ripristino delle pagine di blocco predefinite

Se gli utenti incorrono in errori dopo aver implementato messaggi di blocco personalizzati, è possibile ripristinare i messaggi di blocco predefiniti procedendo come segue:

1. Cancellare tutti i file dalla directory **Websense****BlockPages****en****Custom**. Per impostazione predefinita, il software Websense riprenderà ad usare i file della directory predefinita.

2. Riavviare il Filtering Service (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

Creazione di messaggi di blocco alternativi

Argomenti correlati:

- *Gestione delle pagine di blocco*, pagina 89
- Personalizzazione dei messaggi di blocco, pagina 90

È possibile creare i propri file HTML per inserire il testo desiderato nel frame superiore della pagina di blocco. Utilizzare i file HTML esistenti, creare file alternativi partendo da zero, oppure creare copie del file **block.html** da usare come modello.

- Creare dei messaggi di blocco diversi per ciascuno dei 3 protocolli: HTTP, FTP e Gopher.
- Memorizzare i file nel computer in cui è installato Websense o nel proprio server Web interno (vedere Uso di una pagina di blocco alternativa in un altro computer, pagina 94).

Dopo aver creato i file dei messaggi di blocco alternativi, occorre configurare il software Websense affinché questi possano venire visualizzati (vedere *Configurazione delle impostazioni di filtraggio di Websense*, pagina 57). Durante questa procedura è possibile specificare il messaggio da usare per ciascun protocollo configurabile.

Uso di una pagina di blocco alternativa in un altro computer

Argomenti correlati:

- *Gestione delle pagine di blocco*, pagina 89
- Personalizzazione dei messaggi di blocco, pagina 90
- Creazione di messaggi di blocco alternativi, pagina 94

Anziché usare le pagine di blocco Websense e personalizzare il messaggio nel frame superiore, è possibile creare pagine di blocco in HTML personalizzate e memorizzarle nel proprio server Web interno.



Nota

È anche possibile archiviare le pagine di blocco in un server Web esterno. Se tuttavia questo server ospita un sito incluso nel Master Database, e quel sito fa parte di una categoria bloccata, la pagina di blocco stessa viene bloccata.

Alcune organizzazioni usano pagine di blocco alternative e remote per nascondere l'identità del server di Websense.

La pagina di blocco remota può essere un file HTML qualsiasi; non deve necessariamente avere lo stesso formato delle pagine di blocco predefinite di Websense. L'uso di questo metodo per creare pagine di blocco, tuttavia, impedisce l'uso delle funzioni Continua, Utilizza tempo assegnato e Accesso con password disponibili con le pagine di blocco definite da Websense (predefinite o personalizzate).

Con i file posizionati correttamente, modificare il file eimserver.ini in modo che punti alla nuova pagina di blocco.

- 1. Interrompere i servizi erogati da Websense Filtering Service e Policy Server, nell'ordine indicato (vedere Chiusura e riavvio dei servizi di Websense, pagina 290).
- 2. Nel computer in cui è installato Filtering Service, navigare alla directory bin di Websense (per predefinizione, \Programmi\Websense\bin o /opt/websense/bin).
- 3. Creare una copia di backup di **eimserver.ini** ed archiviarla in un'altra directory.
- 4. Aprire il file **eimserver.ini** in un programma di gestione del testo e cercare la sezione WebsenseServer (all'inizio del file).
- 5. Inserire il nome del computer host o l'indirizzo IP del server che ospita la pagina di blocco, adottando il seguente formato:

```
UserDefinedBlockPage=http://<nome o indirizzo IP del
computer host>
```

Si deve inserire il protocollo dell'URL (http://).

- 6. Salvare e chiudere il programma di gestione del testo.
- 7. Riavviare Websense Policy Server e Filtering Service, nell'ordine indicato.

Una volta avviati i servizi, gli utenti riceveranno la pagina di blocco memorizzata nel computer alternativo.

Utilizzo dei report per valutare i criteri di filtraggio

Argomenti correlati:

- Panoramica sulla creazione dei report, pagina 98
- Report di presentazione, pagina 100
- *Report investigativi*, pagina 119
- Accesso all'attività utente, pagina 147

Websense Manager offre diversi strumenti di creazione dei report da usare nella valutazione dell'efficacia dei criteri di filtraggio definiti. (Websense Manager e i componenti usati per la creazione dei report di Websense devono essere installati nei server Windows.)

- ◆ La pagina Oggi viene visualizzata all'apertura di Websense Manager. Visualizza lo stato operativo del software Websense e può anche visualizzare i grafici relativi alle attività di filtraggio eseguite sulla rete a partire da mezzanotte. Vedere Oggi: integrità, sicurezza e risultati a partire dalla mezzanotte, pagina 22.
- La pagina **Cronologia** visualizza i grafici delle attività di filtraggio eseguite su rete fino a un massimo di 30 giorni, a seconda della quantità di informazioni registrate nel database di registrazione. Questi grafici non includono le attività della giornata in corso. (Vedere *Cronologia: ultimi 30 giorni*, pagina 25.)
- ◆ I Report di presentazione e i Report investigativi offrono varie opzioni per la generazione, la personalizzazione e i tempi di generazione dei report. Per ulteriori informazioni, vedere *Panoramica sulla creazione dei report*, pagina 98.

Se la propria organizzazione ha installato Websense Manager in un server Linux, o ha scelto il programma di creazione dei report Websense Explorer for Linux, anziché i componenti di creazione dei report eseguibili su Windows, le opzioni relative a tale funzione non vengono visualizzate in Websense Manager. Nella pagine Oggi e Cronologia, i grafici relativi al filtraggio di accesso a Internet non vengono visualizzati. Vedere la *Explorer for Linux Administrator's Guide* per informazioni sull'installazione del programma e sulla creazione dei report.

Panoramica sulla creazione dei report

Argomenti correlati:

- Utilizzo dei report per valutare i criteri di filtraggio, pagina 97
- Report di presentazione, pagina 100
- Report investigativi, pagina 119
- Accesso all'attività utente, pagina 147

Oltre ai grafici visualizzati nella pagine Oggi e Cronologia, il software Websense offre 2 opzioni di creazione dei report: report di presentazione e report investigativi.

Nota

Nelle organizzazioni che usano un'amministrazione con delega, alcuni amministratori potrebbero non essere autorizzati ad accedere a tutte le funzioni di creazione dei report. Vedere *Amministrazione con delega*, pagina 241.

Report di presentazione offre un elenco di vari tipi di report. Alcuni sono report tabulari, alcuni sono composti sia da un grafico a barre che da una tabella. Per creare un report di presentazione:

- 1. Selezionare un report dall'apposito elenco.
- 2. Fare clic su Esegui.
- 3. Selezionare un intervallo di date.
- 4. Fare clic su Esegui ora.

Oltre a generare grafici predefiniti, è anche possibile copiarli ed applicarli ad un filtro per report personalizzato che identifica specifici client, categorie, protocolli o azioni da includere. Contrassegnare come Preferiti i tipi di report che si prevede di usare frequentemente in modo da facilitarne il reperimento.

È possibile pianificare i tempi di creazione dei report di presentazione in base ad un giorno/ora specifici o ciclicamente. Per informazioni complete, vedere *Report di presentazione*, pagina 100.

I report **Investigativi** consentono all'utente di navigare lungo i dati in modalità interattiva. La pagina principale visualizza un grafico a barre con il riepilogo delle attività suddivise in base alla classe di rischio. Fare clic sui vari elementi della pagina per aggiornare il grafico o per ottenere una presentazione diversa dei dati.

 Fare clic sul nome della classe e quindi selezionare un livello più dettagliato relativamente a quella classe di rischio. Ad esempio, per la classe di rischio Responsabilità legale, si può scegliere di visualizzare le attività suddivise in base all'utente.

- Fare clic sul nome di un utente nel grafico così generato per visualizzare ulteriori informazioni su quell'utente.
- Scegliere un'opzione diversa dall'elenco Utilizzo Internet per per cambiare il grafico di riepilogo a barre.
- Riempire i campi sopra il grafico a barre per visualizzare simultaneamente due livelli di informazione. Ad esempio, iniziando da un grafico di riepilogo per le categorie, si può scegliere **10**, **Utente** e **5** per visualizzare le attività relative ai 5 utenti principali all'interno delle 10 categorie principali.
- Fare clic su una barra o su un numero per aprire un report dettagliato su quell'elemento (classe di rischio, categoria, utente o altro).
- Fare clic su **Report preferiti** per salvare un formato di report particolarmente utile per un uso futuro, o per generare un report Preferito salvato in precedenza.

Le possibilità sono pressoché infinite. Vedere *Report investigativi*, pagina 119 per dettagli sulle numerose modalità di visualizzazione dei dati relativi all'uso di Internet.

Che cos'è il tempo di navigazione in Internet?

Argomenti correlati:

- Processi del database, pagina 329
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334

È possibile generare sia report di presentazione che report investigativi basati sul tempo di navigazione in Internet (IBT – Internet Browse Time), ossia la durata di tempo che un individuo passa accedendo ai siti Web. Nessun programma di software può rilevare la durata esatta di tempo che una persona passa nella navigazione di un determinato sito, dopo avervi acceduto. Una persona può aprire un sito, visualizzarlo per alcuni secondi e quindi rispondere a una telefonata prima di richiedere un altro sito. Un'altra persona potrebbe passare diversi minuti a leggere il contenuto di un sito prima di accedere al sito successivo.

Il software Websense include un processo del database di registrazione che calcola il tempo di navigazione in Internet (IBT) usando una formula basata su determinati valori configurabili. Questo processo entra in esecuzione una volta al giorno, per cui le informazioni sui tempi di navigazione potrebbero venire generate in ritardo rispetto al tempo della loro registrazione.

Ai fini del calcolo dei tempi di navigazione, una sessione Internet inizia nel momento in cui l'utente apre un browser. Continua fino a quando quell'utente non richiede, almeno ogni 3 minuti, l'accesso ad altri siti Web. (Questa soglia predefinita, associata a un presunto tempo di lettura, è configurabile.)

La sessione in Internet termina quando sono passati più di 3 minuti senza che l'utente abbia richiesto l'accesso a un altro sito. Il software Websense calcola la durata in

tempo totale della sessione, iniziata al momento della prima richiesta e conclusa 3 minuti dopo l'ultima richiesta.

Se l'utente inoltra un'altra richiesta dopo più di 3 minuti, inizia una nuova sessione. Normalmente il tempo di navigazione di un utente comprende molteplici sessioni in un giorno.

Vedere *Processi del database*, pagina 329 e *Configurazione delle opzioni sui tempi di navigazione in Internet*, pagina 334 per informazioni sul processo di calcolo dei tempi di navigazione in Internet e sulle opzioni di configurazione disponibili.

Report di presentazione

Argomenti correlati:

- Copia di un report di presentazione, pagina 103
- Gestione dei Preferiti, pagina 110
- Generazione dei report di presentazione, pagina 111
- Pianificazione dei report di presentazione, pagina 112
- Visualizzazione dell'elenco dei processi pianificati, pagina 117

La pagina **Creazione report > Report di presentazione** include un elenco di grafici e di report tabulari predefiniti che riportano informazioni specifiche ricavate dal database di registrazione (vedere *Introduzione del database di registrazione*, pagina 328). Selezionare un report da questo Catalogo report per visualizzare una breve descrizione.

Si può copiare un report predefinito e personalizzare il filtro del report, specificando client, categorie, protocolli e azioni da includere. È possibile contrassegnare come Preferiti i report usati più di frequente per facilitarne il reperimento.

Si può generare un report in qualsiasi momento oppure pianificare la creazione dei report selezionati in base a un determinato ritardo o una determinata periodicità. Scegliere il formato di output e distribuire i report pianificati a un gruppo selezionato di destinatari.

Se si genera un report direttamente dalla pagina Report di presentazione in formato HTML, il report non viene salvato quando ci si sposta a una pagina diversa. Se si genera e si visualizza immediatamente un report in formato PDF o XLS, il report non viene salvato automaticamente quando si chiude il programma di visualizzazione usato (Adobe Reader o Microsoft Excel).

In alternativa, si può scegliere di salvare il file PDF o XLS anziché visualizzarlo immediatamente, o si può usare la funzione Salva del programma di visualizzazione. In questi casi, accertarsi di eliminare o di spostare periodicamente i file dei report per evitare problemi di disponibilità di spazio sul disco.

I report pianificati vengono automaticamente salvati nella seguente directory:

```
<install path>\ReportingOutput
```

Il percorso predefinito di installazione è C:\Programmi\Websense.

Se un report di presentazione pianificato è stato generato, il file del report, dal nome **presentationreport_0**, viene inviato ai destinatari in allegato ad una e-mail. Il numero cambia incrementalmente per riflettere il numero di report allegati. Tenere presente che il nome dell'allegato non corrisponde al nome del file archiviato nella directory ReportingOutput. Per reperire un report specifico in questa directory, cercare i file creati alla data di esecuzione del processo pianificato.

I report vengono automaticamente eliminati dalla directory ReportingOutput dopo 15 giorni. Se si vuole conservare i report per un periodo di tempo più lungo, includerli nella propria routine di backup oppure pianificarne la generazione e salvare i file inviati via e-mail in un percorso che consenta un'archiviazione a lungo termine.

A seconda del numero di report generati giornalmente, i relativi file possono occupare uno spazio considerevole su disco. Verificare che esista una quantità di spazio sufficiente sul disco fisso del computer in cui è installato Websense Manager. Se le dimensioni della directory ReportingOutput superano un determinato limite prima che i file vengano eliminati automaticamente, è possibile eliminarli manualmente.

Il software Websense genera il report nel formato di scelta: PDF (Adobe Reader), XLS (Microsoft Excel) o HTML. Se si sceglie il formato HTML, il report viene visualizzato nel riquadro del contenuto di Websense Manager. Questi report non possono venire stampati o salvati in un file. Per stampare o salvare un report in un file, scegliere un formato di output in PDF o XLS.

Se si sceglie un formato PDF o XLS, si può scegliere se salvare il file del report su disco o se visualizzarlo in una finestra separata.

Importante

Per visualizzare i report di presentazione in formato PDF, occorre aver installato Adobe Reader v7.0, o versione successiva, nel computer da cui si accede a Websense Manager.

Per visualizzare i report di presentazione in formato XLS, occorre aver installato Microsoft Excel 2003 o versione successiva, nel computer da cui si accede a Websense Manager.

Nella pagina Report di presentazione, navigare nel Catalogo report e selezionare il report desiderato. Usare quindi i comandi disponibili nella pagina per generare il

report, creare una copia per la quale si può personalizzare il filtro di report, ed altro ancora.

Pulsante	Azione
Mostra solo preferiti	Selezionare questa opzione per definire che il Catalogo report deve visualizzare soltanto i report contrassegnati come Preferiti.
	Deselezionare questa opzione per ripristinare l'elenco completo dei report.
Modifica filtro di report	Questa opzione, disponibile soltanto se si è selezionata la copia di un report predefinito, consente di selezionare specifici categorie, protocolli, utenti e azioni da includere nel report. Vedere <i>Copia di un report di presentazione</i> , pagina 103.
Copia	Utilizzato per creare una copia del report selezionato e aggiungerlo al Catalogo report come report personalizzato. Vedere <i>Copia di un report di presentazione</i> , pagina 103. Selezionare il report personalizzato e definire quindi specifici parametri da applicare a questo report facendo clic su Modifica filtro di report .
Preferiti	Utilizzato per contrassegnare come Preferito il report selezionato oppure eliminare la sua designazione di report Preferito. Vedere <i>Gestione dei Preferiti</i> , pagina 110.
	Il Catalogo report visualizza un simbolo a stella accanto ai nomi dei report contrassegnati come Preferiti. Utilizzare la casella di controllo Mostra solo preferiti per definire i report da includere nel Catalogo report.
Elimina	Utilizzato per eliminare la copia del report selezionata dal Catalogo report. Non è consentito eliminare report predefiniti installati insieme al software.
	Se il report eliminato è incluso in un processo pianificato, continuerà ad essere generato da quel processo.
Esegui	Genera il report selezionato dopo aver definito l'intervallo di date e il formato di output. Vedere <i>Generazione dei report di presentazione</i> , pagina 111.
	Per la gestione di altri aspetti del report personalizzato (copia di un report predefinito), vedere <i>Copia di un report di presentazione</i> , pagina 103.
	Per pianificare la generazione di un report in base a diversi orari o a una pianificazione a periodicità regolare, fare clic su Pianificatore.

I pulsanti sopra la pagina offrono ulteriori opzioni applicabili ai report di presentazione.

Pulsante	Azione
Coda processi	Visualizza una pagina in cui vengono elencati tutti i processi pianificati che sono già stati creati, insieme allo stato corrente di ciascun processo. Vedere <i>Visualizzazione</i> <i>dell'elenco dei processi pianificati</i> , pagina 117.
Pianificatore	Consente di definire un processo contenente uno o più report e la cui esecuzione è prevista ad un'ora specifica o in base ad una periodicità regolare pianificata. Vedere <i>Pianificazione</i> <i>dei report di presentazione</i> , pagina 112.

Copia di un report di presentazione

Argomenti correlati:

- Definizione del filtro per report, pagina 104
- *Report di presentazione*, pagina 100

Inizialmente la pagina **Report di presentazione** visualizza il Catalogo report con un elenco di tutti i report predefiniti installati con il software. È possibile generare questi report per un periodo di tempo specifico selezionando un report e quindi facendo clic su Esegui.

Questi report predefiniti possono anche venire usati come modelli e possono venire copiati per creare un filtro di report personalizzato. Si può ad esempio creare un filtro di report per determinare quali utenti, categorie, protocolli e azioni debbano venire inclusi quando si genera un report dalla copia eseguita.

Dopo aver copiato un report e modificato il filtro del report, è possibile copiare il nuovo report per creare variazioni basate su quella copia.

- 1. Selezionare un report dal Catalogo report.
- 2. Fare clic su Copia.

Nel Catalogo report, viene visualizzato un duplicato del nome del report insieme a un codice che indica che si tratta di una copia.

3. Selezionare la copia nel Catalogo report e fare quindi clic su **Modifica filtro di report** per modificare gli elementi del report. Vedere *Definizione del filtro per report*, pagina 104.

Definizione del filtro per report

Argomenti correlati:

- Copia di un report di presentazione, pagina 103
- Generazione dei report di presentazione, pagina 111

I filtri del report consentono di determinare le informazioni da includere in un report. Ad esempio, è possibile scegliere di limitare un report a determinati client, categorie, classi di rischio o protocolli o addirittura a determinate azioni di filtraggio (autorizza, blocca, e così via). È anche possibile assegnare un nuovo nome e una descrizione alla voce del Catalogo report, specificare un logo personalizzato da inserire e impostare altre opzioni tramite il filtro del report.



L'uso di un logo personalizzato richiede un certo livello di preparazione prima di poter definire il filtro del report. Occorre creare il grafico desiderato in un formato grafico supportato e copiare il file nel percorso desiderato. Vedere *Personalizzazione del logo inserito nel report*, pagina 109.

Le opzioni disponibili nel filtro dipendono dal report selezionato. Ad esempio, se si seleziona un report con informazioni sui gruppi, come ad esempio Gruppi principali bloccati per richieste, è possibile definire quali gruppi debbano venire inclusi nel report, ma non è tuttavia possibile scegliere singoli utenti.

Il filtro per i report predefiniti non può essere modificato. È possibile modificare il filtro per la copia di un report predefinito:

1. Selezionare un report da Catalogo report.

Se il pulsante Modifica filtro di report è disattivo, procedere al punto 2.

Se il pulsante Modifica filtro di report è attivo, procedere al punto 3.

2. Fare clic su Copia per creare una copia da personalizzare.

Nel Catalogo report, viene visualizzato un duplicato del nome del report insieme a un codice che indica che si tratta di una copia.

3. Fare clic sul pulsante Modifica filtro di report.

Viene aperta la pagina Filtro di report, con schede separate per la gestione di diversi elementi del report. Selezionare le opzioni appropriate in ciascuna scheda e fare quindi clic su **Avanti** per portarsi alla scheda successiva. Per istruzioni dettagliate, vedere :

- Selezione dei client da includere in un report, pagina 105
- Selezione delle categorie da includere in un report, pagina 106
- Selezione dei protocolli da includere in un report, pagina 107
- Selezione delle azioni da includere in un report, pagina 107

- Impostazione delle opzioni per i report, pagina 108
- 4. Nella scheda **Conferma**, scegliere se eseguire o se pianificare la generazione del report, oltre a salvare il relativo filtro. Vedere *Conferma della definizione dei filtri di report*, pagina 110.

Selezione dei client da includere in un report

Argomenti correlati:

- Selezione delle categorie da includere in un report, pagina 106
- Selezione dei protocolli da includere in un report, pagina 107
- Selezione delle azioni da includere in un report, pagina 107
- Impostazione delle opzioni per i report, pagina 108
- Conferma della definizione dei filtri di report, pagina 110

La scheda **Client** della pagina Report di presentazione > Filtro di report consente di determinare i client da includere nel report. È possibile selezionare almeno un tipo di client per ciascun report. Ad esempio, non è possibile selezionare determinati utenti e determinati gruppi per lo stesso report.

Se la definizione del report specifica un tipo di client particolare, è possibile scegliere dei client di quel tipo o dei client che rappresentano un gruppo più esteso. Ad esempio, se si seleziona un filtro basato su Gruppi principali bloccati per richieste, è possibile selezionare quali gruppi, domini o unità organizzative debbano venire inclusi nel report, ma non è tuttavia possibile selezionare singoli utenti.

Non è necessario eseguire selezioni in questa scheda se si vogliono originare dei report su tutti i client rilevanti.

- 1. Selezionare un tipo di client standard dal menu a discesa.
- 2. Definire il numero massimo di risultati di ricerca dall'elenco Ricerca limite.

A seconda del traffico attivo nella propria organizzazione, potrebbe esserci un grande numero di utenti, gruppi o domini nel database di registrazione. Questa opzione gestisce la lunghezza dell'elenco dei risultati e il tempo necessario a visualizzare i risultati di una ricerca.

3. Inserire uno o più caratteri per la ricerca e fare quindi clic su Cerca.

Utilizzare l'asterisco (*) come carattere jolly per i caratteri mancanti. Ad esempio, G*a potrebbe restituire Gianna, Gaia, Graziella, Gabriella, Giovanna e così via.

Definire la propria stringa di ricerca con attenzione per essere certi che i risultati desiderati siano compresi nel numero selezionato per limitare la ricerca.

- 4. Evidenziare una o più voci dell'elenco dei risultati e fare clic sul pulsante rivolto verso destra (>) per spostarle nell'elenco **Elementi selezionati**.
- 5. Ripetere le operazioni descritte ai punti 2-4, come necessario, per condurre altre ricerche ed aggiungere altri client all'elenco Elementi selezionati.

6. Una volta completate le selezioni, fare clic su **Avanti** per aprire la scheda Categorie. Vedere Selezione delle categorie da includere in un report, pagina 106.

Selezione delle categorie da includere in un report

Argomenti correlati:

- Selezione dei client da includere in un report, pagina 105 ٠
- Selezione dei protocolli da includere in un report, pagina 107
- Selezione delle azioni da includere in un report, pagina 107
- Impostazione delle opzioni per i report, pagina 108 ٠
- Conferma della definizione dei filtri di report, pagina 110

La scheda **Categorie** della pagina Report di presentazione > Filtro di report consente di determinare le informazioni da includere nel report in funzione delle categorie o delle classi di rischio. Vedere Classi di rischio, pagina 41.

Non è necessario eseguire selezioni in questa scheda se si vogliono originare dei report su tutte le categorie e le classi di rischio rilevanti.

1. Selezionare una classificazione: Categoria o Classe di rischio.

Espandere una categoria principale per visualizzare tutte le sotto-categorie. Espandere una classe di rischio per visualizzare un elenco delle categorie correntemente assegnate a quella classe di rischio.

Se il report associato è per una classe di rischio specifica, soltanto la classe di rischio rilevante e le categorie che essa rappresenta sono disponibili per la selezione.



Se si seleziona un sottogruppo di categorie per la classe di rischio indicata nel report, tenere presente la possibilità di modificare il titolo del report in modo che rifletta le selezioni eseguite.

2. Contrassegnare la casella di controllo di ogni categoria o classe di rischio da includere nel report.

Usare i pulsanti Seleziona tutto e Cancella tutto disponibili sotto l'elenco per minimizzare il numero di selezioni necessarie.

3. Fare clic sul pulsante freccia verso destra (>) per portare le selezioni eseguite nell'elenco Elementi selezionati

Se si contrassegna una classe di rischio, facendo clic sulla freccia rivolta verso destra si portano tutte le categorie associate a quella classe nell'elenco Elementi selezionati.

4. Una volta completate le selezioni, fare clic su Avanti per aprire la scheda Protocolli. Vedere Selezione dei protocolli da includere in un report, pagina 107.

Selezione dei protocolli da includere in un report

Argomenti correlati:

- Selezione dei client da includere in un report, pagina 105
- Selezione delle categorie da includere in un report, pagina 106
- Selezione delle azioni da includere in un report, pagina 107
- Impostazione delle opzioni per i report, pagina 108
- Conferma della definizione dei filtri di report, pagina 110

La scheda **Protocolli** della pagina Report di presentazione > Filtro di report consente di determinare i protocolli da includere nel report.

Non è necessario eseguire selezioni in questa scheda se si vuole originare un report su tutti i protocolli rilevanti.

- 1. Espandere e comprimere i gruppi di protocolli utilizzando l'icona accanto al nome del gruppo.
- Contrassegnare la casella di controllo di ogni protocollo da includere nel report. Usare i pulsanti Seleziona tutto e Cancella tutto disponibili sotto l'elenco per ridurre al minimo il numero di selezioni necessarie.
- 3. Fare clic sul pulsante freccia verso destra (>) per portare le selezioni eseguite nell'elenco **Elementi selezionati**.
- 4. Una volta completate le selezioni, fare clic su **Avanti** per aprire la scheda Azioni. Vedere *Selezione delle azioni da includere in un report*, pagina 107.

Selezione delle azioni da includere in un report

Argomenti correlati:

- Selezione dei client da includere in un report, pagina 105
- Selezione delle categorie da includere in un report, pagina 106
- Selezione dei protocolli da includere in un report, pagina 107
- Impostazione delle opzioni per i report, pagina 108
- Conferma della definizione dei filtri di report, pagina 110

La scheda **Azioni** della pagina Report di presentazione > Filtro di report consente di determinare in modo preciso le azioni di filtraggio, come ad esempio quelle consentite dal filtro per restrizioni di accesso, bloccato a tempo, ecc, che devono venire incluse nel report. Se il report specifica un particolare tipo di azione, come ad esempio Bloccato, si sarà limitati a selezionare azioni di quel tipo per il report in questione.

Non è necessario eseguire selezioni in questa scheda se si vuole originare un report su tutte le azioni rilevanti.

- 1. Espandere e comprimere i gruppi di azioni utilizzando l'icona accanto al nome del gruppo.
- 2. Contrassegnare la casella di controllo di ogni azione da includere nel report.

Usare i pulsanti **Seleziona tutto** e **Cancella tutto** disponibili sotto l'elenco per ridurre al minimo il numero di selezioni necessarie.

- 3. Fare clic sul pulsante freccia verso destra (>) per portare le selezioni eseguite nell'elenco **Elementi selezionati**.
- 4. Una volta completate le selezioni, fare clic su **Avanti** per aprire la scheda Opzioni. Vedere *Impostazione delle opzioni per i report*, pagina 108.

Impostazione delle opzioni per i report

Argomenti correlati:

- Personalizzazione del logo inserito nel report, pagina 109
- Selezione dei client da includere in un report, pagina 105
- Selezione delle categorie da includere in un report, pagina 106
- Selezione dei protocolli da includere in un report, pagina 107
- Selezione delle azioni da includere in un report, pagina 107
- Impostazione delle opzioni per i report, pagina 108
- Conferma della definizione dei filtri di report, pagina 110

La scheda **Opzioni** della pagina Report di presentazione > Modifica filtro di report consente di configurare diversi aspetti del report.

1. Modificare **Nome catalogo di report** che deve apparire nel Catalogo report. Il nome può contenere fino a un massimo di 85 caratteri.

Questo nome non appare nel report; viene usato soltanto per identificare una combinazione unica di formato e filtro per report nel Catalogo report.

- 2. Modificare il **Titolo report** visualizzato nel report. Il titolo può contenere fino a un massimo di 85 caratteri.
- 3. Modificare la **Descrizione** che deve apparire nel Catalogo report. La descrizione può contenere fino a un massimo di 336 caratteri.

La descrizione deve poter agevolare l'utente a identificare questa combinazione unica di formato e filtro di report nel Catalogo report.

4. Selezionare un logo che deve apparire nel report.

Vengono elencati tutti i file di immagine supportati nella directory appropriata. Vedere *Personalizzazione del logo inserito nel report*, pagina 109.

5. Contrassegnare la casella di controllo **Salva come Preferito** affinché il report venga incluso nell'elenco dei Preferiti.
Il Catalogo report mostra un simbolo di stella accanto ai report Preferiti. È possibile selezionare **Mostra solo preferiti** nella pagina Catalogo report per ridurre il numero di report elencati e consentire quindi un accesso più rapido a un determinato report.

6. Contrassegnare la casella di controllo **Mostra solo i primi** ed inserire un numero compreso tra 1 e 20 per limitare il numero di elementi visualizzati.

Questa opzione è disponibile soltanto se il report selezionato è formattato come un report Primi n elementi ed è designato a visualizzare un numero limitato di elementi. La limitazione del numero di eventi visualizzati dipende dal tipo di report. Ad esempio, per un report Categorie principali visitate, questa voce determina quante categorie devono apparire nel report.

7. Una volta completate le immissioni e le selezioni, fare clic su **Avanti** per aprire la scheda Conferma. Vedere *Conferma della definizione dei filtri di report*, pagina 110.

Personalizzazione del logo inserito nel report

I report di presentazione predefiniti visualizzano il logo di Websense nell'angolo superiore sinistro. Se si copia un report predefinito e si definisce il suo filtro per report, è possibile scegliere un logo diverso.

1. Creare un file di immagine in uno dei formati seguenti:

•	.bmp	٠	.jpg
٠	.gif	٠	.jpeg
٠	.jfif	٠	.png
•	.jpe	٠	.ttf

- 2. Usare un massimo di 25 caratteri per il nome del file di immagine, inclusa l'estensione.
- 3. Portare il file immagine nella directory seguente:

<install path>\Manager\ReportingTemplates\images

Il percorso di installazione predefinito è C:\Programmi\Websense.

Tutti i file di immagine supportati e contenuti in questa directory appaiono automaticamente nell'elenco a discesa della scheda Opzioni della pagina Filtro di report. L'immagine viene automaticamente ridimensionata in scala in modo da poter essere inserita nello spazio designato per il logo. (Vedere *Impostazione delle opzioni per i report*, pagina 108).

Nota

Non eliminare da questa directory le immagini attive nei filtri di report. Se il file del logo specificato risulta mancante, il report non può essere generato.

Conferma della definizione dei filtri di report

Argomenti correlati:

- Selezione dei client da includere in un report, pagina 105
- Selezione delle categorie da includere in un report, pagina 106
- Selezione dei protocolli da includere in un report, pagina 107
- Selezione delle azioni da includere in un report, pagina 107
- Impostazione delle opzioni per i report, pagina 108

La scheda **Categorie** della pagina Report di presentazione > Filtro di report visualizza il nome e la descrizione che appare nel Catalogo report e consente di scegliere come procedere.

1. Rivedere il Nome e la Descrizione.

Se non è necessario apportare modifiche, fare clic su **Indietro** per ritornare alla scheda Opzioni nella quale si possono apportare le modifiche necessarie. (Vedere *Impostazione delle opzioni per i report*, pagina 108).

2. Indicare come si vuole procedere:

Opzione	Descrizione
Salva	Salva il filtro di report e ritorna al Catalogo report. Vedere <i>Report di presentazione</i> , pagina 100.
Salva e esegui	Salva il filtro di report e apre la pagina Esegui report. Vedere <i>Generazione dei report di presentazione</i> , pagina 111.
Salva e pianifica	Salva il filtro di report e apre la pagina Pianifica report. Vedere <i>Pianificazione dei report di presentazione</i> , pagina 112.

3. Fare clic su **Fine** per implementare la selezione eseguita al punto 2.

Gestione dei Preferiti

Argomenti correlati:

- Report di presentazione, pagina 100
- Generazione dei report di presentazione, pagina 111
- Pianificazione dei report di presentazione, pagina 112

È possibile contrassegnare come Preferito qualsiasi report di presentazione, sia predefinito che personalizzato. Usare questa opzione per identificare i report generati più di frequente e che si vuole poter reperire rapidamente nel Catalogo report.

- 1. Nella pagina **Report di presentazione** evidenziare un report che si genera frequentemente o che si vuole reperire rapidamente.
- 2. Fare clic su Preferito.

Viene visualizzato un simbolo a stella accanto ai nomi dei report Preferiti per consentire di identificarli rapidamente quando tutti i report vengono visualizzati.

3. Contrassegnare la casella di controllo **Mostra solo preferiti** sopra il Catalogo report per generare un elenco che comprenda soltanto i Preferiti. Deselezionare questa casella di controllo per ripristinare l'elenco completo dei report.

Se le proprie necessità cambiano ed un report Preferito non viene più usato frequentemente, è possibile annullare la designazione di Preferito.

- 1. Evidenziare un report che mostri il simbolo di stella come identificazione di report Preferito.
- 2. Fare clic su **Preferito**.

Il simbolo di stella viene eliminato dal nome del report nel Catalogo report. Il report non viene più visualizzato nell'elenco quando si sceglie l'opzione **Mostra solo preferiti**.

Generazione dei report di presentazione

Argomenti correlati:

- *Report di presentazione*, pagina 100
- Pianificazione dei report di presentazione, pagina 112

La generazione immediata di un singolo report comporta l'esecuzione delle operazioni descritte di seguito.



Nota

Prima di generare un report in formato PDF, occorre aver installato Adobe Reader v7.0, o versione successiva, nel computer da cui si accede a Websense Manager.

Prima di generare un report in formato XLS, occorre aver installato Microsoft Excel 2003 o versione successiva, nel computer da cui si accede a Websense Manager.

Se il software sopra indicato non è installato nel computer, si ha la possibilità di salvare il file.

È anche possibile creare dei processi che consistono in uno o più report da generare una volta sola o ciclicamente utilizzando la funzione di pianificazione dei report di presentazione. Vedere *Pianificazione dei report di presentazione*, pagina 112.

1. Nella pagina **Report di presentazione**, evidenziare un report nell'albero del Catalogo report e fare quindi clic su **Esegui**.

- 2. Selezionare la Data di inizio e Data di fine per i dati del report.
- 3. Selezionare un Formato output per il report.

Formato	Descrizione
PDF	Portable Document Format. I file PDF vengono visualizzati in Adobe Reader.
HTML	HyperText Markup Language. I file HTML possono venire visualizzati direttamente nel browser Internet Explorer o Firefox.
XLS	Foglio elettronico Excel . I file XLS vengono visualizzati in Microsoft Excel.

- 4. Se si è selezionato un report **Primi n elementi**, scegliere il numero di elementi da includere nel report.
- 5. Fare clic su **Esegui**.

I report HTML appaiono nel riquadro del contenuto. Se si è scelto un formato PDF o XLS, si può scegliere se aprire il report in una finestra separata o salvare il report su disco.

6. Per stampare un report, usare l'opzione stampa disponibile nel programma usato per la visualizzazione del report.

Per ottenere i risultati migliori, generare un output in PDF o XLS per la stampa. Usare quindi le opzioni di stampa disponibili in Adobe Reader o Microsoft Excel rispettivamente.

È possibile salvare un report in formato PDF o XLS usando la funzione Salva, disponibile in Adobe Reader o Microsoft Excel.

Pianificazione dei report di presentazione

Argomenti correlati:

- Report di presentazione, pagina 100
- Generazione dei report di presentazione, pagina 111
- Visualizzazione dell'elenco dei processi pianificati, pagina 117
- Copia di un report di presentazione, pagina 103

È possibile generare i report di presentazione quando necessario, oppure si può usare la pagina **Report di presentazione > Pianificatore** per creare dei processi che definiscano una pianificazione dei tempi di esecuzione di uno o più report.

I report generati in base a processi pianificati vengono distribuiti a uno o più destinatari via e-mail. Quando si pianificano i processi, valutare se il proprio server e-mail è in grado di gestire le dimensioni e la quantità di report da allegare alle e-mail.

Per accedere al Pianificatore:

- Fare clic sul pulsante **Pianificatore** nell'area superiore della pagina Report di presentazione (sopra il Catalogo report).
- Quando si aggiunge o si modifica il filtro di report di un determinato report, scegliere Salva e pianifica nella scheda Conferma e fare quindi clic su Fine. (Vedere Copia di un report di presentazione, pagina 103.
- Per modificare un processo, fare clic sul collegamento con il nome di quel processo nella pagina Coda processi .
- Fare clic su Aggiungi nella pagina Coda processi per creare un nuovo processo.

La pagina Pianificatore contiene diverse schede per la selezione dei report da generare e i tempi in cui questi vanno generati. Per informazioni dettagliate, vedere .

- Impostazione della pianificazione, pagina 113
- Selezione dei report da pianificare, pagina 115
- Selezione delle opzioni di output, pagina 116
- Selezione dell'intervallo di date, pagina 115

Dopo aver creato i processi, è possibile visualizzare un elenco di processi con il loro stato corrente e altre informazioni utili. Vedere *Visualizzazione dell'elenco dei processi pianificati*, pagina 117.

Impostazione della pianificazione

Argomenti correlati:

- Pianificazione dei report di presentazione, pagina 112
- Selezione dei report da pianificare, pagina 115
- Selezione delle opzioni di output, pagina 116
- Selezione dell'intervallo di date, pagina 115

Definire un processo di creazione di report eseguibile una sola volta o ciclicamente, usando la scheda **Pianificazione** della pagina Report presentazione > Pianificatore.



Nota

Si consiglia di pianificare i processi di creazione dei report in giorni e a orari diversi per evitare di sovraccaricare il database di registrazione e di rallentare la performance della registrazione e la creazione interattiva dei report.

1. Inserire un **Nome processo** che identifichi in modo univoco il processo pianificato.

2. Selezionare un **Criterio di frequenza** e **Opzioni di frequenza** per il processo. Le opzioni disponibili dipendono dal formato selezionato.

Formato	Opzioni
Una volta	Inserire la data esatta di esecuzione del processo oppure fare clic sull'apposita icona per selezionare la data direttamente da un calendario.
Giornalmente	Non sono disponibili altre opzioni di frequenza.
Settimanale	Contrassegnare la casella di controllo di ogni giorno della settimana in cui si vuole eseguire il processo.
Mensile	Inserire le date del mese per l'esecuzione del processo. Le date devono essere costituite da un numero compreso tra 1 e 31 e devono essere separate da virgole (1,10,20)
	Per eseguire il processo in base a date consecutive ogni mese, inserire una data di inizio e di fine separate da una lineetta (3-5).

 In Pianifica orario, definire il tempo di inizio per l'esecuzione del processo. Il processo inizia alla data e all'ora impostate nel computer in cui è installato Websense Manager.



Nota

Per iniziare oggi stesso a generare i report pianificati, selezionare un'ora sufficientemente lontana da consentire di completare la definizione del processo prima del tempo di esecuzione del report.

4. In **Pianifica intervallo temporale**, selezionare una data di inizio del processo e un'opzione per la data di fine.

Opzione	Descrizione
Nessuna data di fine	Il processo continua ad essere eseguito indefinitamente, in base alla pianificazione dei tempi di esecuzione.
	Per interrompere il processo in qualsiasi momento, modificare o cancellare il processo. Vedere <i>Visualizzazione</i> <i>dell'elenco dei processi pianificati</i> , pagina 117.
Termina dopo	Selezionare il numero di volte in cui si vuole eseguire il processo. Una volta raggiunto tale numero, il processo non viene più eseguito ma rimane nella Coda processi fino a quando non viene cancellato. Vedere <i>Visualizzazione</i> <i>dell'elenco dei processi pianificati</i> , pagina 117.
Termina dopo	Definire la data in cui il processo non deve più venire eseguito. Ossia, non verrà più eseguito alla data definita o successivamente a tale data.

5. Fare clic su **Avanti** per aprire la scheda Report. Vedere *Selezione dei report da pianificare*, pagina 115.

Selezione dei report da pianificare

Argomenti correlati:

- Pianificazione dei report di presentazione, pagina 112
- Impostazione della pianificazione, pagina 113
- Selezione delle opzioni di output, pagina 116
- Selezione dell'intervallo di date, pagina 115

Usare la scheda **Seleziona report** della pagina Report di presentazione > Pianificatore, per scegliere i report da includere nel processo.

- 1. Evidenziare un report da includere in questo processo, scegliendolo dall'albero del Catalogo report.
- 2. Fare clic sul pulsante freccia verso destra (>) per portare il report nell'elenco Elementi selezionati.
- 3. Ripetere le operazioni descritte ai punti 1 e 2 fino a quando tutti i report da includere in questo job non vengono visualizzati nell'elenco **Elementi** selezionati.
- 4. Fare clic su **Avanti** per aprire la scheda Intervallo di date. Vedere *Selezione dell'intervallo di date*, pagina 115.

Selezione dell'intervallo di date

Argomenti correlati:

- Pianificazione dei report di presentazione, pagina 112
- Impostazione della pianificazione, pagina 113
- Selezione dei report da pianificare, pagina 115
- Selezione delle opzioni di output, pagina 116

Usare la scheda **Intervallo di date** della pagina Report di presentazione > Pianificatore per scegliere l'intervallo di date per il processo. Le opzioni disponibili dipendono dalla selezione eseguita in **Intervallo di date**.

Intervallo di date	Descrizione
Tutte le date	I report includono tutte le date disponibili nel database di registrazione. Non è necessario eseguire altre selezioni.
	Se questa opzione viene usata per una ripetizione dei processi, potrebbero risultare informazioni duplicate nei report generati in esecuzioni separate.
Date specifiche	Selezionare il tempo di inizio esatto (Da) e il tempo di fine (A) per i report inclusi in questo processo.
	Questa opzione è ideale per i processi di cui si prevede un'unica esecuzione. La selezione di questa opzione con un'esecuzione ripetuta, crea report duplicati.
Date relative	Usare gli elenchi a discesa per selezionare il numero di periodi da includere nel report (Questo/a, Ultimo, Ultimi 2, e così via) e il tipo di periodo (Giorni, Settimane e Mesi). Ad esempio, il processo potrebbe fare riferimento alle Ultime 2 settimane o all'Ultimo mese.
	La Settimana rappresenta una settimana di calendario, da domenica a sabato. Il Mese rappresenta un mese di calendario. Ad esempio, Questa settimana produce un report da domenica fino ad oggi compreso; Questo mese produce un report dal primo del mese fino ad oggi compreso; Ultima settimana produce un report da domenica scorsa fino a sabato; e così via.
	Questa opzione è ideale per i processi con una pianificazione a tempi ripetuti. Consente di definire la quantità di dati da visualizzare in ogni report e di minimizzare la duplicazione di dati nei report che prevedono varie esecuzioni.

Una volta definito il range per il processo, fare clic su **Avanti** per visualizzare la scheda Output. Vedere *Selezione delle opzioni di output*, pagina 116.

Selezione delle opzioni di output

Argomenti correlati:

- Pianificazione dei report di presentazione, pagina 112
- Impostazione della pianificazione, pagina 113
- Selezione dei report da pianificare, pagina 115
- Selezione dell'intervallo di date, pagina 115

Dopo aver selezionato i report per un processo, usare la scheda **Output** per selezionare il formato di output e le opzioni di distribuzione.

1. Selezionare un formato di file per il report completato.

Formati	Descrizione
PDF	Portable Document Format. I destinatari devono disporre di Adobe Reader v7.0 o versione successiva per poter visualizzare i report in PDF.
XLS	Foglio elettronico Excel. I destinatari devono disporre di Microsoft Excel 2003 o versione successiva per poter visualizzare i report in Excel.

2. Inserire gli indirizzi e-mail per la distribuzione del report.

Inserire ciascun indirizzo in una riga separata.

- 3. Contrassegnare la casella di controllo **Personalizza oggetto e testo del messaggio e-mail**, se desiderato. Inserire quindi l'**Oggetto** e il **Corpo** del testo per la distribuzione della e-mail di questo processo.
- 4. Fare clic su **Salva processo** per salvare e implementare la definizione del processo e per visualizzare la pagina della Coda processi.
- 5. Rivedere questo processo e altri processi pianificati, se necessario. Vedere *Visualizzazione dell'elenco dei processi pianificati*, pagina 117.

Visualizzazione dell'elenco dei processi pianificati

Argomenti correlati:

- Report di presentazione, pagina 100
- Pianificazione dei report di presentazione, pagina 112
- Selezione delle opzioni di output, pagina 116
- Pianificazione dei report investigativi, pagina 141

La pagina **Report di presentazione > Coda processi** contiene un elenco dei processi pianificati, creati per i report di presentazione. L'elenco riporta lo stato corrente di ogni processo nonché altre informazioni utili riguardo al processo stesso, come ad es. la frequenza della sua esecuzione. Da questa pagina è anche possibile aggiungere ed eliminare dei processi pianificati, sospendere un processo in corso, ed altro ancora.

(Per rivedere i processi pianificati per la creazione di report investigativi, vedere *Gestione dei processi pianificati per i report investigativi*, pagina 144.)

Colonna	Descrizione
Nome del processo	Il nome assegnato al momento della creazione del processo.
Stato	 Può essere uno dei seguenti: ABILITATO indica un processo che viene eseguito in base a uno schema di ricorrenze prestabilite. DISABILITATO indica un processo inattivo e che non viene eseguito.
Frequenza	Lo schema della ricorrenza di esecuzione (Una volta, Giornalmente, Settimanalmente, Mensilmente) definito per questo processo.
Cronologia	Fare clic sul collegamento Dettagli per aprire la pagina Cronologia processo per il processo selezionato. Vedere <i>Visualizzazione di Cronologia processo</i> , pagina 119.
Prossima pianificazione	La data e l'ora dell'esecuzione successiva prevista.
Titolare	Il nome utente dell'amministratore che ha pianificato il processo.

L'elenco riporta le informazioni seguenti per ogni processo.

Utilizzare le opzioni disponibili nella pagina per la gestione dei processi. Alcuni di questi pulsanti richiedono che si contrassegnino innanzi tutto le caselle di controllo accanto al nome di ciascun processo che si vuole includere.

Opzione	Descrizione
Nome processo, collegamento	Apre la pagina Pianificatore nella quale si può modificare la definizione del processo. Vedere <i>Pianificazione dei report di presentazione</i> , pagina 112.
Aggiungi processo	Apre la pagina Pianificatore nella quale si può creare la definizione dei un nuovo processo. Vedere <i>Pianificazione dei report di presentazione</i> , pagina 112.
Elimina	Elimina da Coda processi tutti i processi selezionati nell'elenco. Dopo aver eliminato un processo, questo non può essere ripristinato.
	Per interrompere temporaneamente un determinato processo, usare il pulsante Disabilita .
Esegui ora	Avvia immediatamente l'esecuzione dei processi selezionati nell'elenco. Questa esecuzione è in aggiunta alle esecuzioni già pianificate.
Abilita	Attiva nuovamente i processi disattivati che sono stati selezionati nell'elenco. Il processo inizia la sua esecuzione in base alla pianificazione di esecuzione.
Disabilita	Interrompe l'esecuzione dei processi attivati che sono stati selezionati nell'elenco. Usare questa opzione per sospendere temporaneamente il processo che si potrebbe voler ripristinare in futuro.

Visualizzazione di Cronologia processo

Argomenti correlati:

- *Pianificazione dei report di presentazione*, pagina 112
- Visualizzazione dell'elenco dei processi pianificati, pagina 117

Utilizzare la pagina **Report di presentazione > Coda processi > Cronologia processi** per visualizzare le informazioni relative ai tentativi recenti di eseguire il processo selezionato. La pagina elenca ciascun report separatamente e fornisce le informazioni seguenti:

Colonna	Descrizione
Nome del report	Il titolo stampato sul report.
Data di inizio	La data e l'ora di inizio della sua esecuzione.
Data di fine	La data e l'ora di completamento del report.
Stato	Indica il completamento o non completamento del report.
Messaggio	Include informazioni rilevanti sul processo, come ad esempio se il report è stato inviato tramite e-mail.

Report investigativi

Argomenti correlati:

- Report di riepilogo, pagina 121
- Report di riepilogo multi-livello, pagina 126
- Report dettagliati flessibili, pagina 127
- Report Dettagli attività utente, pagina 132
- *Report standard*, pagina 137
- *Report investigativi preferiti*, pagina 138
- Pianificazione dei report investigativi, pagina 141
- Report casi atipici, pagina 144
- Output su file, pagina 145
- Collegamento con il database e impostazioni predefinite dei report, pagina 342

Utilizzare la pagina **Creazione report > Report investigativi** per analizzare in modalità interattiva l'attività di filtraggio dell'uso di Internet .

La pagina Report investigativi visualizza inizialmente un report di riepilogo delle attività suddivise in base alla classe di rischio. Nel report di riepilogo si può fare clic sui collegamenti e sugli elementi disponibili per esplorare aree di interesse e acquisire un visione d'insieme dell'uso di Internet all'interno della propria organizzazione. Vedere *Report di riepilogo*, pagina 121.

Report di riepilogo multi-livello (vedere *Report di riepilogo multi-livello*, pagina 126) e report dettagliati flessibili (vedere *Report dettagliati flessibili*, pagina 127) consentono di analizzare le informazioni riportate da prospettive diverse.

È possibile accedere ad altri tipi di visualizzazione dei report e a funzioni relative ai report investigativi dai collegamenti disponibili nell'area superiore della pagina. Vedere la tabella qui sotto per un elenco dei collegamenti e delle funzioni a cui si può accedere. (Non tutti i collegamenti sono disponibili in tutte le pagine.)

Opzione	Azione
Dettaglio attività utente giorno/mese	Visualizza una finestra di dialogo che consente di definire un report riguardante l'attività specifica di un utente, nel corso di una giornata o di un mese. Per ulteriori informazioni, vedere <i>Report Dettagli attività utente</i> , pagina 132.
Report standard	Visualizza un elenco di report predefiniti in modo da poter facilmente visualizzare una combinazione specifica dei dati presentati. Vedere <i>Report standard</i> , pagina 137.
Report preferiti	Consente di salvare il report in uso come un Preferito e di visualizzare un elenco di report Preferiti che si può generare o pianificare. Vedere <i>Report investigativi preferiti</i> , pagina 138.
Coda processo	Visualizza un elenco dei processi pianificati per i report investigativi . Vedere <i>Pianificazione dei report investigativi</i> , pagina 141.
Casi atipici	Visualizza report che mostrano un uso di Internet particolarmente fuori dalla norma. Vedere <i>Report casi</i> <i>atipici</i> , pagina 144.
Opzioni	Visualizza la pagina per la selezione di un database di registrazione diverso per la creazione dei report. La pagina Opzioni consente anche di personalizzare determinate funzioni di creazione dei report, come ad es. il periodo di tempo indicato inizialmente nei report di riepilogo e le colonne predefinite per i report dettagliati. Vedere <i>Collegamento con il database e impostazioni predefinite dei</i> <i>report</i> , pagina 342.

Opzione	Azione
	Fare clic su questo pulsante, a destra dei campi di ricerca, per esportare il report corrente in un file elettronico compatibile con Microsoft Excel.
	Verrà visualizzato un messaggio che chiede di aprire o di salvare il file. Per aprire il file, occorre aver installato Microsoft Excel 2003 o versione successiva. Vedere <i>Output</i> <i>su file</i> , pagina 145.
	Fare clic su questo pulsante, a destra dei campi di ricerca, per esportare il report corrente in un file PDF compatibile con Adobe Reader.
	Verrà visualizzato un messaggio che chiede di aprire o di salvare il file. Per aprire il file, occorre aver installato Adobe Reader 7.0 o versione successiva. Vedere <i>Output su file</i> , pagina 145.

Tenere presente che il contenuto dei report riflette le informazioni registrate nel database di registrazione. Se si disattiva la registrazione per determinati nomi utente, indirizzi IP o categorie (vedere *Configurazione di Filtering Service per la registrazione*, pagina 314), quelle informazioni non verranno incluse. Analogamente, se si disattiva una registrazione per determinati protocolli (vedere *Modifica di un filtro di protocollo*, pagina 53), non saranno disponibili richieste di tali protocolli. Se si vuole che i report includano sia il nome del domini (www.dominio.it) che il percorso a una particolare pagina del dominio (/prodotto/prodottoA), occorre registrare l'intero URL (vedere *Configurazione della registrazione di URL completi*, pagina 333).

I report investigativi di Websense sono limitati dal processore e dalla memoria disponibile nel computer in cui è installato Websense Manager, nonché da alcune risorse di rete. Alcuni report estesi potrebbero richiedere tempi di generazione molto lunghi. Il messaggio sullo stato di avanzamento include un'opzione per il salvataggio del report come un report Preferito affinché sia possibile pianificare una sua esecuzione separata. Vedere *Pianificazione dei report investigativi*, pagina 141.

Report di riepilogo

Argomenti correlati:

- *Report di riepilogo multi-livello*, pagina 126
- Report dettagliati flessibili, pagina 127
- *Report Dettagli attività utente*, pagina 132
- Report standard, pagina 137
- *Report investigativi preferiti*, pagina 138
- Pianificazione dei report investigativi, pagina 141
- Report casi atipici, pagina 144
- *Output su file*, pagina 145

Inizialmente la pagina dei report investigativi visualizza un report di riepilogo sull'uso effettuato da tutti gli utenti, in base alla classe di rischio, e mostra l'attività del giorno corrente ricavata dal database di registrazione. Il criterio di misurazione adottato per questo grafico a barre iniziale sono gli Accessi (numero di volte che il sito è stato richiesto). Per configurare il periodo di tempo relativo a questo report di riepilogo iniziale, vedere *Collegamento con il database e impostazioni predefinite dei report*, pagina 342.

Modificare rapidamente le informazioni contenute nel report oppure approfondire i dettagli del report facendo clic sui vari collegamenti e opzioni disponibili nella pagina.

1. Selezionare una delle seguenti opzioni dall'elenco Misura.

Opzione	Descrizione
Accessi	Il numero di richieste di un determinato URL.
	In base alla configurazione definita per il Log Server, si potrebbe trattare di accessi veri e propri che comportano la registrazione di un record separato per l'accesso a ciascun elemento che fa parte di un sito richiesto, o potrebbe trattarsi di visite, ossia l'unificazione di diversi elementi del sito in un unico record di registrazione. Vedere <i>Configurazione dei file</i> <i>cache di registro</i> , pagina 321.
Larghezza di banda [KB]	La quantità di dati, in kilobyte, in riferimento sia alla richiesta iniziale ricevuta dall'utente sia la risposta ricevuta dal sito Web. Questa è rappresentata dal totale dei valori di Inviati e Ricevuti.
	Tenere presente che alcuni prodotti di integrazione non inviano queste informazioni al software Websense. Due esempi sono il Check Point FireWall-1 e Cisco PIX Firewall. Se i prodotti di integrazione non inviano queste informazioni e Websense Network Agent è stato installato, attivare l'opzione Registra richieste HTTP affinché il NIC
	appropriato sia in grado di creare report con informazioni sulla larghezza di banda. Vedere <i>Configurazione delle</i> <i>impostazioni della scheda dell'interfaccia di rete (NIC)</i> , pagina 355.
Inviati [KB]	Il numero di kilobyte inviati in base al tipo di richiesta di uso di Internet. Questo rappresenta la quantità di dati trasmessi, che potrebbe essere associata ad una semplice richiesta di URL o a un invio più consistente se l'utente si registra, ad esempio, in un sito Web.

Opzione	Descrizione
Ricevuti [KB]	Il numero di kilobyte ricevuti in risposta alla richiesta. Questo include tutti i testi, le immagini grafiche e gli script che fanno parte del sito.
	Per i siti bloccati, il numero di kilobyte varia in funzione del software che crea il record di registrazione. Quando Websense Network Agent registra i record, il numero di byte ricevuti per un sito bloccato rappresenta le dimensioni della pagina di blocco di Websense.
	Se i record di registrazione vengono creati da Websense Security Gateway, a seguito di una scansione in tempo reale, i kilobyte ricevuti rappresentano le dimensioni della pagina scannerizzata. Per ulteriori informazioni sulla scansione in tempo reale, vedere <i>Analisi del contenuto con le opzioni di</i> <i>Tempo reale</i> , pagina 149.
	Se un altro prodotto d integrazione crea i record di registrazione, i kilobyte ricevuti per un sito bloccato potrebbero essere pari a (0), potrebbero rappresentare le dimensioni della pagina di blocco o potrebbero essere costituiti da un valore ottenuto dal sito richiesto.
Tempo di navigazione	Una stima della quantità di tempo passato a visitare il sito. Vedere <i>Che cos'è il tempo di navigazione in Internet?</i> , pagina 99.

2. Modificare il raggruppamento primario del report selezionando un'opzione dall'elenco **Visualizza utilizzo di Internet per**, visualizzato sopra il report.

Le opzioni variano in base al contenuto del database di registrazione e ad altre considerazioni di rete. Ad esempio, se esiste soltanto un gruppo o un dominio nel database di registrazione, i Gruppi e i Domini non vengono inclusi nell'elenco. Analogamente, se esistono troppi utenti (oltre 5.000) o gruppi (oltre 3.000), queste opzioni non vengono visualizzate. (È possibile configurare alcuni di questi limiti. Vedere *Opzioni di visualizzazione e di output*, pagina 344.)

3. Fare clic su un nome nella colonna sinistra (o sulla freccia accanto al nome) per visualizzare un elenco di opzioni, come ad esempio in base all'utente, al dominio o all'azione.

Le opzioni disponibili sono simili a quelle elencate in Visualizza uso di Internet per, e personalizzate al fine di costituire un sotto-gruppo rappresentativo del contenuto correntemente visualizzato.

Nota

A volte un'opzione, come ad esempio Utente o Gruppo, viene visualizzata con le lettere in rosso . In questo caso, la selezione di quell'opzione potrebbe produrre un report molto esteso e molto lento da generare. Considerare la possibilità di analizzare con attenzione i dettagli prima di selezionare quell'opzione.

4. Selezionare una di queste opzioni per generare un nuovo report di riepilogo che includa le informazioni selezionate per la voce associata.

Ad esempio, in un report di riepilogo in base alla Classe di rischio, facendo clic su "per Utente", nella classe di rischio Responsabilità legale, si genererà un report relativo all'attività di ciascun utente nella classe di rischio Responsabilità legale.

- 5. Fare clic su una nuova voce della colonna sinistra e quindi selezionare un'opzione che consenta di visualizzare più dettagli riguardo a quel particolare elemento.
- 6. Usare le frecce accanto a un titolo di colonna per cambiare l'ordinamento in base al quale i report vengono elencati.
- 7. Agire sul report di riepilogo tramite le opzioni disponibili sopra il grafico. Visualizzare maggiori dettagli facendo clic sugli elementi di interesse del nuovo report.

Opzione	Azione
Percorso report (Utente > Giorno)	Accanto all'elenco Visualizza utilizzo di Internet per viene visualizzato un percorso che mostra le selezioni effettuate per la creazione del report corrente. Fare clic su un collegamento qualunque del percorso per ritornare a quella visualizzazione di dati.
Visualizza	Selezionare un periodo di tempo per il report: Un giorno, Una settimana, Un mese o Tutti. Il report viene aggiornato per mostrare i dati relativi al periodo di tempo selezionato.
	Usare i pulsanti a freccia adiacenti per spostarsi lungo i dati disponibili, un periodo di tempo (giorno, settimana, mese) per volta.
	Se si cambia questa selezione, i campi di Visualizza da vengono aggiornati per riflettere il periodo di tempo visualizzato.
	Il campo Visualizza visualizzerà Personalizza, anziché un periodo di tempo, se si sceglie una data specifica nei campi di Visualizza da o tramite la finestra di dialogo Preferiti.
Visualizza da a	Le date riportate in questi campi si aggiornano automaticamente per riflettere il periodo di tempo visualizzato nel caso si apportino modifiche nel campo Visualizza .
	In alternativa, inserire la data esatta di inizio e di fine della generazione dei report oppure fare clic sull'icona calendario per selezionare le date desiderate.
	Fare clic sul pulsante freccia verso destra per aggiornare il report dopo aver selezionato le date.
Grafico a torta / Grafico a barre	Se il grafico a barre è attivo, fare clic su Grafico a torta per visualizzare il report di riepilogo corrente come un grafico a torta. Fare clic sull'etichetta di una sezione del grafico per visualizzare le stesse opzioni disponibili quando si fa clic su una voce nella colonna sinistra del grafico a barre. Se il grafico a torta è attivo, fare clic su Grafico a barre
	grafico a barre.

Opzione	Azione
Schermo intero	Selezionare questa opzione per visualizzare il report investigativo corrente in una finestra separata senza i riquadri di navigazione di destra e di sinistra.
Anonimo/Nomi	Fare clic su Anonimo per definire che i report visualizzino un numero di identificazione utente assegnato internamente, anziché visualizzare il nome dell'utente.
	Se i nomi sono nascosti, fare clic su Nomi per visualizzare i nomi utente in questi percorsi.
	In alcuni casi, i nomi utente non possono venire visualizzati. Per ulteriori informazioni, vedere <i>Configurazione di Filtering Service per la registrazione</i> , pagina 314.
	Se si fa clic su Anonimo e quindi ci si sposta in una visualizzazione di dati diversa, come ad esempio una visualizzazione di dettagli o di casi atipici, i nomi utente rimangono nascosti nel nuovo report. Tuttavia, per ritornare alla visualizzazione di riepilogo con i nomi nascosti, occorre usare i collegamenti disponibili nell'area superiore del report, non gli elementi del percorso (breadcrumbs) visualizzati nell'intestazione.
	Se si vuole che i singoli amministratori non abbiano mai accesso ai nomi utente inseriti nei report, assegnarli a un ruolo in base al quale i permessi assegnati impediscano la loro visualizzazione nei report investigativi nonché l'accesso ai report di presentazione.
Cerca per	Selezionare un elemento del report dall'elenco e inserire quindi il valore intero o parziale della ricerca nella casella di controllo adiacente.
	Fare clic sul pulsante freccia adiacente per avviare la ricerca e visualizzare i risultati.
	Inserire un indirizzo IP parziale, come ad esempio 10.5, cercare tutti i subnet che in questo particolare esempio vanno da 10.5.0.0 a 10.5.255.255.

- 8. Aggiungere un sottogruppo di informazioni per tutte o per alcune delle voci selezionate nella colonna di sinistra creando un report di riepilogo multi-livello. Vedere *Report di riepilogo multi-livello*, pagina 126.
- 9. Creare un report tabulare per un elemento specifico incluso nella colonna di sinistra, facendo clic sul numero adiacente o sulla barra di misurazione. Questo report dettagliato può essere modificato al fine di soddisfare specifiche esigenze. Vedere *Report dettagliati flessibili*, pagina 127.

Report di riepilogo multi-livello

Argomenti correlati:

- Report investigativi, pagina 119
- Report di riepilogo, pagina 121
- Report dettagliati flessibili, pagina 127
- *Report Dettagli attività utente*, pagina 132
- Report standard, pagina 137
- Report investigativi preferiti, pagina 138
- Pianificazione dei report investigativi, pagina 141
- Report casi atipici, pagina 144
- *Output su file*, pagina 145

I report di riepilogo mostrano un secondo livello di informazioni a integrazione delle informazioni principali visualizzate. Ad esempio, se la visualizzazione principale mostra le classi di rischio, è possibile definire un secondo livello per le categorie più richieste nell'ambito di ciascuna classe di rischio. Per citare un altro esempio, se il report principale mostra le richieste per ogni categoria, è possibile visualizzare le 5 categorie e i 10 utenti con il più alto numero di richieste di ciascuna di esse.

Utilizzare le impostazioni disponibili sopra il report di riepilogo per creare un report di riepilogo multi-livello.

1. Nell'elenco **Seleziona i primi**, scegliere un numero che determina il numero di voci principali (colonna sinistra) da includere nel report. Il report che ne risulta includerà le voci principali con i valori maggiori. (Questo mostra le date più lontane se Giorno è la voce principale.)

In alternativa, contrassegnare la casella di controllo accanto alle voci individuali desiderate, nella colonna di sinistra, per includere solo queste voci nel report. Il campo **Seleziona i primi** visualizza **Personalizza**.

- 2. Dall'elenco per, scegliere le informazioni secondarie da includere nel report.
- 3. Nel campo **Visualizza**, scegliere il numero di risultati secondari da includere nel report per ogni voce principale.
- 4. Fare clic su Visualizza risultati per generare il report di riepilogo multi-livello. Il report di riepilogo viene aggiornato per mostrare soltanto il numero di voci principali selezionate. Sotto la barra di ogni voce principale, viene visualizzato un elenco di voci secondarie
- 5. Usare le frecce accanto a un titolo di colonna per cambiare l'ordine in base al quale vengono elencati i report.

Per ritornare a un report di riepilogo multi-livello, selezionare un'opzione diversa in **Visualizza utilizzo di Internet per**. In alternativa, fare clic su una delle voci principali o secondarie e selezionare un'opzione per generare un nuovo report investigativo riguardo a tali informazioni.

Report dettagliati flessibili

Argomenti correlati:

- Report investigativi, pagina 119
- Report di riepilogo, pagina 121
- Report di riepilogo multi-livello, pagina 126
- Report investigativi preferiti, pagina 138
- Pianificazione dei report investigativi, pagina 141
- Report casi atipici, pagina 144
- *Output su file*, pagina 145
- Collegamento con il database e impostazioni predefinite dei report, pagina 342
- Colonne dei report dettagliati flessibili, pagina 130

I report dettagliati offrono una visualizzazione tabulare delle informazioni contenute nel database di registrazione. Si può accedere alla visualizzazione di un report dettagliato nella pagina principale dopo aver visualizzato un report di riepilogo per il quale si vogliono ottenere ulteriori dettagli.

È possibile richiedere una visualizzazione dettagliata da qualunque riga. Tuttavia, quando si richiede un report dettagliato in base agli accessi, è consigliabile iniziare da una riga che mostri meno di 100.000 accessi. Se una riga contiene più di 100.000 accessi, il numero di accessi viene visualizzato in rosso per segnalare che la generazione di un report dettagliato può comportare lunghi tempi di esecuzione.

La visualizzazione di un report dettagliato viene considerata *flessibile* in quanto consente di definire a piacimento il proprio report. Si possono aggiungere o eliminare colonne di informazioni e modificare l'ordine delle colonne visualizzate. Queste informazioni vengono organizzate in base all'ordine delle colonne. È anche possibile invertire l'ordine delle voci di ogni colonna, da ascendenti a discendenti e viceversa.

I report investigativi di Websense sono limitati dal processore e dalla memoria disponibile nel computer con installato Websense Manager, nonché da alcune risorse di rete. Le richieste di report estesi possono anche incorrere in un time-out. Quando si richiede un report esteso, sono disponibili varie opzioni per la generazione di un report senza incorrere in un time-out.



In qualsiasi elenco a discesa o elenco di valori, le opzioni appaiono in rosso. Le lettere in rosso segnalano che la selezione di quell'opzione potrebbe comportare la generazione di un report molto lungo. È normalmente più efficace approfondire i dettagli prima di selezionare quell'opzione.

- 1. Generare un report di riepilogo o un report multi-livello nella pagina principale dei report investigativi. (Vedere *Report di riepilogo*, pagina 121 o *Report di riepilogo multi-livello*, pagina 126.)
- 2. Analizzare i risultati in dettaglio per concentrarsi sulle informazioni di maggior interesse.

Tuttavia se si genera un report sugli accessi, è consigliabile analizzare in dettaglio una voce che mostri meno di 100.000 accessi prima di aprire la visualizzazione del report dettagliato.

3. Fare clic sul numero o sulla barra che corrisponde alla riga di cui si vogliono analizzare i dettagli. Per includere molteplici righe in un report, contrassegnare la casella di controllo di ogni riga interessata prima di fare clic sul numero o sulla barra di una di esse.

Viene visualizzato un messaggio che mostra lo stato di avanzamento del caricamento del report dettagliato.

Nota

Se la generazione del report impiega molto tempo, considerare la possibilità di salvarlo come un report Preferito facendo clic sull'apposito collegamento nel messaggio Caricamento in corso e pianificare la sua esecuzione in un secondo tempo. Vedere *Report investigativi preferiti*, pagina 138.

4. Rivedere le informazioni contenute nel report iniziale.

Le colonne predefinite variano, a seconda che si tratti di un report sugli accessi, sulla larghezza di banda o sui tempi di navigazione e a seconda delle selezioni effettuate nella pagina Opzioni. (Vedere *Collegamento con il database e impostazioni predefinite dei report*, pagina 342.)

5. Fare clic su Modifica report nell'area superiore della pagina.

L'elenco **Report in uso** della finestra di dialogo Modifica report mostra le colonne incluse nel report dettagliato corrente.

 Selezionare il nome di una colonna nell'elenco Colonne disponibili o nell'elenco Report in uso e fare clic sul pulsante a freccia rivolta verso destra (>) o verso sinistra (<) per spostare la colonna nell'altro elenco. Scegliere un massimo di 7 colonne per il report. La colonna che mostra il valore della misurazione (accessi, larghezza di banda, tempo di navigazione), ricavata dal report di riepilogo iniziale, è la colonna all'estrema destra. Si può scegliere di non visualizzarla quando si modifica il report.

Vedere *Colonne dei report dettagliati flessibili*, pagina 130 per un elenco delle colonne disponibili e per la descrizione di ognuna di esse.

7. Selezionare il nome di una colonna dell'elenco **Report in uso** ed utilizzare i pulsanti a freccia su e già per cambiare l'ordine delle colonne.

La colonna in alto nell'elenco del Report in uso diventa la colonna di sinistra del report.

8. Fare clic sul collegamento **Riepilogo** o **Dettagli** sopra il report per passare da una visualizzazione all'altra.

Opzione	Descrizione
Riepilogo	Occorre eliminare la colonna Ora per poter visualizzare il report di riepilogo. I report di riepilogo raggruppano sotto un'unica voce tutti i record che condividono un elemento in comune. L'elemento specifico varia a seconda delle informazioni contenute nel report. Normalmente, la colonna all'estrema destra prima del valore di misurazione mostra l'elemento di riepilogo.
Dettagli	L'opzione Dettagli visualizza ogni record come una riga distinta. È possibile visualizzare la colonna Ora.

- 9. Fare clic su Invia per generare il report definito.
- 10. Utilizzare le opzioni seguenti per modificare il report visualizzato.
 - Utilizzare le opzioni di Visualizza sopra il report per modificare il periodo di tempo coperto dal report.
 - Fare clic sulla freccia rivolta verso l'alto o verso il basso nell'intestazione di una colonna per invertire l'ordine ascendente o discendente della colonna e dei dati ad essa associati.
 - Fare clic sul collegamento Avanti o Indietro sopra e sotto il report per visualizzare altre eventuali pagine del report. Per impostazione predefinita, ciascuna pagina contiene 100 righe. Il numero di righe può essere modificato in base alle proprie necessità. Vedere *Opzioni di visualizzazione e di output*, pagina 344.
 - Fare clic sull'URL per aprire in una nuova finestra il sito Web richiesto.
- 11. Fare clic su **Report preferiti** se si vuole salvare il report in modo da poterlo generare ancora rapidamente o periodicamente (vedere *Salvataggio di un report come Preferito*, pagina 139).

Colonne dei report dettagliati flessibili

Argomenti correlati:

- *Report dettagliati flessibili*, pagina 127
- Report investigativi preferiti, pagina 138
- Pianificazione dei report investigativi, pagina 141

La tabella sottostante descrive le colonne disponibili per i report dettagliati (vedere *Report dettagliati flessibili*, pagina 127).

Non tutte le colonne sono disponibili in qualsiasi momento. Ad esempio, se la colonna Utente viene visualizzata, Gruppo non è disponibile; se Categoria è visualizzata, Classe di rischio non è disponibile.

Nome colonna	Descrizione
Utente	Nome dell'utente che ha inoltrato la richiesta. Le informazioni sull'utente devono essere disponibili nel database di registrazione per poter essere incluse nei report. Le informazioni sui gruppi non sono disponibili nei report basati sugli utenti.
Giorno	La data di invio della richiesta.
Nome host URL	Il nome del dominio (chiamato anche nome host) del sito richiesto.
Dominio	Il dominio del servizio di directory per il client directory- based (utente o gruppo, dominio o unità organizzativa) che ha inviato la richiesta.
Gruppo	Nome del gruppo cui appartiene il richiedente. I singoli nomi utente non vengono inclusi nei report basati sui gruppi. Se l'utente che ha richiesto il sito appartiene a più di un gruppo del servizio di directory, il report elenca molteplici gruppi in questa colonna.
Classe di rischio	La classe di rischio associata alla categoria alla quale appartiene il sito richiesto. Se la categoria fa parte di molteplici classi di rischio, tutte le classi di rischio rilevanti vengono incluse nell'elenco. Vedere <i>Assegnazione delle</i> <i>categorie alle classi di rischio</i> , pagina 312.
Oggetto di directory	Il percorso della directory per l'utente che ha inviato la richiesta, escluso il nome utente. Normalmente, questo comporta molteplici righe per lo stesso traffico in quanto ogni utente appartiene alle directory di più percorsi. Se si sta usando un servizio di directory LDAP, questa colonna non è disponibile.
Disposizione	L'azione effettuata dal software Websense come risultato della richiesta, come ad esempio l'autorizzazione concessa ad una categoria o una categoria bloccata.

Nome colonna	Descrizione
Server di origine	L'indirizzo IP del computer che ha inviato le richieste a Filtering Service. Questo è il computer su cui è in esecuzione il prodotto di integrazione o Websense Network Agent.
Protocollo	Il protocollo della richiesta.
Gruppo di protocolli	Gruppo del Master Database nel quale rientra il protocollo richiesto.
IP di origine	L'indirizzo IP del computer dal quale è stata inviata la richiesta.
IP di destinazione	Indirizzo IP del sito richiesto.
URL completo	Il nome del dominio e il percorso del sito richiesto (esempio: http://www.mio dominio.it/prodotti/elementouno/). Se non si registrano URL completi nel log, questa colonna rimane vuota. Vedere <i>Configurazione della registrazione di URL</i> <i>completi</i> , pagina 333.
Mese	Il mese di calendario in cui è stata inviata la richiesta.
Porta	La porta TCP/IP attraverso la quale l'utente ha comunicato con il sito.
Larghezza di banda	La quantità di dati, in kilobyte, in riferimento sia alla richiesta iniziale ricevuta dall'utente sia la risposta ricevuta dal sito Web. Questa è rappresentata dal totale dei valori di Inviati e Ricevuti.
	Tenere presente che alcuni prodotti di integrazione non inviano queste informazioni al software Websense. Due esempi sono il Check Point FireWall-1 e Cisco PIX Firewall. Se i prodotti di integrazione non inviano queste informazioni e Websense Network Agent è stato installato, attivare l'opzione Registra richieste HTTP (registrazione avanzata nel log) affinché il NIC appropriato sia in grado di creare report con informazioni sulla larghezza di banda. Vedere <i>Configurazione delle impostazioni della scheda</i> <i>dell'interfaccia di rete (NIC)</i> , pagina 355.
Byte inviati	Il numero di byte inviati come richiesta Internet. Questo rappresenta la quantità di dati trasmessi, che potrebbe essere associata ad una semplice richiesta di URL o a un invio più consistente se l'utente si registra, ad esempio, in un sito Web.

Nome colonna	Descrizione
Byte ricevuti	Il numero di byte ricevuti da Internet in risposta alla richiesta. Questo include tutti i testi, le immagini grafiche e gli script che fanno parte del sito.
	Per i siti bloccati, il numero di byte varia in funzione del software che crea il record di registrazione. Quando Websense Network Agent registra i record, il numero di byte ricevuti per un sito bloccato rappresenta le dimensioni della pagina di blocco.
	Se i record del log vengono creati da Websense Security Gateway, a seguito della scansione in tempo reale, i byte ricevuti rappresentano le dimensioni della pagina scannerizzata. Per ulteriori informazioni sulla scansione in tempo reale, vedere <i>Analisi del contenuto con le opzioni di</i> <i>Tempo reale</i> , pagina 149.
	Se un altro prodotto di integrazione crea i record di registrazione, i byte ricevuti per un sito bloccato potrebbero essere pari a (0), potrebbero rappresentare le dimensioni della pagina di blocco o potrebbero essere costituiti da un valore ottenuto dal sito richiesto.
Ora	L'ora del giorno della richiesta del sito, espressa nel formato HH:MM:SS, in base alle 24 ore.
Categoria	La categoria in base alla quale si è filtrata la richiesta. Questa può essere una categoria ricavata dal Websense Master Database o una categoria personalizzata.

Report Dettagli attività utente

Argomenti correlati: • Report investigativi, pagina 119

Fare clic sul collegamento **Dettaglio attività utente giorno/mese** per generare un report Dettaglio attività utente. Questo report offre un'interpretazione grafica dell'attività svolta in Internet dall'utente e riferita a un'intera giornata o a un mese.

Prima di tutto, generare un report per un utente specifico in riferimento ad una data selezionata. Da questo report è possibile generare un altro report sull'attività dello stesso utente riferita a un intero mese. Per informazioni dettagliate, vedere .

- Dettaglio giornaliero attività utente, pagina 133
- Dettaglio mensile attività utente, pagina 134

Dettaglio giornaliero attività utente

Argomenti correlati:

- Report investigativi, pagina 119
- *Report Dettagli attività utente*, pagina 132
- Dettaglio mensile attività utente, pagina 134

Il report Dettaglio giornaliero attività utente offre un quadro più approfondito dell'attività di un utente specifico nel corso di una giornata.

- 1. Selezionare **Dettaglio attività utente/mese** nell'area superiore della pagina principale. Viene visualizzata la finestra di dialogo Dettaglio giornaliero attività utente.
- 2. Inserire il nome dell'utente, o una parte del nome, nel campo **Cerca utente** e fare quindi clic su **Cerca**.

La ricerca visualizza un elenco scorrevole contenente fino a un massimo di 100 nomi utenti ricavati dal database di registrazione.

- 3. Eseguire le selezioni desiderate dall'elenco Seleziona utente.
- 4. Nel campo **Seleziona giorno**, si può accettare l'ultima data dell'attività visualizzata per impostazione predefinita, oppure scegliere una data diversa.

Si può digitare la nuova data o fare clic sull'icona del calendario per selezionare una data. La casella di controllo del calendario indica l'intervallo di date coperto dal database di registrazione attivo.

5. Fare clic su **Attività giornaliera utente** per visualizzare un report dettagliato sull'attività di quel particolare utente alla data richiesta.

Il report iniziale visualizza la sequenzialità temporale dell'attività dell'utente in incrementi di 5 minuti. Ciascuna richiesta viene visualizzata come un'icona che corrisponde a una categoria del Websense Master Database. Una singola icona rappresenta tutte le categorie personalizzate. (Il colore delle icone corrisponde al raggruppamento dei rischi incluso nei report Dettaglio mensile attività utente. Vedere *Dettaglio mensile attività utente*, pagina 134.)

Posare il mouse sopra l'icona per visualizzare l'ora esatta, la categoria e l'azione per la relativa richiesta.

Usare i controlli riportati qui di seguito per modificare la visualizzazione del report o per leggere una didascalia.

Opzione	Descrizione
Giorno precedente / Giorno successivo	Visualizza l'attività Internet dell'utente svolta nel corso del giorno di calendario precedente o successivo.
Tabella	Visualizza un elenco di ciascun URL richiesto, con la data e l'ora della richiesta, la categoria e l'azione intrapresa (bloccata, autorizzata o altro).

Opzione	Descrizione
Dettagli	Apre la visualizzazione grafica iniziale del report.
Raggruppa accessi simili / Visualizza tutti gli accessi	Unifica in una singola riga tutte le richieste inviate entro 10 secondi una dall'altra e associate allo stesso dominio, categoria e azione. Questo comporta una visualizzazione riepilogativa ancora più concisa delle informazioni.
	La soglia di tempo standard è di 10 secondi. Se occorre modificare questo valore, vedere <i>Opzioni di visualizzazione</i> <i>e di output</i> , pagina 344.
	Dopo aver fatto clic sul link, questo diventa Visualizza tutti gli accessi e ripristina l'elenco originale di ciascuna richiesta.
Controllo vista categorie	Visualizza nel report in uso un elenco di tutte le categorie, con il nome e l'icona che le rappresentano.
	È possibile determinare le categorie da includere nel report selezionando le caselle di controllo rilevanti. Fare quindi clic su Accetta per aggiornare il report in base alle selezioni eseguite.

6. Fare clic su **Dettaglio mensile attività utente**, sopra il report, per visualizzare l'attività eseguita dallo stesso utente nel corso dell'intero mese. Per ulteriori informazioni, vedere *Dettaglio mensile attività utente*, pagina 134.

Dettaglio mensile attività utente

Argomenti correlati:

- *Report investigativi*, pagina 119
- *Report Dettagli attività utente*, pagina 132
- Dettaglio giornaliero attività utente, pagina 133
- *Mappatura delle categorie*, pagina 135

Con il report Dettaglio giornaliero attività utente aperto, è possibile passare a visualizzare l'attività mensile di quello stesso utente.

- 1. Aprire un report Dettaglio giornaliero attività utente. Vedere *Dettaglio giornaliero attività utente*, pagina 133.
- 2. Fare clic su **Dettaglio mensile attività utente** in alto.

Il nuovo report visualizza un'immagine di calendario con ciascuna area del giorno che mostra piccoli blocchi colorati che rappresentano l'attività Internet dell'utente di quel giorno. Le richieste di accesso ai siti che fanno parte di categorie personalizzate vengono visualizzate come blocchi grigi.

3. Fare clic su **Legenda categorie di database** nell'area superiore sinistra per osservare come i colori rappresentino un rischio potenziale basso o alto per il sito richiesto.

Le assegnazioni delle categorie sono fisse e non possono venire modificate. Vedere *Mappatura delle categorie*, pagina 135.

4. Fare clic su **Indietro** o **Avanti** per visualizzare l'attività Internet di questo utente per il mese precedente o successivo.

Mappatura delle categorie

Argomenti correlati:

- *Report investigativi*, pagina 119
- *Report Dettagli attività utente*, pagina 132
- Dettaglio mensile attività utente, pagina 134

L'elenco che segue identifica le categorie rappresentate da ciascuno dei colori utilizzati dai report Dettaglio giornaliero attività utente e Dettaglio mensile attività utente.

Tenere presente che i nomi delle categorie del Master Database sono soggette a modifica. Altre categorie possono inoltre venire aggiunte o alcune di esse eliminate in qualsiasi momento.

Colore	Categorie
Grigio	Categorie personalizzate
	Traffico non-HTTP
Blu scuro	Business ed economia e tutte le sottocategorie
	Educazione e tutte le sottocategorie
	Salute
	Tecnologia informatica , tra cui le sottocategorie Motori di ricerca e Portali, Web Hosting)
	Miscellanea e sottocategorie quali Reti gestite di Content Delivery, Contenuto Dinamico, Immagini (Media), Image Server e Indirizzi IP privati.
	Produttività/Pubblicità
Azzurro	Droghe/Farmaci prescrivibili
	Governo e sottocategorie quali Argomenti militari
	Tecnologia informativa/Siti di traduzione URL
	Miscellanea, soltanto la categoria madre
	Notizie e Media, soltanto la categoria madre
	Eventi speciali

Colore	Categorie
Giallo /verde	Aborto e relative sottocategorie
	Materiale per adulti / Educazione sessuale
	Larghezza di rete (tra cui Radio e TV via Internet, Archiviazione e Storage personale in rete e backup e Streaming media)
	Intrattenimento, con le relative sotto-categorie MP3
	Giochi
	Governo/Gruppi politici
	Tecnologia informatica/Sicurezza del Computer
	Comunicazione via Internet/E-mail attraverso il Web
	Miscellanea /Server per il download di file
	Miscellanea /Errori di Rete
	Notizie e Media /Riviste Alternative
	Produttività tra cui le relative categorie di Scambio di messaggi istantanei, Forum e bacheche, Intermediazione e Commercio in linea
	Religione e tutte le relative sottocategorie, tra cui Religioni non tradizionali ed occulte, Folclore e Religioni tradizionali
	Sicurezza, soltanto la categoria madre
	Acquisti in linea e relative sottocategorie
	Organizzazioni sociali e relative sottocategorie
	Società e Stili di vita , e le relative sottocategorie quali Argomenti d'interesse omosessuale o bisessuale, Passatempo, Siti Web di incontri, Ristoranti e Conviti.
	Sport e relative sottocategorie
	Viaggi e turismo
	Definiti dagli utenti
	Veicoli

Colore	Categorie
Arancione	Materiale per adulti /Nudità
	Gruppi di sostegno
	Larghezza di banda/Telefonia via Internet
	Droghe , e le relative sottocategorie tra cui Abuso di droga, Marijuana, Additivi e Composti non regolati
	Tecnologia informatica/Elusione via proxy
	Comunicazione via Internet e le relative sottocategorie quali Web Chat
	Ricerca di lavoro
	Miscellanea /Non classificato
	Produttività e relative categorie, quali Download di Freeware e Software e Guadagna navigando
	Religione
	Società e stili di vita e le relative sottocategorie quali Alcool e tabacco, Relazioni personali e Incontri
	Cattivo gusto
	Armi
Rosso	Materiale per adulti e le sotto-categorie seguenti: Contenuto per adulti, Biancheria intima e Costumi da bagno, Sesso
	Larghezza di banda/Scambio di file Peer-to-Peer
	Giochi d'azzardo
	Argomenti illeciti o discutibili
	Tecnologia informatica/Hacking (Pirateria informatica)
	Militanza ed estremismo
	Razzismo e Odio
	Sicurezza e le relative sottocategorie quali Keylogger, siti Web dannosi, Falsificazione di pagine Web (Phishing) e Spyware (programmi spia)
	Violenza

Report standard

Argomenti correlati:

- *Report investigativi*, pagina 119
- Report investigativi preferiti, pagina 138
- Pianificazione dei report investigativi, pagina 141

I report standard consentono di visualizzare un set particolare di informazioni con rapidità senza usare il processo drill-down.

1. Fare clic sul collegamento **Report standard** nella pagina dei Report investigativi principali.

2. Scegliere un report che contenga le informazioni desiderate. Sono disponibili i report seguenti.

Livelli di attività più elevati

- Utenti con il maggior numero di accessi
- Primi 10 utenti per i 10 URL più visitati
- · Primi 5 utenti in acquisti, intrattenimento e sport
- Primi 5 URL per le 5 categorie più visitate

Consumo di banda più elevato

- · Gruppi che occupano maggiormente la larghezza di banda
- · Gruppi che consumano la maggior parte della banda in Streaming Media
- Report dettagliato URL su utenti per perdita di larghezza di banda
- Primi 10 gruppi per categorie di larghezza di banda

Utenti maggiormente collegati

- Quali utenti sono collegati per la maggior parte del tempo?
- Quali utenti trascorrono la maggior parte del tempo su siti delle categorie di produttività?

Più bloccati

- Utenti bloccati più volte
- Siti bloccati più volte
- Report dettagliato URL su utenti bloccati
- Prime 10 categorie bloccate

Rischio di sicurezza più elevato

- Categorie principali per rischio di sicurezza
- Utenti principali del protocollo P2P
- · Primi utenti dei siti in categorie di sicurezza
- URL per i primi 10 computer con attività spyware

Responsabilità legale

- Rischio di responsabilità legale per categoria
- Utenti principali per le categorie Adulti
- 3. Visualizzare il report indicato.
- 4. Salvare il report come un Preferito se si vuole generarlo periodicamente. Vedere *Report investigativi preferiti*, pagina 138.

Report investigativi preferiti

Argomenti correlati:

- Report investigativi, pagina 119
- Pianificazione dei report investigativi, pagina 141

È possibile salvare la maggior parte dei report investigativi come **Preferiti**. Questo include i report che si generano per approfondire specifiche informazioni, i report standard e i report dettagliati che sono stati modificati per soddisfare specifiche esigenze. Si può generare il report Preferito in qualsiasi momento oppure pianificarne l'esecuzione in base a giorni e ore specifici.

Nelle organizzazioni che usano un'amministrazione con delega, il permesso al salvataggio e alla pianificazione dei Preferiti viene assegnata dal Super Administrator. Gli amministratori che possiedono questo tipo di permesso possono generare e pianificare soltanto i Preferiti che hanno salvato; non hanno accesso ai Preferiti salvati da altri amministratori.

Per informazioni dettagliate sulla gestione dei report Preferiti, vedere:

- Salvataggio di un report come Preferito, pagina 139
- Generazione o cancellazione di un report Preferito, pagina 140
- Modifica di un report Preferito, pagina 140

Salvataggio di un report come Preferito

Argomenti correlati:

- *Report investigativi preferiti*, pagina 138
- Modifica di un report Preferito, pagina 140

Adottare la procedura seguente per salvare un report come Preferito.

- 1. Si può generare un report investigativo con il formato e le informazioni desiderate.
- 2. Fare clic su **Report preferiti**.
- 3. Accettare o modificare il nome visualizzato da Websense Manager.

Il nome assegnato può contenere lettere, numeri e caratteri di sottolineatura (_). Non si possono usare spazi o altri caratteri speciali.

4. Fare clic su Aggiungi.

Il nome del report viene aggiunto all'elenco dei Preferiti.

- 5. Selezionare un report dall'elenco e quindi selezionare un'opzione per la gestione del report. In funzione dell'opzione scelta, vedere:
 - Generazione o cancellazione di un report Preferito, pagina 140
 - Pianificazione dei report investigativi, pagina 141

Generazione o cancellazione di un report Preferito

Argomenti correlati:

- Report investigativi preferiti, pagina 138
- Modifica di un report Preferito, pagina 140

È possibile generare un report preferito in qualsiasi momento o eliminare i report superati.

1. Fare clic su **Report preferiti** per visualizzare un elenco di report salvati come Preferiti.



Nota

Se la propria organizzazione usa un'amministrazione con delega, questo elenco non includerà i report preferiti salvati da altri amministratori.

2. Selezionare il report desiderato dall'apposito elenco.

Se il report desiderato non è stato salvato come Preferito, vedere *Salvataggio di un report come Preferito*, pagina 139.

- 3. A seconda delle necessità:
 - Fare clic su **Esegui ora** per generare e visualizzare immediatamente il report selezionato.
 - Fare clic su **Pianificazione** per pianificare la generazione di un report in un secondo tempo o periodicamente. Per ulteriori informazioni, vedere *Pianificazione dei report investigativi*, pagina 141.
 - Fare clic su Elimina per eliminare il report dall'elenco dei Preferiti.

Modifica di un report Preferito

Argomenti correlati:

- *Report investigativi*, pagina 119
- Report investigativi preferiti, pagina 138

Si può creare facilmente un nuovo report Preferito simile a un report Preferito esistente, procedendo come segue:

1. Fare clic su **Report preferiti** per visualizzare un elenco di report salvati come Preferiti.



Nota

Se la propria organizzazione usa un'amministrazione con delega, questo elenco non includerà i report preferiti salvati da altri amministratori.

- Selezionare ed eseguire il report Preferito esistente che si avvicina di più al nuovo report che si vuole creare. (Vedere *Generazione o cancellazione di un report Preferito*, pagina 140).
- 3. Modificare il report visualizzato, come necessario.
- 4. Fare clic su **Report preferiti** per salvare il report revisionato come un report Preferito con un nuovo nome. (Vedere *Salvataggio di un report come Preferito*, pagina 139.)

Pianificazione dei report investigativi

Argomenti correlati:

- *Report investigativi preferiti*, pagina 138
- Salvataggio di un report come Preferito, pagina 139
- Gestione dei processi pianificati per i report investigativi, pagina 144

Occorre salvare un report investigativo come Preferito prima di poterlo pianificare per un'esecuzione in un secondo tempo o con periodicità regolare. Una volta che il processo dei report pianificati è stato eseguito, i report così ottenuti vengono inviati via e-mail ai destinatari designati. Quando si pianificano i processi, valutare se il proprio server e-mail è in grado di gestire le dimensioni e la quantità di report da allegare alle e-mail.

I file dei report pianificati vengono automaticamente archiviati nella seguente directory:

<install path>\webroot\Explorer\<name>\

Il percorso di installazione predefinito è C:\Programmi\Websense. Se il processo pianificato ha un destinatario unico, il suo <nome> costituisce la prima parte

dell'indirizzo e-mail (prima di @). Nel caso di molteplici destinatari, i report vengono salvati in una directory dal nome Altri.



I report salvati da un processo eseguito periodicamente, utilizzano ogni volta lo stesso nome di file. Se si vogliono tenere i file per un periodo più lungo di un ciclo, cambiare il nome del file o copiare il file in un altro percorso.

A seconda delle dimensioni e del numero di report pianificati, questa directory potrebbe diventare molto grande. Pulire la directory periodicamente, eliminando i file dei report non più necessari.

- 1. È possibile salvare uno o più report come Preferiti. (Vedere Salvataggio di un report come Preferito, pagina 139).
- 2. Fare clic su Report preferiti per visualizzare un elenco di report salvati come Preferiti.



Nota

Se la propria organizzazione usa i ruoli di amministrazione con delega, questo elenco non includerà i report preferiti salvati da altri amministratori.

- 3. Evidenziare fino a un massimo di 5 report per un'esecuzione come parte del processo definito.
- 4. Fare clic su **Pianificazione** per creare un processo pianificato di creazione dei report e quindi fornire le informazioni richieste nella pagina Pianifica report.

Si consiglia di pianificare i processi di creazione dei report in giorni e a orari diversi per evitare di sovraccaricare il database di registrazione e di rallentare la performance relativa alla registrazione e alla creazione interattiva dei report.

Campo	Descrizione
Frequenza	Selezionare la frequenza (Una volta, Giornalmente, Settimanalmente, Mensilmente) dell'esecuzione di questo processo.
Data di inizio	Scegliere il giorno della settimana o la data di calendario per l'esecuzione del processo per la prima (o unica) volta.
Esecuzione	Definire l'ora del giorno per l'esecuzione del processo.
Indirizzo e-mail	Usare il campo Indirizzo e-mail aggiuntivo per aggiungere gli indirizzi necessari a questo elenco.
	Evidenziare nel processo uno o più indirizzi e-mail dei destinatari che devono ricevere i report. (Accertarsi di deselezionare gli indirizzi che non devono ricevere i report.)

Campo	Descrizione
Indirizzi e-mail aggiuntivi	Inserire un indirizzo e-mail e fare clic su Aggiungi per aggiungerlo all'elenco E-mail .
	Il nuovo indirizzo e-mail viene automaticamente evidenziato come gli altri indirizzi e-mail selezionati.
Personalizzare l'oggetto e il testo della e-mail.	Contrassegnare questa casella di controllo per personalizzare la riga dell'oggetto e il testo della e-mail.
	Se questa casella non è evidenziata, si useranno l'oggetto e il testo predefiniti.
Oggetto della e- mail	Inserire il testo che dovrà apparire nella riga dell'oggetto della e-mail quando i report vengono distribuiti.
	Il testo predefinito della riga "Oggetto" è il seguente:
	Processo pianificato per la creazione dei report investigativi
Testo e-mail	Inserire il testo da aggiungere al messaggio e-mail per la distribuzione dei report pianificati.
	La e-mail contiene il testo riportato di seguito, con il proprio testo che sostituisce la dicitura <testo PERSONALIZZATO>:</testo
	Il Pianificatore report ha generato il file o i file allegati il/ alle <data ora="">.</data>
	<testo personalizzato=""></testo>
	Per verificare il report o i report generati, fare clic sui collegamenti seguenti.
	Nota - Il collegamento non funzionerà se il destinatario non ha accesso al server Web dal quale il processo è stato inviato.
Nome del processo pianificato	Assegnare un nome univoco al processo pianificato. Il nome serve ad identificare questo processo nella Coda processi. Vedere <i>Gestione dei processi pianificati per i report</i> <i>investigativi</i> , pagina 144.
Formato di output	Selezionare un formato di file per i report pianificati.
	PDF - I file PDF (Portable Document Format) possono venire visualizzati in Adobe Reader.
	Excel - I file in Excel vanno visualizzati in Microsoft Excel.
Intervallo di date	Definire l'intervalle delle date a cui si riferiscono i report di questo processo.
	Tutte le date - Tutte le date disponibili nel database di registrazione.
	Relativo - Usare il periodo di tempo (Giorni, Settimane o Mesi) e il periodo di tempo specifico da includere (Questo, Ultimo, Ultimi 2, e così via).
	Specifico - Definire delle date o un intervallo di date specifici per i report di questo processo.

5. Fare clic su Avanti per aprire la scheda Conferma pianificazione.

6. Fare clic su **OK** per salvare le selezioni eseguite e per andare alla pagina Coda processi (vedere *Gestione dei processi pianificati per i report investigativi*, pagina 144).

Gestione dei processi pianificati per i report investigativi

Argomenti correlati:

- *Report investigativi*, pagina 119
- Pianificazione dei report di presentazione, pagina 112

Se si crea un processo pianificato per la creazione di report investigativi, viene visualizzata la pagina **Coda processi** che riporta il nuovo processo e un elenco dei processi pianificati esistenti. Si può accedere alla pagina facendo clic sul collegamento **Coda processi** della pagina principale dei report investigativi.

Nota

Se la propria organizzazione usa un'amministrazione con delega, questa pagina non includerà i processi pianificati da altri amministratori.

La sezione **Pianifica dettaglio report** include un elenco dei processi pianificati in base alla data della loro creazione nonché la loro pianificazione definitiva e il loro stato corrente. Sono inoltre disponibili le opzioni seguenti.

Opzione	Descrizione
Modifica	Visualizza la pianificazione definita per questo processo e consente di modificarla, se necessario.
Elimina	Elimina il processo ed aggiunge una voce alla sezione Registro di stato che mostra il processo come eliminato.

La sezione **Registro di stato** include un elenco di tutti i processi che sono stati in qualche modo modificati, con il relativo tempo di inizio pianificato, il tempo di completamento effettivo e lo stato del processo.

Fare clic su **Cancella registro stato** per eliminare tutte le voci dalla sezione Registro di stato.

Report casi atipici

Argomenti correlati:

- *Report investigativi*, pagina 119
- *Report di riepilogo*, pagina 121
Il report Casi atipici visualizza gli utenti di cui si sono registrate nel database le attività Internet più insolite. Il software Websense calcola l'attività media di tutti gli utenti in base alla categoria, al giorno, all'azione (denominata a volte "disposizione") e al protocollo. Visualizza quindi l'attività dell'utente che mostra statisticamente la varianza più significativa rispetto ai valori medi. Tale varianza viene calcolata come la deviazione standard dalla media.

1. Nella pagina principale dei report investigativi, generare un report di riepilogo che visualizza le informazioni per le quali si vogliono vedere i casi atipici. I report selezionati, in blu e sottolineati, adiacenti all'Utilizzo di Internet per campo, vengono riportati nel report Casi atipici.

Ad esempio per visualizzare i casi atipici in base agli accessi nell'ambito di una determinata categoria, selezionare Categoria dall'elenco Utilizzo di Internet per e selezionare Accessi come valore di Misura.



I report Casi atipici non possono venire generati in base ai tempi di navigazione. Se si inizia da un report di riepilogo che mostra i tempi di navigazione, il report Casi atipici viene basato sugli accessi.

2. Fare clic su Casi atipici.

Le righe vengono organizzate in ordine discendente con la varianza più alta all'inizio. Ciascuna riga riporta quanto segue:

- Totale (accessi o larghezza di banda) per l'utente, la categoria, il protocollo, il giorno e l'azione.
- Media (accessi o larghezza di banda) per tutti gli utenti, per una particolare categoria, protocollo, giorno e azione.
- Varianza dalla media per l'utente.
- 3. Per visualizzare l'attività di un singolo utente in questa categoria nel corso del tempo, fare clic sul nome dell'utente.

Ad esempio, se l'attività di un utente è particolarmente alta in un dato giorno, fare clic sul nome di quell'utente per aprire un report che consenta un approfondimento dell'attività svolta da quell'utente.

Output su file

Argomenti correlati:

- Report investigativi, pagina 119
- Stampa dei report investigativi, pagina 146

Dopo aver generato un report investigativo, si possono usare i pulsanti sopra il report per salvarlo in un file. Il pulsante su cui si fa clic determina il formato del file.

Opzione	Descrizione
	Salva il report in formato XLS . Se Microsoft Excel 2003 o versione successiva è installato nel computer dal quale si accede a Websense Manager, viene visualizzato un messaggio che consente di visualizzare o di salvare il report. In caso contrario, viene visualizzato un messaggio che richiede la selezione di una directory e di un nome di file per il report salvato.
	Usare le opzioni disponibili in Microsoft Excel per stampare, salvare o inviare il report via e-mail.
	Genera il report in formato PDF . Se Adobe Reader v7.0 o versione successiva è installato nel computer dal quale si accede a Websense Manager, viene visualizzato un messaggio che consente di visualizzare o di salvare il report. In caso contrario, viene visualizzato un messaggio che richiede la selezione di una directory e di un nome di file per il report salvato. Usare le opzioni disponibili in Adobe Acrobat per
	stampare, salvare o inviare il report via e-mail.

Stampa dei report investigativi

Argomenti correlati:	
• Report investigativi, pagina 119	
Output su file, pagina 145	

È possibile stampare i report investigativi procedendo come segue:

- Usando la funzione di stampa del broswer Web mentre il report è visualizzato.
- Creando un file PDF o XLS e quindi usando la funzione di stampa di Adobe Reader o di Microsoft Excel (vedere *Output su file*, pagina 145).

Sebbene l'impostazione dei report preveda la stampa da un browser, si consiglia di fare una prova di stampa per verificare i risultati.

I report Dettaglio mensile attività utente sono configurati per una stampa in modalità orizzontale. Tutti gli altri report sono configurati per una stampa verticale.

Quando si crea il proprio report (vedere *Report dettagliati flessibili*, pagina 127), la larghezza delle colonne varia a secondo delle informazioni inserite. L'orientamento della pagina diventa orizzontale se il report è più largo di 8,5 poll. (21,50 cm).

Il contenuto della pagina avrà una larghezza pari a 7,50 poll. (19 cm) o 10 poll. (25,4 cm) Nel caso di un formato A4, i margini verranno leggermente ridotti seppure

sempre all'interno del range di stampa. (L'impostazione predefinita per le dimensioni carta è Lettera ossia 8,5 x 11 poll. (21,50 x 27,9 cm). Se si sta lavorando con le dimensioni carta A4, accertarsi di modificare questa impostazione nel file wse.ini. Vedere *Opzioni di visualizzazione e di output*, pagina 344.

Accesso all'attività utente

Argomenti correlati:

- *Report investigativi*, pagina 119
- Configurazione delle preferenze per la creazione dei report, pagina 314
- Attività utente, pagina 346

L'attività utente di Websense consente di valutare le proprie attività di navigazione in Internet e di correggerle, se necessario, per conformarle ad eventuali linee guida aziendali. Questa funzione è conforme inoltre ai regolamenti governativi che richiedono alle organizzazioni di consentire agli utenti la verifica del tipo di informazioni raccolte.

Se la funzione Attività utente è stata attivata nella propria organizzazione, è possibile accedervi direttamente dal browser:

- 1. Inserire l'URL fornito da Websense Administrator oppure fare clic sul collegamento Attività utente nella pagina di accesso a Websense Manager che aprirà la pagina di accesso alla creazione automatica di report.
- 2. Se **Policy Server** mostra un elenco a discesa, scegliere l'indirizzo IP di Policy Server che registra le informazioni relative alle attività Internet.

Per assistenza, contattare il proprio Websense Administrator.

- 3. Inserire il Nome utente e la Password normalmente usati per collegarsi in rete.
- 4. Fare clic su Inizia sessione.

Websense Manager apre un report investigativo che mostra la propria attività Internet in base alle classi di rischio. Fare clic sui vari collegamenti ed elementi della pagina per accedere ad altre opzioni ed ottenere visualizzazioni alternative delle informazioni archiviate sulla propria attività. Consultare la **Guida** in linea per istruzioni sull'uso dei report. 7

Analisi del contenuto con le opzioni di Tempo reale

Argomenti correlati:

- *Opzioni di scansione*, pagina 151
- *Categorizzazione del contenuto e scansione per l'identificazione di minacce*, pagina 152
- Scansione dei file, pagina 153
- Eliminazione di un contenuto, pagina 155
- Creazione di report sull'attività di scansione in tempo reale, pagina 158

Il software di filtraggio Websense filtra l'attività svolta in Internet in base ai criteri attivi definiti e alle informazioni archiviate nel Master Database. Se si dispone di Websense Content Gateway o di Websense Web Security Gateway, è anche possibile analizzare i siti e il contenuto dei file Web in tempo reale.

A seconda dei moduli di cui si dispone, sono disponibili 2 opzioni di analisi in tempo reale: categorizzazione del contenuto e scansione in tempo reale a scopo di Sicurezza.

- Usare la funzione di **categorizzazione del contenuto** per valutare il contenuto degli URL che non sono stati bloccati (in base ai criteri attivi e alla categorizzazione degli URL di Websense Master Database) e restituire una categoria da usare nel filtraggio.
- Se si dispone di Websense Web Security Gateway, sono disponibili 3 opzioni di scansione di sicurezza in tempo reale.
 - L'opzione Scansione contenuti analizza il contenuto Web per rilevare potenziali minacce di sicurezza quali plishing (falsificazione di pagine Web), ridirezionamento dell'URL, minacce Web e proxy avoidance (elusione via Proxy).
 - L'opzione **Scansione file** analizza il contenuto dei file per determinare la categoria di una minaccia, come ad esempio virus, cavallo di Troia o worm.
 - L'opzione **Rimozione dei contenuti** elimina il contenuto attivo dalle pagine Web richieste.

Se una di queste opzioni è attiva, vengono analizzati soltanto i siti **non** ancora bloccati e basati sui propri criteri e sulla loro categorizzazione nel Websense Master Database. Per ulteriori informazioni, vedere *Opzioni di scansione*, pagina 151.



Importante

I filtri per restrizione di accesso e gli URL non filtrati prevalgono sulla categorizzazione in tempo reale.

Se un utente richiede l'accesso a un sito a cui è stato assegnato un filtro per restrizione di accesso (vedere *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172) o incluso nell'elenco degli URL non filtrati (vedere *Ridefinizione di un filtro per specifici siti*, pagina 186), la richiesta viene autorizzata anche se si effettua una scansione in tempo reale e si identificano delle minacce.

Per trarre vantaggio da queste funzioni di sicurezza in tempo reale, inserire in 2 campi la chiave di sottoscrizione che include il supporto di Websense Content Gateway or Websense Web Security Gateway:

- In Websense Manager (andare a Impostazioni > Account).
- Nell'interfaccia di gestione di Websense Content Gateway (andare alla scheda Configure > My Proxy > Subscription > Subscription Manager).

Occorrono diversi minuti affinché i due prodotti possano scaricare e sincronizzare i database necessari e quindi visualizzare tutte le funzioni di tempo reale in entrambi gli strumenti di gestione.

Opzioni di tempo reale di Websense

Le opzioni di tempo reale di Websense aiutano ad assicurare la continuità della sicurezza di rete. Usare queste opzioni per scannerizzare un contenuto di Internet e per assegnarlo a una categoria di filtraggio. Il risultato ottenuto in tempo reale viene inviato a Filtering Service che procede a filtrare il sito in base all'azione assegnata alla sua categorizzazione in tempo reale nell'ambito dei criteri attivi.

Download del database

Le opzioni di tempo reale usano piccoli database installati con Websense Web Security Gateway, il quale verifica, a intervalli regolari, la disponibilità di eventuali aggiornamenti dei database. Gli aggiornamenti di questi database si verificano indipendentemente dagli aggiornamenti del Master Database (tra cui gli aggiornamenti del database in tempo reale). Ogni volta che si usa il comando ./WCGAdmin start per avviare Websense Security Gateway, viene avviato lo scaricamento del database. Se il download non riesce, si tenterà un altro scaricamento ogni 15 minuti fino a quando lo scaricamento non viene completato.

L'intervallo predefinito per l'aggiornamento del database è di 15 minuti. È possibile modificare questo intervallo modificando il valore di **PollInterval** del file /**opt/bin**/ **downloadservice.ini** disponibile nel computer in cui è installato Websense Content Gateway.

Una volta modificato il file **downloadservice.ini**, occorre interrompere e riavviare Websense Content Gateway dalla riga di comando.

- Per interrompere, inserire: /opt/WCG/WCGAdmin stop
- Per riavviare, inserire: /opt/WCG/WCGAdmin start

Opzioni di scansione

Utilizzare la pagina **Impostazioni** >**Scansione in tempo reale** per attivare e configurare le opzioni in tempo reale. Le opzioni di scansione individuale vengono descritte in dettaglio nelle sezioni che seguono.

- Categorizzazione del contenuto e scansione per l'identificazione di minacce, pagina 152
- Scansione dei file, pagina 153
- Eliminazione di un contenuto, pagina 155

Per ciascuna opzione, si dispone di 2 scelte:

- Disattivo. Non si prevedono scansioni o blocchi in tempo reale. Questa opzione non offre alcuna ulteriore sicurezza.
- Consigliato o Attivo. Se il proprio sito è stato configurato per una scansione in tempo reale, questa impostazione consente la migliore performance. Le scansioni vengono eseguite sulla base di 2 fattori:
 - Gli elenchi Esegui sempre la scansione e Non eseguire mai la scansione della scheda Impostazioni > Scansione in tempo reale > Eccezioni (vedere *Perfezionamento della scansione*, pagina 156).
 - Se il software Websense ha rilevato che il sito comprende contenuti dinamici, i siti segnalati come comprendenti contenuti dinamici vengono scannerizzati. Il marcatore che identifica un sito come comprendente contenuti dinamici non è configurabile dall'utente.

I siti con contenuti dinamici inclusi nell'elenco Non eseguire mai la scansione non vengono scannerizzati.

• **Tutto.** Tutte le pagine Web richieste vengono scannerizzate. Le uniche eccezioni sono quelle riportate nell'elenco Non eseguire mai la scansione.

Questa opzione assicura il livello massimo di sicurezza, ma potrebbe considerevolmente rallentare la performance del sistema.



Attenzione

I siti riportati nell'elenco Non eseguire mai la scansione non vengono, in nessuna circostanza, analizzati. Se un sito incluso nell'elenco Non eseguire mai la scansione sembra essere compromesso, le opzioni di tempo reale non analizzano e non rilevano il codice dannoso.

Categorizzazione del contenuto e scansione per l'identificazione di minacce

Argomenti correlati:

- Opzioni di scansione, pagina 151
- Scansione dei file, pagina 153
- *Eliminazione di un contenuto*, pagina 155
- Perfezionamento della scansione, pagina 156
- Creazione di report sull'attività di scansione in tempo reale, pagina 158

I contenuti Web cambiano rapidamente. È stato statisticamente dimostrato che la maggior parte del contenuto Web è dinamico. Inoltre, Internet ospita una quantità sempre maggiore di contenuto generato dagli utenti come ad esempio quello pubblicato nelle comunità virtuali sociali. Questo materiale non è soggetto alle linee guida relative al contenuto o allo stile, che disciplinano i siti Web aziendali.

Se la categorizzazione di un contenuto è attiva, i siti selezionati vengono categorizzati in tempo reale e la categoria che ne risulta viene inviata al software di filtraggio di Websense per essere bloccata o autorizzata in base ai criteri attivi.



Consentire l'accesso completo a un determinato URL (vedere *Configurazione della registrazione di URL completi*, pagina 333) se si intende generare report su attività di scansione in tempo reale. In caso contrario, i record di registrazione includeranno soltanto il dominio (www.dominio.it) del sito categorizzato mentre le pagine individuali di un sito potrebbero rientrare in categorie diverse.

Se il proprio sito usa WebCatcher per segnalare a Websense, Inc. degli URL non categorizzati (vedere *Configurazione di WebCatcher*, pagina 324), gli URL

categorizzati tramite una categorizzazione del contenuto verranno inclusi ed inviati al Master Database.

Se la sottoscrizione posseduta include Websense Security Gateway, sarà anche possibile specificare che quel sito deve venire scannerizzato per minacce alla sicurezza.

Utilizzare la pagina **Impostazioni > Scansione in tempo reale** per specificare quando usare la categorizzazione e la scansione del contenuto.

1. Nell'area Categorizzazione dei contenuti selezionare **Disattivo** o **Attivo** (predefinizione) per determinare se eseguire la scansione. Vedere *Opzioni di scansione*, pagina 151.

Dopo aver determinato la categoria, qualsiasi altra opzione in tempo reale configurata viene applicata al fine di garantire un livello superiore di sicurezza.

- (Websense Security Gateway) Nell'area Scanning content (Scansione cotnenuti), selezionare Off (Disattivo) (predefinizione), Recommended (Consigliato) o All (Tutto) per determinare il livello di scansione.
- 3. Eseguire una delle operazioni seguenti:
 - Per aggiungere siti agli elenchi di Non eseguire mai la scansione o Esegui sempre la scansione, selezionare la scheda Eccezioni. Vedere *Perfezionamento della scansione*, pagina 156.
 - Per modificare le impostazioni di altre opzioni in tempo reale, proseguire alla pagina Opzioni comuni. Vedere *Scansione dei file*, pagina 153 e *Eliminazione di un contenuto*, pagina 155.
- 4. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

I report di presentazione contengono dettagli sui tentativi di accesso ai siti contenenti minacce. Vedere *Report di presentazione*, pagina 100 per ulteriori informazioni sull'esecuzione dei report Websense.

Scansione dei file

Argomenti correlati:

- Opzioni di scansione, pagina 151
- *Categorizzazione del contenuto e scansione per l'identificazione di minacce*, pagina 152
- Eliminazione di un contenuto, pagina 155
- Perfezionamento della scansione, pagina 156
- Creazione di report sull'attività di scansione in tempo reale, pagina 158

La scansione dei file analizza il contenuto dei file di applicazioni in entrata che gli utenti cercano di scaricare o di aprire in modalità remota. Questa opzione di tempo reale restituisce una categoria al software Websense di filtraggio in modo che il file venga autorizzato o bloccato, come necessario.

È buona pratica scannerizzare tutti i file **eseguibili** (ad esempio, i file **.exe** e **.dll**). È anche possibile identificare altri tipi di file da scannerizzare e definire una dimensione massima su sui eseguire la scansione.



Utilizzare la scheda **Impostazioni> Scansione in tempo reale > Opzioni comuni** per definire quando va usata la scansione dei file.

- Nell'area Scansione file, selezionare Disattivo, Consigliato (predefinizione) o Tutto per determinare il livello di scansione da applicare. Vedere *Opzioni di* scansione, pagina 151.
- 2. Fare clic su Impostazioni avanzate.
- 3. L'opzione **Esegui la scansione di tutti i tipi di file con contenuto eseguibile** è selezionata per predefinizione. Deselezionare questa casella di controllo se si preferisce visualizzare tutte le estensioni dei file da scannerizzare.
- 4. Per specificare altri tipi di file da scannerizzare, inserire l'estensione del file (ad es.**ppt** o **wmv**) e fare quindi clic su **Aggiungi**. L'estensione dei file può contenere soltanto caratteri alfanumerici, un segno di sottolineatura (_) o una lineetta (-). Non includere il punto che precede l'estensione.

Per eliminare un'estensione di file dall'elenco Estensioni file selezionate, selezionare l'estensione da eliminare e fare quindi clic su **Rimuovi**.

- In Opzioni, inserire le dimensioni massime per i file da scannerizzare (per predefinizione, 10 MB). Selezionare **Personalizza** per inserire delle dimensioni fino a 4096 MB (4 GB). I file con dimensioni superiori a quelle specificate non vengono scannerizzati.
- 6. Eseguire una delle operazioni seguenti:
 - Per aggiungere siti agli elenchi di Non eseguire mai la scansione o Esegui sempre la scansione, selezionare la scheda Eccezioni. Vedere *Perfezionamento della scansione*, pagina 156.
 - Per modificare le impostazioni di altre opzioni di tempo reale, proseguire alla scheda Opzioni comuni. Vedere *Categorizzazione del contenuto e scansione per l'identificazione di minacce*, pagina 152 e *Eliminazione di un contenuto*, pagina 155.
- 7. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Numerosi report di presentazione contengono dettagli sui tentativi di scaricamento di file che rappresentano un rischio. Vedere *Report di presentazione*, pagina 100 per istruzioni sull'esecuzione dei report Websense.

Vedere *Gestione del traffico in base al tipo di file*, pagina 197 per informazioni sul blocco dei file in base al tipo e alla categoria di URL.

Eliminazione di un contenuto

Argomenti correlati:

- Opzioni di scansione, pagina 151
- *Categorizzazione del contenuto e scansione per l'identificazione di minacce*, pagina 152
- Scansione dei file, pagina 153
- Perfezionamento della scansione, pagina 156
- Creazione di report sull'attività di scansione in tempo reale, pagina 158

Potenziali minacce al sistema possono essere nascoste nel contenuto attivo inviato con le pagine Web. Un metodo per preservare l'integrità del sistema è accertare che questo tipo di contenuto non entri mai.

Le opzioni in tempo reale consentono di specificare che il contenuto di determinati linguaggi di scripting (ActiveX, JavaScript o VB Script) venga eliminato dalle pagine Web in entrata. Se l'opzione di eliminazione del contenuto è attiva, il contenuto dei linguaggi di scripting specificati verrà eliminato dai siti segnalati come siti contenenti contenuti dinamici o dai siti inclusi nell'elenco Esegui sempre la scansione (vedere *Opzioni di scansione*, pagina 151)

Il contenuto viene eliminato soltanto dopo che le opzioni in tempo reale hanno categorizzato il sito e il software di filtro Websense ha determinato i criteri da applicare.

Le pagine Web basate su un contenuto attivo che è stato eliminato, non funzioneranno come previsto. Per consentire un accesso completo ai siti che richiedono un contenuto attivo, disattivare l'opzione di eliminazione del contenuto o aggiungere i siti all'elenco Non eseguire mai la scansione.

L'utente che richiede una pagina con un contenuto attivo non riceverà alcuna notifica riguardo all'eliminazione del contenuto.

Utilizzare la scheda **Impostazioni > Scansione in tempo reale > Opzioni comuni** per specificare quando eliminare un contenuto dai siti con contenuto dinamico.

1. Nell'area Rimozione dei contenuti, selezionare i tipi di contenuti attivi che dovrebbero venire eliminati dalle pagine Web in entrata.

- 2. Per modificare le impostazioni di altre opzioni in tempo reale, vedere:
 - *Categorizzazione del contenuto e scansione per l'identificazione di minacce*, pagina 152
 - *Scansione dei file*, pagina 153.
- 3. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Per disattivare l'eliminazione di contenuti per ogni linguaggio selezionato, deselezionare la relativa casella di controllo.

Perfezionamento della scansione

Argomenti correlati:

- Opzioni di scansione, pagina 151
- *Categorizzazione del contenuto e scansione per l'identificazione di minacce*, pagina 152
- Scansione dei file, pagina 153
- Eliminazione di un contenuto, pagina 155

Usare gli elenchi Esegui sempre la scansione e Non eseguire mai la scansione per personalizzare l'azione svolta dalle opzioni di scansione Consigliato e Tutto.

- Se si imposta un'opzione di tempo reale su Consigliato o su Attivo, i siti con contenuto dinamico e i siti inclusi nell'elenco Esegui sempre la scansione vengono scannerizzati (vedere *Opzioni di scansione*, pagina 151). I siti inclusi nell'elenco Non eseguire mai la scansione vengono ignorati.
- Se si imposta un'opzione di tempo reale su Tutto, i siti inclusi nell'elenco Non eseguire mai la scansione vengono ignorati. Questa scansione migliora la performance.

Usare con cautela l'elenco Non eseguire mai la scansione. Se un sito incluso in questo elenco viene compromesso, Websense Security Gateway non scannerizza quel sito al fine di identificare il problema di sicurezza.

Usare la pagina **Impostazioni > Scansione in tempo reale > Eccezioni** per inserire automaticamente e modificare le voci degli elenchi Esegui sempre la scansione e Non eseguire mai la scansione.

Per aggiungere dei siti all'elenco Esegui sempre la scansione e Non eseguire mai la scansione:

1. Inserire i nomi dei siti nel campo URL.

Inserire soltanto il nome dell'host (ad es. **thissite.com**). Non è necessario inserire l'URL completo. Accertarsi di inserire sia il dominio sia l'estensione; **thissite.com** e **thissite.net** sono voci distinte.

È consentito inserire soltanto uno dei nomi host per volta.

 Nella colonna Opzioni, selezionare le opzioni in tempo reale da applicare a tutti i siti inseriti. Si può selezionare una o più opzioni. Tenere presente che Minacce per la sicurezza si riferisce soltanto alla scansione del contenuto, non alla scansione dei file. Gli elenchi Esegui sempre la scansione e Non eseguire mai la scansione non determinano la scansione dei file.

Per applicare diverse opzioni a diversi siti, inserire i siti separatamente.

3. Selezionare Aggiungi a Esegui sempre la scansione o Aggiungi a Non eseguire mai la scansione.

Un sito può essere incluso in uno solo dei 2 elenchi. Non è ad esempio consentito specificare che lo stesso sito debba venire sempre scannerizzato per identificare minacce e mai per l'eliminazione di un contenuto.

- Per modificare l'elenco in cui va inserito un determinato sito, selezionare innanzi tutto il sito e quindi usare i pulsanti a freccia verso destra (>) o verso sinistra (>) per spostare il sito in un nuovo elenco.
- Per eliminare un sito da entrambi gli elenchi, selezionare il sito e fare quindi clic su **Rimuovi**.
- Al termine della procedura, fare clic su OK per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su Salva tutto.

Per modificare le opzioni di scansione associate a un sito:

- 1. Selezionare l'elenco Esegui sempre la scansione o Non eseguire mai la scansione e fare quindi clic su **Modifica**.
- 2. Nella finestra Modifica regole, selezionare le nuove opzioni per il nome host:
 - Nessuna modifica mantiene l'impostazione corrente.
 - Attiva indica che il contenuto verrà scannerizzato per l'opzione specificata, come ad esempio la categorizzazione del contenuto.
 - Disattiva indica che non si effettuerà alcuna scansione per l'opzione specificata. Se un'opzione viene disattivata, la performance può migliorare, ma la sicurezza potrebbe venire compromessa.
- 3. Una volta terminate le modifiche, fare clic su **OK** per ritornare alla finestra Modifica regole della scheda Eccezioni.
- 4. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Creazione di report sull'attività di scansione in tempo reale

Argomenti correlati:

- Opzioni di scansione, pagina 151
- *Categorizzazione del contenuto e scansione per l'identificazione di minacce*, pagina 152
- Scansione dei file, pagina 153
- Eliminazione di un contenuto, pagina 155

Se la sottoscrizione ricevuta include funzioni di scansione in tempo reale, sarà possibile analizzare gli effetti esercitati da tale funzioni sui report di presentazione e sui report investigativi.

Nella pagina Report di presentazione, è disponibile un gruppo di report dal nome Minacce di sicurezza in tempo reale. Questi report sono rivolti specificatamente alle attività con potenziali minacce. Come per tutti i report di presentazione, è possibile copiare un report su potenziali minacce della sicurezza e modificare il suo filtro per migliorare le informazioni incluse quando si genera un report da quella copia.

Alcuni report su potenziali minacce della sicurezza includono una colonna ID minaccia. Si può fare clic su un ID minaccia per aprire la pagina Websense Security Labs che descrive il tipo di minaccia identificato.

Altri report di presentazione contengono informazioni su attività di scansione in tempo reale, nonché attività di filtraggio standard. Copiare un report predefinito e modificare il suo filtro per creare un report riguardante in modo specifico attività di scansione in tempo reale.

Importante

Attivare la registrazione degli URL completi (vedere *Configurazione della registrazione di URL completi*, pagina 333) per accertare che i report sulle attività di scansione in tempo reale siano accurati. In caso contrario, i report includeranno soltanto il dominio (WWW.dominio.it) del sito categorizzato anche se le pagine individuali del sito potrebbero rientrare in categorie diverse o contenere diversi tipi di minacce.

Ad esempio, il report Dettaglio URL completi per categoria che fa parte del gruppo di Attività Internet del Catalogo report contiene un elenco dettagliato di ciascun URL a cui si è acceduto all'interno di ciascuna categoria. Per creare un report specifico sulla scansione in tempo reale, copiare il report Dettaglio URL completi per categoria e modificare il relativo filtro. Nella scheda Azioni, selezionare soltanto le azioni autorizzate e bloccate che sono associate alla scansione in tempo reale. Nella scheda Opzioni, modificare il titolo del Catalogo report e il nome del report per segnalarlo come un report sulla scansione in tempo reale. Ad esempio si possono modificare il nome e il titolo in Tempo reale: Dettaglio URL completi per categoria.

I report investigativi possono anche venire usati per esaminare più in dettaglio le attività di scansione in tempo reale.

- 1. Nell'elenco a discesa Visualizza utilizzo Internet per, selezionare Azione.
- Nel report che ne risulta, fare clic su un'azione in tempo reale, come ad esempio Categoria bloccata in tempo reale, per visualizzare un elenco di opzioni di approfondimento dei dettagli.
- 3. Fare clic sull'opzione di approfondimento dei dettagli desiderata, come ad esempio Categoria o Utente.
- 4. Fare clic sul valore degli Accessi o sulla barra di una riga qualsiasi per visualizzare i relativi dettagli
- 5. Fare clic su **Modifica report** nell'area superiore della pagina, per aggiungere la colonna degli URL completi al report.

Vedere *Report investigativi*, pagina 119 per ulteriori informazioni sull'uso di tutte le funzioni relative ai report investigativi.

Metodo di registrazione delle scansioni in tempo reale

Quando si usano le opzioni di scansione in tempo reale, tenere presente che esistono differenze nel modo in cui le attività di filtraggio standard del Web e le attività di scansione in tempo reale vengono registrate.

Per l'attività di filtraggio normale del Web, sono disponibili varie opzioni per ridurre le dimensioni del database di registrazione.

- Attivare visite per registrare soltanto un record per ciascun sito Web richiesto. Vedere Configurazione dei file cache di registro, pagina 321.
- Attivare consolidamento per unificare in un unico record del registro diverse richieste con alcuni elementi in comune. Vedere Configurazione delle opzioni di consolidamento, pagina 322.
- Disattivare Registrazione URL completo per registrare soltanto il nome del dominio (www.dominio.it) per ciascuna richiesta e non il percorso alla pagina specifica del dominio (/products/productA). Vedere Configurazione della registrazione di URL completi, pagina 333.
- Attivare **Registrazione categorie selettiva** per limitare la registrazione alle categorie selezionate ritenute cruciali per la propria organizzazione. Vedere *Configurazione di Filtering Service per la registrazione*, pagina 314.

Le funzioni di scansione in tempo reale, tuttavia, sono legate solo parzialmente a queste impostazioni. Quando una scansione in tempo reale analizza un sito, crea 2 record separati per il registro.

 I record dei filtri Web traggono vantaggio da qualsiasi impostazione implementata per la riduzione delle dimensioni, e sono disponibili per tutti i report di filtraggio Web. • I record in tempo reale ignorano la maggior parte delle impostazioni di riduzione delle dimensioni. Ogni accesso viene registrato separatamente, le richieste a tutte le categorie vengono registrate e i record non vengono unificati. Il record in tempo reale viene generato indipendentemente dal fatto che il sito sia bloccato o autorizzato come risultato della scansione in tempo reale. Soltanto l'impostazione di registrazione degli URL completi viene rispettata per quanto riguarda i record in tempo reale.

Se si sono attivate le opzioni di riduzione delle dimensioni del database di registrazione, i numeri che appaiono nei report in tempo reale potrebbero **non** corrispondere a quelli contenuti nei report di filtro standard anche se i report sono stati configurati per gli stessi utenti, per lo stesso periodo di tempo e per le stesse categorie. Ad esempio, se si è scelto di registrare le visite e un utente richiede un sito analizzato da una funzione di scansione in tempo reale, la richiesta di questo utente verrà visualizzata, nei report di filtro standard, come una visita, ma potrebbe venire visualizzata come una serie di molteplici accessi nei report sulla scansione in tempo reale.

Per confrontare i dati ottenuti dai filtri standard e da quelli del tempo reale, **disattivare** le impostazioni di riduzione delle dimensioni del database di registrazione. Poiché questo potrebbe comportare un database di dimensioni molto alte e a rapida crescita, accertarsi che il computer in cui è installato il database di registrazione abbia uno spazio su disco sufficiente per l'archiviazione e l'elaborazione, nonché una capacità di memoria adeguata.

Vedere *Amministrazione della creazione dei report*, pagina 309 per ulteriori informazioni sulle impostazioni di configurazione relative alla riduzione delle dimensioni. Vedere *Report di presentazione*, pagina 100 e *Report investigativi*, pagina 119 per informazioni sulla generazione dei report.

Filtro per i client remoti

Argomenti correlati:

- Modalità di funzionamento di Remote Filtering, pagina 162
- Configurazione delle impostazioni di Remote Filtering, pagina 168

Gli utenti di molte organizzazione dispongono di laptop che a volte portano con sé fuori dall'ambiente di rete. Per gli utenti remoti che usano il sistema operativo Microsoft Windows, è possibile filtrare richieste Internet implementando Websense Remote Filtering, una funzione opzionale disponibile sia per Websense Web Security che per Websense Web Filter.

Remote Filtering monitora il traffico HTTP, SSL e FTP, applicando i criteri assegnati a singoli utenti o a gruppi, o applica i criteri predefiniti, a seconda di come l'utente si collega al computer remoto. Remote Filtering non filtrerà in base ai criteri assegnati ai computer o alla rete. Per ulteriori informazioni, vedere *Identificazione degli utenti remoti*, pagina 165.

I filtri basati sulla larghezza di banda non sono supportati per i client remoti (vedere *Uso di Bandwidth Optimizer per la gestione della larghezza di banda*, pagina 195). La larghezza di banda generata dal traffico remoto non viene inclusa nelle misurazioni e nei report associati alla larghezza di banda.

Il filtraggio di Remote Filtering riguardo a richieste FTP e SSL, come ad esempio HTTPS, può essere costituito soltanto da un blocco a da un'autorizzazione all'accesso. Se un utente remoto richiede l'accesso a un sito FTP o HTTPS, ad esempio, da una categoria a cui è stata assegnata un'azione di assegnazione durata o di conferma, il sito viene bloccato per i client di Remote Filtering. Quando questi computer navigano dall'interno di una rete, le azioni di filtro per il tempo assegnato e la conferma vengono applicate normalmente.

Per implementare Remote Filtering, occorre aver installato i componenti seguenti:

 Remote Filtering Server deve trovarsi entro il firewall più esterno e i computer remoti devono disporre dell'autorizzazione di comunicazione con il server. Normalmente viene installato nella *zona demilitarizzata di rete*, Demilitarized Zone – DMZ, ossia fuori dal firewall che protegge il resto della rete. È possibile installare fino a 3 server di Remote Filtering per disporre di funzioni di failover. • Il client Remote Filtering deve essere installato su ciascun computer dotato del sistema operativo Windows e viene utilizzato fuori dalla rete.



Tutte le comunicazioni tra il client Remote Filtering e Remote Filtering Server vanno autenticate e codificate

Modalità di funzionamento di Remote Filtering

Argomenti correlati:

- Internamente alla rete, pagina 163
- Esternamente alla rete, pagina 164
- Identificazione degli utenti remoti, pagina 165
- Comunicazione con il server non riuscita, pagina 166
- Virtual Private Network (VPN), pagina 167
- Configurazione delle impostazioni di Remote Filtering, pagina 168

Se un computer remoto invia una richiesta via HTPP, SSL o FTP, il suo client Remote Filtering comunica con Remote Filtering Server. Remote Filtering Server comunica con Websense Filtering Service per determinare l'azione da svolgere. Remote Filtering Server risponde quindi al client Remote Filtering consentendo l'accesso al sito o inviando il messaggio di blocco del caso.

Se il browser del computer in cui è installato il client Remote Filtering invia una richiesta via HTTP, SSL o FTP, il client Remote Filtering deve decidere se effettuare una query in Remote Filtering Server relativamente alla richiesta. Questa determinazione dipende dalla posizione del computer rispetto alla rete.

Internamente alla rete

Argomenti correlati:

- Modalità di funzionamento di Remote Filtering, pagina 162
- Esternamente alla rete, pagina 164
- Identificazione degli utenti remoti, pagina 165
- Comunicazione con il server non riuscita, pagina 166
- Virtual Private Network (VPN), pagina 167
- Configurazione delle impostazioni di Remote Filtering, pagina 168

Quando si avvia un computer *dall'interno* della rete, il client Remote Filtering tenta l'invio di un pacchetto **heartbeat** a Remote Filtering Server nella DMZ della rete. L'invio dell'heartbeat riesce in quanto la sua porta è aperta nel firewall interno.



In questo caso, il client Remote Filtering diventa passivo e non effettua query in Remote Filtering Server riguardo a richieste di accesso in Internet. Queste richieste vengono invece inviate direttamente al prodotto di integrazione (come ad esempio Cisco Pix, Microsoft ISA Server) oppure a Network Agent di Websense. La richiesta viene quindi filtrata come qualsiasi altra richiesta interna.

Esternamente alla rete

Argomenti correlati:

- Modalità di funzionamento di Remote Filtering, pagina 162
- Internamente alla rete, pagina 163
- Identificazione degli utenti remoti, pagina 165
- Comunicazione con il server non riuscita, pagina 166
- Virtual Private Network (VPN), pagina 167
- Configurazione delle impostazioni di Remote Filtering, pagina 168

Quando si avvia un computer *esternamente* alla rete, il client Remote Filtering tenta l'invio di un pacchetto heartbeat a Remote Filtering Server. L'invio dell'heartbeat non riesce in quanto la sua porta è bloccata nel firewall esterno.



L'invio non riuscito dell'heartbeat comporta l'invio da parte del client Remote Filtering a Remote Filtering Server nella DMZ della rete, di una query relativa ad ogni richiesta HTTP, SSL o FTP attraverso la porta configurata (predefinizione 80). Remote Filtering Server inoltra quindi la richiesta di filtraggio al Websense Filtering Service internamente alla rete. Filtering Service valuta la richiesta e invia una riposta a Remote Filtering Server. La risposta viene infine inviata al computer remoto. Se il sito è bloccato, il client Remote Filtering richiede e riceve la relativa pagina di blocco che viene quindi visualizzata per l'utente.

Il client Remote Filtering ritarda qualsiasi richieste filtrata fino a quando non riceve una risposta da Remote Filtering Server. In base alla risposta ricevuta, il client Remote Filtering autorizza l'accesso al sito o visualizza la pagina di blocco. Un file del registro monitora le attività di Remote Filtering, come ad esempio le entrate e le uscite su rete, le modalità "fail open" (consente il passaggio di traffico non controllato) o "fail closed" (blocca il traffico - chiusura contro errori) e il riavvio del client. Il client Remote Filtering crea il file registro al suo primo avvio. L'utente determina la presenza e le dimensioni del file registro. Vedere *Configurazione delle impostazioni di Remote Filtering*, pagina 168.

Identificazione degli utenti remoti

Argomenti correlati:

- Modalità di funzionamento di Remote Filtering, pagina 162
- Internamente alla rete, pagina 163
- Esternamente alla rete, pagina 164
- Comunicazione con il server non riuscita, pagina 166
- Virtual Private Network (VPN), pagina 167
- Configurazione delle impostazioni di Remote Filtering, pagina 168

La modalità con cui un utente si collega al computer remoto determina i criteri che verranno applicati.

Se un utente si collega usando le credenziali (dati di accesso alla directory di rete) di dominio memorizzate nella cache, Websense Filtering Service sarà in grado di identificare il nome utente e applicherà quindi al computer remoto i criteri definiti per l'utente o per il gruppo. L'attività in Internet verrà registrata sotto il nome utente di rete.

Se l'utente accede con l'account utente locale, Filtering Service non può identificare il nome utente e applica quindi i criteri predefiniti. L'attività in Internet verrà registrata sotto il nome utente locale. Remote Filtering non filtrerà in base ai criteri assegnati ai computer o alla rete.

Nota

Gli utenti remoti vengono sempre filtrati in base alle loro credenziali di accesso, come qui descritto. Le impostazioni selettive di autenticazione non sono applicabili a questi utenti.

Comunicazione con il server non riuscita

Argomenti correlati:

- Modalità di funzionamento di Remote Filtering, pagina 162
- Internamente alla rete, pagina 163
- Esternamente alla rete, pagina 164
- Identificazione degli utenti remoti, pagina 165
- Virtual Private Network (VPN), pagina 167
- Configurazione delle impostazioni di Remote Filtering, pagina 168

L'applicazione del filtro si verifica quando il client Remote Filtering, esterno alla rete, stabilisce la comunicazione con Remote Filtering Server nella DMZ della rete. Potrebbe tuttavia accadere che la comunicazione non riesca.

L'azione che il client Remote Filtering deve usare se non può stabilire il contatto con Remote Filtering Server è configurabile. Per predefinizione, il client Remote Filtering usa l'impostazione **fail open** (autorizza traffico non controllato), che autorizza tutte le richieste via HTTP, SSL e FTP quando la comunicazione tra questi componenti non può essere stabilita. Il client Remote Filtering continua a cercare di comunicare con Remote Filtering Server. Se la comunicazione non può essere stabilita, vengono applicati i criteri di filtro appropriati.

Se il client Remote Filtering è stato configurato per **fail closed** (chiusura contro errori) viene applicato un timeout (predefinizione: 15 minuti). L'orologio inizia a contare all'avvio del computer remoto. Il client Remote Filtering tenta immediatamente il collegamento con Remote Filtering Server e continua ciclicamente lungo tutti i Remote Filtering Server fino a quando il collegamento non viene stabilito.

Se l'utente dispone di un accesso Web all'avvio, non viene applicato alcun filtro (ossia, tutte le richieste vengono autorizzate) fino a quando il client Remote Filtering non si collega a Remote Filtering Server. Se la comunicazione viene stabilita, vengono applicati i criteri di filtro appropriati.

Se il client Remote Filtering non riesce a collegarsi entro il periodo di timeout configurato, tutti gli accessi a Internet vengono bloccati (chiusura contro errori) fino a quando non viene stabilito il collegamento con Remote Filtering Server.

Nota

Se per un motivo qualunque Remote Filtering Server non riesce a stabilire il collegamento con Websense Filtering Service, viene restituito un errore al client Remote Filtering e il filtro adotta la modalità "fail open" (autorizza traffico non controllato).

Il periodo di timeout consente agli utenti, che pagano per avere accesso a Internet durante i loro viaggi, di avviare il computer e a stabilire il collegamento senza incorrere in un blocco di accesso. Se l'utente non stabilisce il collegamento con Internet prima della scadenza del periodo di timeout di 15 minuti, l'accesso al Web non potrà venire stabilito durante tale sessione. In questo caso, l'utente dovrà riavviare il computer per iniziare nuovamente il tempo di timeout previsto.

Per modificare l'impostazione di autorizzazione (fail open) o di blocco (fail closed) e modificare il valore del timeout, vedere *Configurazione delle impostazioni di Remote Filtering*, pagina 168.

Virtual Private Network (VPN)

Argomenti correlati:

- Modalità di funzionamento di Remote Filtering, pagina 162
- Internamente alla rete, pagina 163
- Esternamente alla rete, pagina 164
- Identificazione degli utenti remoti, pagina 165
- Comunicazione con il server non riuscita, pagina 166
- Configurazione delle impostazioni di Remote Filtering, pagina 168

Websense Remote Filtering supporta i collegamenti VPN, incluso lo split-tunneled con il traffico di rete aziendale che va nella VPN e il traffico Internet direttamente verso Internet. Quando si collega un computer alla rete interna tramite la VPN (non split-tunneled), il client Remote Filtering può inviare un pacchetto heartbeat a Remote Filtering Server. Ciò comporta che il client Remote Filtering diventi passivo e che tutte le richieste HTTP, SSL e FTP inviate dal computer remoto vengano filtrate dal prodotto di integrazione interno o da Network Agent, come accade con altri computer collegati in rete.

Quando un computer remoto si collega alla rete interna tramite un client VPN splittunneled, il client Remote Filtering rileva questa condizione e non invia un pacchetto heartbeat a Remote Filtering Server. Il client Remote Filtering presume di trovarsi in modalità di funzionamento esterno e invia richieste a Remote Filtering Server per l'applicazione del filtro.

Il software Websense supporta la modalità "split-tunneled" per i seguenti client VPN:

- Checkpoint SecureClient
- Cisco
- ♦ Juniper/Netscreen
- Microsoft PPTP
- Nokia
- Nortel
- SonicWALL

Configurazione delle impostazioni di Remote Filtering

Argomenti correlati:

- Modalità di funzionamento di Remote Filtering, pagina 162
- Internamente alla rete, pagina 163
- Esternamente alla rete, pagina 164
- Identificazione degli utenti remoti, pagina 165
- Comunicazione con il server non riuscita, pagina 166
- Virtual Private Network (VPN), pagina 167

Gli utenti con qualifica totale di Super Administrator possono usare la pagina Impostazioni > Generale > Remote Filtering per configurare le opzioni che incidono su tutti i client Remote Filtering associati con questa installazione.

Per ulteriori informazioni sul funzionamento di Remote Filtering, vedere *Modalità di funzionamento di Remote Filtering*, pagina 162.

1. Selezionare la casella di controllo **Chiusura contro errori** per bloccare l'accesso a Internet da parte dei client Remote Filtering a meno che i rispettivi computer non siano in comunicazione con Remote Filtering Server.

Per impostazione predefinita, questa opzione non è selezionata e ciò significa che gli utenti remoti hanno un accesso non filtrato a Internet nel caso in cui i loro computer non possano comunicare con Remote Filtering Server.

2. Se si seleziona l'opzione Chiusura contro errori, utilizzare il campo **Timeout chiusura contro errori** per selezionare il numero di minuti - fino a 60 (predefinizione: 15) - oppure scegliere l'opzione **Nessun timeout**.

Durante il periodo di timeout, tutte le richieste HTPP, SSL e FTP vengono autorizzate.

Se il client Remote Filtering non riesce a collegarsi con Remote Filtering Server entro il periodo di timeout configurato, tutti gli accessi a Internet verranno bloccati (chiusura contro errori).

La selezione dell'opzione **Nessun timeout** potrebbe bloccare un computer remoto prima che l'utente possa stabilire il collegamento con Internet, ad esempio da un hotel o tramite un provider che offre un tipo di accesso a pagamento in base all'uso. Il client Remote Filtering continua inoltre il tentativo di comunicazione con Remote Filtering Server.



Attenzione

Websense, Inc., non consiglia la selezione dell'opzione Nessun timeout né consiglia l'impostazione di un lungo periodo di timeout. 3. Selezionare **Dimensioni massime per il file di registro**(in megabyte), fino a 10. Scegliere **Nessun registro** per disattivare la registrazione.

Questa opzione determina le dimensioni e l'esistenza del file di registro che il computer remoto crea quando viene scollegato dal Remote Filtering Server. Il file registro rileva gli eventi seguenti:

- Il computer esce dalla rete
- Il computer ritorna in rete
- Il client Remote Filtering viene riavviato
- Si verifica la condizione di autorizzazione del traffico non controllato
- Si verifica la condizione di chiusura contro errori
- Il client Remote Filtering riceve un aggiornamento dei criteri

Il computer conserva le 2 registrazioni più recenti. Queste registrazioni possono venire utilizzate per diagnosticare/risolvere problemi di collegamento o altri problemi associati a Remote Filtering.

Perfezionamento dei criteri di filtraggio

Ai fini della massima semplicità, il filtraggio dell'uso di Internet prevede un unico criterio che applichi un filtro di categoria e un filtro di protocollo, 24 ore al giorno, 7 giorni alla settimana. Il software Websense dispone tuttavia di strumenti che vanno molto al di là di questa modalità di filtraggio di base per consentire il livello di flessibilità necessario alla gestione dell'uso di Internet. A questo proposito, è possibile:

- creare filtri per restrizioni di accesso al fine di bloccare l'accesso a tutti i siti ad eccezione di un elenco di siti specifici per determinati utenti (vedere *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172).
- creare **categorie personalizzate** per ridefinire la modalità di filtraggio di alcuni siti selezionati (vedere *Gestione delle categorie*, pagina 179).
- ricategorizzare gli URLs per spostare dei siti dalla loro assegnazione predefinita ad una categoria del Master Database a un'altra categoria definita da Websense o a una categoria personalizzata (vedere URL ricategorizzati, pagina 188).
- definire degli URL non filtrato per consentire agli utenti di accedere a determinati siti, anche se tali siti sono assegnati a una categoria bloccata in base al filtro di categoria attivo (vedere *Definizione di URL non filtrati*, pagina 187).
- implementare restrizioni relative all'uso della larghezza di banda e bloccare gli utenti dall'accesso a categorie e protocolli altrimenti autorizzati, nel caso l'uso della larghezza di banda raggiunga una soglia specificata.
- definire le parole chiave da utilizzare per bloccare i siti che fanno parte di categorie e di protocolli autorizzati, se il blocco in base alla parole chiave è stato attivato (vedere *Filtro basato su parole chiave*, pagina 184).
- definire i tipi di file utilizzati per bloccare i siti che fanno parte di categorie e di protocolli autorizzati, se il blocco in base alla parole chiave è stato attivato (vedere *Gestione del traffico in base al tipo di file*, pagina 197).

Restrizione dell'accesso degli utenti a un elenco definito di siti Internet

Argomenti correlati:

- Filtri per restrizioni di accesso e priorità di un filtro, pagina 172
- Creazione di un filtro per restrizioni di accesso, pagina 174
- Modifica di un filtro per restrizioni di accesso, pagina 174

I filtri per restrizioni di accesso offrono un metodo molto preciso di filtraggio degli accessi a Internet. Ciascun filtro per restrizioni di accesso è costituito da un elenco di siti Web. Come i filtri di categoria, i filtri per restrizioni di accesso vengono aggiunti ai criteri e applicati nel corso di un determinato periodo di tempo. Se un filtro per restrizioni di accesso è attivo all'interno di un singolo criterio, gli utenti assegnati a quel criterio potranno visitare soltanto i siti inclusi nell'elenco. Tutti gli altri siti saranno bloccati.

Ad esempio, se il criterio di Primo livello prevede un filtro per restrizioni di accesso che consente soltanto l'accesso alcuni siti educativi e di riferimento bibliografico, gli studenti soggetti a questo criterio di Primo livello potranno visitare soltanto quei siti e nessun altro.



Importante

Se un filtro per restrizioni di accesso è attivo, il software Websense verifica soltanto la presenza nel filtro di un sito richiesto. Non viene eseguita un'altra verifica.

Ciò significa che se un sito autorizzato dal filtro viene infettato da un codice dannoso, le richieste di accesso a quel sito da parte degli utenti vengono sempre autorizzate indipendentemente dalla categorizzazione del sito nel Master Database o dalla funzione di Scansione in tempo reale.

Se un filtro per restrizioni di accesso è attivo, verrà visualizzata una pagina di blocco per gli URL richiesti che non sono inclusi in quel filtro.

Il software Websense può supportare fino a 2.500 filtri per restrizioni di accesso, contenenti un totale di 25.000 URL.

Filtri per restrizioni di accesso e priorità di un filtro

In alcuni casi, potrebbe essere applicabile a un singolo utente più di un criterio. Ciò si verifica se un utente appartiene a più di un gruppo e se i gruppi sono soggetti

all'applicazione di diversi criteri. Inoltre un URL potrebbe essere incluso in un filtro per restrizioni di accesso ed essere definito come un URL non filtrato.

Se molteplici criteri definiti per un gruppo sono applicabili a un utente, l'impostazione **Utilizzare blocchi più restrittivi** (vedere *Ordine di filtraggio*, pagina 82) determina come l'utente deve venire filtrato. Per impostazione predefinita, questa funzione è disattiva.

Il software Websense determina quali impostazioni di filtraggio sono meno restrittive a livello di filtro. Nei casi in cui un utente possa venire filtrato da molteplici criteri, uno dei quali applica un filtro per restrizioni di accesso, un criterio "meno restrittivo" potrebbe essere controproducente.

Se l'opzione Utilizzare blocchi più restrittivi è impostata su Disattivato:

- Se il filtro di categoria **Blocca sempre** e un filtro per restrizioni di accesso sono applicabili, il filtro per restrizioni di accesso è considerato meno restrittivo.
- Se un altro filtro di categoria e un filtro per restrizioni di accesso sono applicabili, il filtro di categoria è sempre considerato meno restrittivo.

Ciò significa che anche se il filtro per restrizioni di accesso autorizza l'accesso al sito e il filtro di categoria blocca il sito, il sito viene bloccato.

Se l'opzione **Utilizzare blocchi più restrittivi** è **Attiva**, un filtro per restrizioni di accesso è considerato meno restrittivo di qualsiasi filtro di categoria, ad eccezione di Blocca sempre.

La tabella che segue riepiloga come l'impostazione **Utilizzare blocchi più restrittivi** agisce sul filtro nel caso dell'applicazione di molteplici criteri:

	Utilizzare blocchi più restrittivi - Disattivato	<i>Utilizzare blocchi più restrittivi - Attivato</i>
filtro per restrizioni di accesso +filtro di categoria Blocca sempre	filtro per restrizioni di accesso (richiesta autorizzata)	Blocca sempre (richiesta bloccata)
filtro per restrizioni di accesso + categoria autorizzata	filtro di categoria (richiesta autorizzata)	filtro per restrizioni di accesso (richiesta autorizzata)
filtro per restrizioni di accesso + categoria bloccata	filtro di categoria (richiesta bloccata)	filtro per restrizioni di accesso (richiesta autorizzata)
filtro per restrizioni di accesso + Categoria Assegna durata/ Conferma	filtro di categoria (richiesta limitata da Assegna durata/Conferma)	filtro per restrizioni di accesso (richiesta autorizzata)
filtro per restrizioni di accesso + URL non filtrato	URL non filtrato (richiesta autorizzata)	filtro per restrizioni di accesso (richiesta autorizzata)

Creazione di un filtro per restrizioni di accesso

Argomenti correlati:

- *Gestione dei filtri*, pagina 48
- *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172
- Modifica di un filtro per restrizioni di accesso, pagina 174

Usare la pagina **Aggiungi filtro per restrizioni di accesso** (a cui si può accedere dalla pagina **Filtri** o **Modifica criteri**) per assegnare al nuovo filtro un nome univoco e una descrizione. Dopo aver creato il filtro, inserire un elenco di URL autorizzati, assegnare il filtro e un criterio e applicare il criterio ai client.

1. Inserire un **Nome filtro** univoco. Il nome deve contenere da 1 a 50 caratteri e non può includere i caratteri seguenti:

* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

I nomi assegnati ai filtri possono includere spazi, trattini e apostrofi.

2. Inserire una breve **Descrizione** del filtro. Questa descrizione deve apparire accanto al nome del filtro nella sezione Filtri per restrizione di accesso della pagina Filtri e deve specificare lo scopo del filtro al fine di aiutare gli amministratori a gestire i criteri nel corso del tempo.

Le restrizioni relative ai caratteri usati per il nome dei filtri sono anche applicabili alle descrizioni, con due eccezioni: le descrizioni possono includere punti (.) e virgole (,).

3. Per visualizzare e modificare il nuovo filtro, fare clic su **OK**. Per abbandonare le modifiche e ritornare alla pagina Filtri, fare clic su **Annulla**.

Quando si crea un nuovo filtro per restrizioni di accesso, questo viene aggiunto all'elenco **Gestione criteri > Filtri > Filtro per restrizioni di accesso**. Fare clic sul nome di un filtro per modificare il filtro.

Per terminare la personalizzazione del nuovo filtro, procedere a *Modifica di un filtro per restrizioni di accesso*.

Modifica di un filtro per restrizioni di accesso

Argomenti correlati:

- *Restrizione dell'accesso degli utenti a un elenco definito di siti Internet*, pagina 172
- Filtri per restrizioni di accesso e priorità di un filtro, pagina 172
- Creazione di un filtro per restrizioni di accesso, pagina 174
- *Modifica di un criterio*, pagina 79

Il filtro per restrizioni di accesso è costituito da un elenco di siti Web (URL o indirizzi IP) e da espressioni regolari usate per identificare siti specifici a cui gli utenti possono accedere. Quando il filtro viene applicato ai client, questi client non possono visitare un sito che non sia incluso nell'elenco.

Importante

Se un filtro per restrizioni di accesso è attivato, il software Websense verifica la presenza nel filtro di un sito richiesto. Non viene eseguita un'altra verifica.

Ciò significa che se un sito autorizzato dal filtro viene infettato da un codice dannoso, le richieste di accesso a quel sito da parte degli utenti vengono ancora autorizzate indipendentemente dalla categorizzazione del sito nel Master Database o dalla funzione di Scansione in tempo reale.

Usare la pagina **Gestione criteri > Filtri > Modifica filtro per restrizioni di accesso** per apportare le modifiche necessarie a un filtro per restrizioni di accesso esistente. È possibile modificare il nome e la descrizione del filtro, visualizzare un elenco di criteri associati al filtro e gestire la selezione dei siti da includere nel filtro.

Quando si modifica un filtro per restrizioni di accesso, le modifiche incidono su tutti i criteri che impongono l'applicazione del filtro.

- 1. Verificare il nome e la descrizione del filtro. Per modificare il nome del filtro, fare clic su **Rinomina** ed inserire quindi il nuovo nome. Il nome viene aggiornato in tutti i criteri che applicano il filtro per restrizioni di accesso selezionato.
- 2. Usare il campo **Criteri che usano questi filtri** per valutare il numero di criteri che applicano attualmente questo filtro. Se uno o più criteri applicano il filtro, fare clic su **Visualizza i criteri** per visualizzare il relativo elenco.
- 3. In Aggiungi o Elimina i siti, inserire gli URL e gli indirizzi IP che si vuole aggiungere al filtro per restrizioni di accesso. Inserire un URL o un indirizzo IP per riga.

Non è necessario includere il prefisso HTPP://.

Se un sito viene filtrato in base alla categoria assegnatagli nel Master Database, il software Websense associa l'URL all'indirizzo IP corrispondente. Questo non è applicabile ai filtri per restrizioni di accesso. Per autorizzare l'URL e l'indirizzo IP di un sito, aggiungerli entrambi al filtro.

- 4. Fare clic sul pulsante freccia verso destra (>) per portare gli URL e gli indirizzi IP nell'elenco dei siti autorizzati.
- 5. Oltre ad aggiungere singoli siti al filtro per restrizioni di accesso, è possibile aggiungere espressioni regolari che corrispondono a molteplici siti. Per creare un'espressione, fare clic su **Avanzate**.
 - Inserire un'espressione regolare per riga e fare clic sulla freccia rivolta verso destra per spostare l'espressione nell'elenco dei siti Autorizzati.
 - Per verificare che un'espressione regolare corrisponda ai siti rilevanti, fare clic su **Verifica**.

- Vedere Uso delle espressioni regolari, pagina 200 per informazioni dettagliate sull'uso di espressioni regolari applicate al filtro.
- 6. Verificare gli URL, gli indirizzi IP e le espressioni regolari dell'elenco Siti autorizzati.
 - Per modificare un sito o un'espressione regolare, selezionarli e fare clic su Modifica.
 - Per eliminare un sito o un'espressione regolare dall'elenco, selezionarli e fare clic su **Elimina**.
- 7. Dopo aver modificato il filtro, fare clic su **OK** per inserire le modifiche nella cache e ritornare alla pagina Filtri. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta di siti dalla pagina Modifica criterio

Argomenti correlati:

- Restrizione dell'accesso degli utenti a un elenco definito di siti Internet, pagina 172
- Filtri per restrizioni di accesso e priorità di un filtro, pagina 172
- Creazione di un filtro per restrizioni di accesso, pagina 174
- Modifica di un criterio, pagina 79

Utilizzare la pagina **Criteri > Modifica criterio > Aggiungi siti** per aggiungere dei siti a un filtro per restrizioni di accesso.

Inserire un URL o un indirizzo IP per riga. Se non si specifica un protocollo, il software Websense aggiunge automaticamente il prefisso **HTTP:**//.

Una volta terminate le modifiche, fare clic su **OK** per ritornare alla pagina Modifica criterio. Occorre inoltre fare clic su **OK** nella pagina Modifica criterio per inserire le modifiche apportate nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Le modifiche apportate a un filtro per restrizioni di accesso verranno duplicate in tutti i criteri di applicazione del filtro.

Copia di filtri e criteri nei ruoli

Argomenti correlati:

- Creazione di un filtro di categoria, pagina 49
- *Creazione di un filtro di protocollo*, pagina 52
- Creazione di un filtro per restrizioni di accesso, pagina 174
- *Creazione di un criterio*, pagina 78

I Super Administrator possono utilizzare la pagina **Filtri > Copia filtri nel ruolo** e **Criteri > Copia criteri nel ruolo** per copiare uno o più filtri o criteri in un ruolo di amministrazione con delega. Una volta che il filtro o il criterio sono stati copiati, gli amministratori con delega possono usare i filtri o i criteri per filtrare i client da loro gestiti.

- Nel ruolo di destinazione, il tag "(Copiato)" viene aggiunto alla fine del nome del filtro o del criterio. Viene aggiunto un numero se lo stesso filtro o criterio vengono copiati numerose volte.
- Gli amministratori con delega possono assegnare un nuovo nome o modificare i filtri o i criteri che sono stati copiati nei loro rispettivi ruoli.
- I filtri di categoria copiati in un ruolo di amministrazione con delega definiscono l'azione di filtraggio su Autorizza per le categorie personalizzate create nel ruolo. Gli amministratori con delega dovranno aggiornare i filtri di categoria copiati per definire l'azione da associare alle loro categorie personalizzate in base al ruolo.
- Le modifiche apportate da un amministratore con delega a un filtro o a un criterio copiati nel ruolo da un Super Administrator non agiscono sul filtro o sul criterio originale del Super Administrator o su qualsiasi altro ruolo che ha ricevuto una copia del filtro o del criterio.
- Le restrizioni di Blocco filtro non agiscono sul filtro o sul criterio originali del Super Administrator ma agiscono sulla copia del filtro o del criterio ricevuta dall'amministratore con delega.
- Poiché gli amministratori con delega sono soggetti alle restrizioni di Blocco filtro, i filtri di categoria e di protocollo Autorizza sempre non possono venire copiati in un ruolo di amministrazione con delega.

Per copiare un filtro o un criterio:

- 1. Nella pagina Copia filtri nel ruolo o Copia criteri nel ruolo, verificare che i criteri o i filtri corretti appaiano nell'elenco visualizzato nell'area superiore della pagina.
- 2. Utilizzare l'elenco a discesa **Selezionare un ruolo** per selezionare un ruolo di destinazione.
- 3. Fare clic su OK.

Una finestra di dialogo pop-up indica che i filtri o i criteri selezionati sono in corso di copia. La procedura di copia potrebbe richiedere del tempo.

Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Una volta completata la procedura di copia, i filtri o i criteri copiati saranno disponibili per gli amministratori con delega nel ruolo selezionato, la prossima volta che questi si collegano a Websense Manager. Se un amministratore con delega è collegato a un ruolo con un accesso regolato da criteri mentre i filtri o criteri vengono copiati, non vedrà i nuovi filtri o i nuovi criteri fino a quando non si scollega e si ricollega.

Definizione dei Componenti filtro

Utilizzare la pagina **Gestione criterio > Componenti filtro** per accedere agli strumenti usati per perfezionare e personalizzare il modo in cui il software Websense applica i criteri di accesso a Internet definiti per la propria organizzazione. I 4 pulsanti visualizzati nella schermata sono associati alle azioni seguenti:

Modifica categorie	• Ricategorizzazione di un URL (vedere <i>Ridefinizione di un filtro per specifici siti</i> , pagina 186). Ad esempio, se la categoria Acquisti in linea viene bloccata dai criteri di filtro a Internet, ma si vuole autorizzare l'accesso ai siti di specifici fornitori o partner, è possibile spostare questi siti in una categoria autorizzata, come ad esempio Business ed economia.
	• Definire o modificare le categorie personalizzate (vedere <i>Creazione di una categoria personalizzata</i> , pagina 182). Creare altre sottocategorie all'interno delle categorie principali definite da Websense o all'interno della categoria principale definita dall'utente ed assegnare quindi gli URL alle nuove categorie.
	• Assegnare parole chiave a una categoria (vedere <i>Filtro basato su parole chiave</i> , pagina 184). Per ricategorizzare e bloccare l'accesso ai siti il cui URL contiene una stringa specifica, definire innanzi tutto le parole chiave e quindi attivare il blocco in base alle parole chiave in un filtro di categoria.
	• Creare delle espressioni regolari (vedere <i>Uso delle espressioni regolari</i> , pagina 200), schemi o modelli che possano venire usati per creare corrispondenze con molteplici URL, ed assegnarli a una categoria.
Modifica protocolli	Definire o modificare le definizioni di protocolli personalizzati (vedere <i>Creazione di un protocollo</i> <i>personalizzato</i> , pagina 193 e <i>Modifica dei protocolli</i> <i>personalizzati</i> , pagina 190). Ad esempio, se i membri della propria organizzazione usano uno strumento di messaggistica personalizzato, è possibile creare una definizione di protocollo personalizzato al fine di consentire l'uso di quello strumento e di mantenere bloccati altri protocolli di Messaggistica immediata e Chat.

Tipi di file	Creare o modificare le definizione dei tipi di file, usate per bloccare determinati tipi di file che sono tuttavia autorizzati in altre categorie (vedere <i>Gestione del traffico in base al tipo</i> <i>di file</i> , pagina 197).
URL non filtrati	Definire determinati siti come siti autorizzati per tutti i client anche se appartenenti a una categoria bloccata (vedere <i>Definizione di URL non filtrati</i> , pagina 187). Tenere presente che l'aggiunta di un URL a questo elenco non acquisisce priorità rispetto al filtro di categoria Blocca sempre o ai filtri per restrizioni di accesso.

Gestione delle categorie

Argomenti correlati:

- Modifica delle categorie e dei loro attributi, pagina 179
- Creazione di una categoria personalizzata, pagina 182
- *Filtro basato su parole chiave*, pagina 184
- Ridefinizione di un filtro per specifici siti, pagina 186

Il software Websense dispone di vari metodi per l'applicazione di un filtro ai siti non inclusi nel Master Database e per la modifica del modo in cui i singoli siti del Master Database vengono filtrati.

- Creare categorie personalizzate per un filtraggio e una creazione di report più specifici.
- Usare URL ricategorizzati per definire categorie per siti non categorizzati o per modificare la categoria di siti inclusi nel Master Database.
- Definire delle **parole chiave** per ricategorizzare tutti i siti i cui URL contengono una determinata stringa.

Modifica delle categorie e dei loro attributi

Argomenti correlati:

- Creazione di una categoria personalizzata, pagina 182
- Revisione di tutti gli attributi personalizzati delle categorie, pagina 181
- Modifiche globali ai filtri di categoria, pagina 181
- Filtro basato su parole chiave, pagina 184
- Ridefinizione di un filtro per specifici siti, pagina 186

Utilizzare la pagina Gestione criteri >Componenti filtro >Modifica Modifica categorie per creare e modificare categorie personalizzate, URL ricategorizzati e parole chiave.

Le categorie esistenti, sia definite da Websense sia personalizzate, vengono elencate nell'area superiore del riquadro del contenuto. Per visualizzare le impostazioni personalizzate associate a una categoria o per creare nuove definizioni personalizzate, selezionare innanzi tutto una categoria dall'elenco.

Per visualizzare un elenco di tutti gli URL personalizzati, delle parole chiave e delle espressioni regolari associate a tutte le categorie, fare clic su **Visualizza tutte le parole chiave/URL personalizzati** nella barra degli strumenti nell'area superiore della pagina. Per ulteriori informazioni, vedere *Revisione di tutti gli attributi personalizzati delle categorie*, pagina 181.

 Per creare una nuova categoria, fare clic su Aggiungi e quindi andare alla sezione Creazione di una categoria personalizzata, pagina 182 per le istruzioni necessarie.

Per eliminare una categoria personalizzata esistente, selezionarla e fare quindi clic su **Elimina**. Non è consentito eliminare categorie definite da Websense.

- Per modificare il nome o la descrizione di una categoria personalizzata, selezionare la categoria e fare clic su **Rinomina** (vedere *Assegnazione di un nuovo nome a una categoria personalizzata*, pagina 182).
- Per modificare l'azione di filtro associata a una categoria in tutti i filtri di categoria, fare clic su **Sovrascrivi azione** (vedere *Modifiche globali ai filtri di categoria*, pagina 181).
- L'elenco URL ricategorizzati include i siti ricategorizzati (URL e indirizzi IP) che sono stati assegnati a questa categoria.
 - Per aggiungere un sito all'elenco, fare clic su Aggiungi URL. Per ulteriori istruzioni, vedere URL ricategorizzati, pagina 188.
 - Per modificare un sito ricategorizzato esistente, selezionare il relativo URL o indirizzo IP e fare quindi clic su **Modifica**.
- L'elenco delle **Parole chiave** mostra le parole chiave che sono state associate a questa categoria.
 - Per definire una parola chiave associata alla categoria selezionata, fare clic su Aggiungi parole chiave. Per ulteriori istruzioni, vedere *Filtro basato su* parole chiave, pagina 184.
 - Per modificare la definizione di una parola chiave esistente, selezionarla e fare quindi clic su **Modifica**.
- Oltre agli URL e alle parole chiave, è possibile definire le Espressioni regolari per una data categoria. Ciascuna espressione regolare rappresenta uno schema o un modello usati per associare molteplici siti alla categoria.

Per visualizzare o per creare espressioni regolari per la categoria, fare clic su **Avanzate**.

Per definire un'espressione regolare, fare clic su Aggiungi espressioni (vedere Uso delle espressioni regolari, pagina 200).
- Per modificare un'espressione regolare esistente, selezionarla e fare quindi clic su **Modifica**.
- Per eliminare un URL ricategorizzato, una parola chiave o un'espressione regolare, selezionare la voce da eliminare e fare quindi clic su Elimina.

Una volta completate le modifiche nella pagina Modifica categorie, fare clic su **OK** per inserire le modifiche nella cache e ritornare alla pagina Componenti filtro. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Revisione di tutti gli attributi personalizzati delle categorie

Usare la pagina **Gestione criteri > Modifica categorie > Visualizza tutte le parole chiave/URL personalizzati** per verificare le definizioni di URL personalizzati, parole chiave e espressioni regolari. È anche possibile eliminare le definizioni che non sono più necessarie.

La pagina contiene 3 tabelle simili, una per ogni attributo della categoria: URL personalizzati, parole chiave o espressioni regolari. In ciascuna tabella, l'attributo viene elencato accanto al nome della categoria alla quale è stato associato.

Per eliminare un attributo di categoria, selezionare la relativa casella di controllo e fare clic su **Elimina**.

Per ritornare alla pagina Modifica categorie, fare clic su **Chiudi**. Se si sono eliminate delle voci nella pagina Visualizza tutte le parole chiave/URL personalizzati, fare clic su **OK** nella pagina Modifica categorie per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Modifiche globali ai filtri di categoria

Usare la pagina **Componenti filtro > Modifica categorie > Sovrascrivi azione** per modificare l'azione associata a una categoria in tutti i filtri di categoria esistenti. Questo determina anche l'azione predefinita applicata alla categoria nei nuovi filtri.

Sebbene questa modifica assuma priorità rispetto all'azione applicata alla categoria in tutti i filtri esistenti, gli amministratori potranno in seguito modificare questi filtri per applicarvi un'azione diversa.

Prima di modificare le impostazioni di filtro applicate a una categoria, verificare innanzi tutto che il nome della categoria corretta sia visualizzato accanto a **Categoria selezionata**. Si può quindi:

1. scegliere una nuova **Azione** (Autorizza, Blocca, Conferma o Assegna durata). Per ulteriori informazioni, vedere *Azioni di filtraggio*, pagina 44.

Per predefinizione, l'opzione **Non modificare le impostazioni correnti** è selezionata per tutte le opzioni disponibili nella pagina.

- 2. Specificare se si vuole o non si vuole applicare **Blocca per parole chiave**. Per ulteriori informazioni, vedere *Filtro basato su parole chiave*, pagina 184.
- 3. Specificare se si vuole o non si vuole applicare **Blocca per tipi di file** e personalizzare quindi le impostazioni relative al blocco. Per ulteriori informazioni, vedere *Gestione del traffico in base al tipo di file*, pagina 197.

4. In **Filtri avanzati**, specificare se si vuole o meno usare Bandwidth Optimizer per gestire l'accesso ai siti HTTP e personalizzare le impostazioni del blocco. Per ulteriori informazioni, vedere *Uso di Bandwidth Optimizer per la gestione della larghezza di banda*, pagina 195.

Importante

- Le modifiche apportate qui agiscono su ogni filtro di categoria esistente, ad eccezione di **Blocca sempre** e **Autorizza sempre**.
- Fare clic su OK per ritornare alla pagina Modifica categorie (vedere *Modifica delle categorie e dei loro attributi*, pagina 179). Le modifiche non vengono inserite nella cache fino a quando non fa clic su OK nella pagina Modifica categorie.

Assegnazione di un nuovo nome a una categoria personalizzata

Usare la pagina **Componenti filtro > Modifica categorie > Rinomina categoria** per modificare il nome o la descrizione associati a una categoria personalizzata.

• Utilizzare il campo **Nome categoria** per modificare il nome della categoria. Il nuovo nome deve essere univoco e non può superare i 50 caratteri.

Il nome non può includere i seguenti caratteri:

* < > { } ~ ! \$ % & @ # . " | \setminus & + = ? / ; : ,

• Utilizzare il campo **Descrizione** per modificare la descrizione della categoria. La descrizione non può superare 255 caratteri.

Le restrizioni relative ai caratteri usati per il nome delle categorie è anche applicabile alle descrizioni, con due eccezioni: le descrizioni possono includere punti (.) e virgole (,).

Una volta terminate le modifiche, fare clic su **OK** per ritornare alla pagina Modifica categorie. Le modifiche non vengono inserite nella cache fino a quando non fa clic su **OK** nella pagina Modifica categorie.

Creazione di una categoria personalizzata

Argomenti correlati:

- Modifica delle categorie e dei loro attributi, pagina 179
- Filtro basato su parole chiave, pagina 184
- *Ridefinizione di un filtro per specifici siti*, pagina 186

Oltre ad usare le 90 e più categorie definite da Websense nel Master Database, è possibile definire le proprie **categorie personalizzate** per offrire filtri e creazione di report più specifici. Ad esempio, si possono creare categorie personalizzate del tipo:

- Viaggi d'affari, per l'accesso a siti di fornitori autorizzati che i dipendenti possono usare per acquistare biglietti d'aereo, noleggiare macchine e prenotare alberghi;
- Materiali di riferimento, per raggruppare siti di dizionari ed enciclopedie online ritenuti importanti ad esempio per gli studenti di una scuola;
- Sviluppo professionale, per raggruppare siti di training e altre risorse che i dipendenti sono incoraggiati ad usare per migliorare le proprie conoscenze.

Usare la pagina **Gestione criteri > Componenti filtro > Modifica categorie > Aggiungi categoria** per aggiungere categorie personalizzate a qualsiasi categoria principale. È possibile creare fino a 100 categorie personalizzate.

1. Inserire un nome univoco e descrittivo in **Nome categoria**. Il nome non può includere i seguenti caratteri:

* < > { } ~ ! \$ % & @ # . " | \setminus & + = ? / ; : ,

2. Inserire una Descrizione per la nuova categoria.

Le restrizioni relative ai caratteri da usare per il nome delle categorie è anche applicabile alle descrizioni, con due eccezioni: le descrizioni possono includere punti (.) e virgole (,).

- 3. Selezionare una categoria principale dall'elenco **Aggiungi a**. Per predefinizione, l'opzione **Tutte le categorie** è selezionata.
- 4. Inserire i siti (URL o indirizzi IP) che si vogliono aggiungere a questa categoria. Per ulteriori informazioni, vedere *URL ricategorizzati*, pagina 188.

È anche possibile modificare questo elenco dopo aver creato la categoria.

5. Inserire le parole chiave che si vogliono associare a questa categoria. Per ulteriori informazioni, vedere *Filtro basato su parole chiave*, pagina 184.

È anche possibile modificare questo elenco dopo aver creato la categoria.

6. Definire un'Azione di filtro predefinita da applicare a questa categoria in tutti i filtri di categoria esistenti. È anche possibile modificare in un secondo tempo questa azione nei singoli filtri.



Nota

I filtri di categoria copiati in un ruolo di amministrazione con delega definiscono l'azione di filtraggio su Autorizza per le categorie personalizzate create nel ruolo. Gli amministratori con delega dovranno aggiornare i filtri di categoria copiati per definire l'azione da associare alle loro categorie personalizzate in base al ruolo.

- 7. Attivare le azioni **Filtri avanzati** (blocco in base alle parole chiave, ai tipi di file o alla larghezza di banda) da applicare a questa categoria in tutti i filtri di categoria esistenti.
- 8. Una volta terminata la definizione della nuova categoria, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Modifica categorie. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

La nuova categoria viene aggiunta all'elenco Categorie e l'URL personalizzato e le informazioni relative alle parole chiave per la categoria vengono visualizzate.

Filtro basato su parole chiave

Argomenti correlati:

- URL ricategorizzati, pagina 188
- Configurazione delle impostazioni di filtraggio di Websense, pagina 57
- Creazione di un filtro di categoria, pagina 49
- *Modifica di un filtro di categoria*, pagina 50
- *Gestione delle categorie*, pagina 179

Le parole chiave sono associate a categorie e quindi vengono utilizzate per offrire protezione contro i siti che non sono stati esplicitamente aggiunti al Master Database o definiti come URL personalizzati. Per attivare il blocco in base a parole chiave eseguire le tre operazioni seguenti:

- 1. Attivare il blocco in base a parole chiave a livello globale (vedere *Configurazione delle impostazioni di filtraggio di Websense*, pagina 57).
- 2. Definire le parole chiave associate ad una categoria (vedere *Definizione di parole chiave*, pagina 185).
- 3. Attivare, nel filtro di categoria attivo, il blocco in base a parole chiave da applicare ad una categoria specifica (vedere *Modifica di un filtro di categoria*, pagina 50).

Una volta definite le parole chiave e dopo aver attivato per una specifica categoria il blocco in base a parole chiave, il software Websense blocca qualsiasi sito che contenga nel suo URL una o più delle parole chiave definite e registra il sito come sito appartenente alla categoria specificata. Il sito viene bloccato anche se altri URL inclusi nella categoria sono autorizzati.

Ad esempio, se la categoria Sport è autorizzata in un filtro di categoria attivo, ma si vuole bloccare l'accesso ai siti di pallacanestro, è possibile associare la parola "fip" a Sport e attivare il blocco in base a parole chiave. Ciò significa che, ad esempio, gli URL seguenti verranno bloccati e registrati come appartenenti alla categoria Sport.

- ◆ www.fip.it/
- fipcrl.it
- fiplazio.it
- allenatorifip.it

Fare attenzione quando si definiscono parole chiave di non creare un eccessivo numero di blocchi indesiderati.



Se si sta usando Websense Web Security, evitare l'associazione di parole chiave a qualsiasi sotto-categoria di Protezione estesa. Il blocco in base a parole chiave non viene applicato a queste categorie.

Se una richiesta viene bloccata in base a una parola chiave, questo viene segnalato nella pagina di blocco di Websense ricevuta dall'utente.

Definizione di parole chiave

Argomenti correlati:

- Modifica di un filtro di categoria, pagina 50
- *Gestione delle categorie*, pagina 179
- Filtro basato su parole chiave, pagina 184 ٠
- Uso delle espressioni regolari, pagina 200

La parola chiave è una stringa di caratteri (costituita ad esempio da una parola, una frase o un acronimo) che è possibile trovare in un URL. Assegnare delle parole chiave a una categoria e quindi attivare il blocco in base a parole chiave, nel relativo filtro di categoria.

Usare la pagina Gestione criteri > Componenti filtro > Modifica categorie > Aggiungi parole chiave per associare della parole chiave a determinate categorie. Se occorre modificare le definizione di una parola chiave, usare la pagina Modifica parole chiave.

Se si definiscono parole chiave, fare attenzione ad evitare blocchi indesiderati. Ad esempio, se si vuole usare la parola chiave "sesso" per bloccare l'accesso a siti con materiale per adulti si potrebbero indirettamente bloccare richieste di parole come ad esempio, "possessore" e siti come ad esempio assessoratoambiente.it, comune.milano.it/assessori.

Inserire una parola chiave per riga.

- Non includere spazi nelle parole chiave. Le stringhe per URL e CGI non possono includere spazi tra le parole.
- Inserire una barra obliqua (\) prima di eventuali caratteri speciali, ad esempio:

., # ? * +

Se non si inserisce la barra obligua, il software Websense ignora i caratteri speciali.

• Se si sta usando Websense Web Security, evitare l'associazione di parole chiave a qualsiasi sotto-categoria di Protezione estesa. Il blocco in base a parole chiave non viene applicato a queste categorie.

Una volta terminata l'aggiunta o la modifica di parole chiave, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Modifica categorie. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Per poter applicare il blocco in base alle parole chiave, occorre anche:

- 1. Attivare il blocco in base a parole chiave tramite la pagina **Impostazioni > Filtri** (vedere *Configurazione delle impostazioni di filtraggio di Websense*, pagina 57).
- 2. Attivare il blocco in base a parole chiave in uno o più filtri di categoria attivi (vedere *Modifica di un filtro di categoria*, pagina 50).

Ridefinizione di un filtro per specifici siti

Argomenti correlati:

- Creazione di una categoria personalizzata, pagina 182
- Filtro basato su parole chiave, pagina 184
- Definizione di URL non filtrati, pagina 187
- URL ricategorizzati, pagina 188

Con gli URL personalizzati, è possibile:

- Applicare un filtro più preciso a determinati siti non inclusi nel Websense Master Database. Per predefinizione, l'azione applicata alla categoria Miscellanea/Non classificato viene utilizzata per filtrare questi siti.
- Filtrare i siti in modo diverso rispetto alla categoria loro assegnata nel Master Database.

Il software Websense cerca l'esistenza di definizioni di URL personalizzati riguardo a un determinato sito prima di consultare il Master Database e quindi filtra il sito in base alla categoria assegnata all'URL personalizzato.

Sono disponibili 2 tipi di URL personalizzati: non filtrato e ricategorizzato.

- Gli URL non filtrati sono liberamente accessibili da parte di tutti gli utenti che non sono soggetti al filtro di categoria Blocca sempre o a un filtro per restrizioni di accesso (vedere *Definizione di URL non filtrati*, pagina 187).
- Gli URL ricategorizzati sono stati spostati dallo loro categoria nel Master Database ad un'altra categoria, definita da Websense o personalizzata (vedere URL ricategorizzati, pagina 188).

Per predefinizione, un URL ricategorizzato non è bloccato. Viene filtrato in base all'azione applicata alla sua nuova categoria da ogni filtro di categoria attivo.

Se un sito viene filtrato in base alla categoria che gli è stata assegnata nel Master Database, il software Websense associa l'URL all'indirizzo IP corrispondente. Questo non è applicabile agli URL personalizzati. Per modificare il modo in cui un sito viene filtrato, definire sia il suo URL che il suo indirizzo IP, come un URL personalizzato.

Se un sito è accessibile tramite molteplici URL, definire ciascun URL, che può essere usato per accedere al sito, come un URL personalizzato per assicurare che il sito venga autorizzato o bloccato in base alle definizioni.

Se un sito viene spostato in un nuovo dominio e si usa un ridirezionamento HTTP per inviare gli utenti al nuovo URL, il nuovo URL non viene automaticamente filtrato come il sito d'origine. Per accertarsi che il sito sia adeguatamente filtrato al nuovo indirizzo, creare un nuovo URL personalizzato.

Definizione di URL non filtrati

Argomenti correlati:

- *Gestione delle categorie*, pagina 179
- Ridefinizione di un filtro per specifici siti, pagina 186
- URL ricategorizzati, pagina 188

Usare la pagina **Gestione criteri > Componenti filtro > URL non filtrati** per definire un elenco di siti a cui qualsiasi utente può accedere a meno che il sito non sia soggetto al filtro di categoria Blocca sempre o a un filtro per restrizioni di accesso.

L'elenco dei **Siti autorizzati**, situato nell'area destra del riquadro del contenuto, elenca i siti non filtrati (URL e indirizzi IP) e le espressioni regolari che si sono definite (vedere *Uso delle espressioni regolari*, pagina 200). Ciascun sito è associato a una categoria.

- L'URL può essere associato alla categoria che gli è stata assegnata nel Master Database o può venire ricategorizzato.
- Se un utente richiede accesso a un URL non filtrato, la richiesta viene registrata come un URL personalizzato ed autorizzata nell'ambito della categoria alla quale è stato assegnato.

Per aggiungere un URL non filtrato:

1. In **Definisci URL non filtrati**, inserire un URL o un indirizzo IP per riga e fare quindi clic sulla freccia rivolta verso destra (>).

Il software Websense non crea una corrispondenza tra un URL personalizzato e il suo indirizzo IP. Per autorizzare sia l'URL che l'indirizzo IP di un sito, aggiungerli entrambi all'elenco URL non filtrati.

2. Per aggiungere un'espressione regolare che corrisponda a molteplici siti, fare clic su **Avanzate**. Inserire un'espressione regolare per riga e fare quindi clic sulla freccia rivolta verso destra per spostare l'espressione nell'elenco degli URL non filtrati. Per verificare che uno schema corrisponda ai siti previsti, fare clic su **Verifica**.

Per ulteriori informazioni, vedere Uso delle espressioni regolari, pagina 200.

3. Una volta terminato, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Modifica categorie. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Per eliminare un sito dall'elenco degli URL non filtrati, selezionare il relativo URL, indirizzo IP o espressione regolare e fare quindi clic su **Elimina**.

URL ricategorizzati

Argomenti correlati:

- *Gestione delle categorie*, pagina 179
- Ridefinizione di un filtro per specifici siti, pagina 186
- Definizione di URL non filtrati, pagina 187

Usare la pagina Gestione criteri > Componenti filtro > Modifica categorie > Ricategorizza URL per aggiungere dei siti a qualsiasi categoria. Modificare, come necessario, i siti ricategorizzati esistenti nella pagina Modifica URL ricategorizzati

Ricategorizzare gli URL per modificare il modo in cui i siti vengono filtrati e registrati. Se si aggiungono siti ricategorizzati:

- Inserire ciascun URL o indirizzo IP in una riga separata.
- Includere il protocollo per ogni sito non-HTTP. Se non si include il protocollo, il software Websense filtra il sito come un sito HTTP.

Per i siti HTTPS, includere anche il numero di porta (https://63.212.171.196:443/, https://www.bancainlinea.com:443/).

 Il software Websense riconosce gli URL personalizzati esattamente come stati inseriti. Se la categoria Motori di ricerca e Portali è bloccata, ma si ricategorizza ad esempio it.yahoo.com in una categoria con accesso autorizzato, il sito viene autorizzato soltanto se l'utente digita l'intero indirizzo. Se un utente digita it.images.search.yahoo.com oppure soltanto it.yahoo.com, il sito rimane bloccato. Se tuttavia si ricategorizza it.yahoo.com, tutti i siti che includono yahoo.it nel loro indirizzo vengono autorizzati.

Una volta terminata l'aggiunta o la modifica dei siti ricategorizzati, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Modifica categorie. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Dopo aver salvato gli URL ricategorizzati, usare lo strumento **Categoria URL** disponibile nel riquadro dei collegamenti di destra per verificare che il sito venga assegnato alla categoria corrente. Vedere *Uso della Casella degli strumenti per verificare il comportamento dei filtri*, pagina 201.

Gestione dei protocolli

Il Websense Master Database include la definizione di protocolli usati per filtrare i protocolli Internet diversi da HTTP, HTTPS e FTP. Queste definizioni includono applicazioni Internet e metodi di trasferimento di dati, come ad esempio quelli usati per la messaggistica immediata, streaming media, scambio di file, trasferimento di file, e-mail e altre operazioni di rete e di database.

Queste definizioni per protocolli possono venire anche usate per filtrare i protocolli o le applicazioni che aggirano un firewall passando attraverso le porte utilizzate normalmente dal traffico HTTP. I dati di messaggistica immediata, ad esempio, possono entrare in una rete il cui firewall blocca tale messaggistica immediata, passando attraverso le porte HTTP. Il software Websense identifica con precisione questi protocolli e li filtra in base ai criteri configurati.



Nota

Occorre aver installato Network Agent per attivare i filtri di protocollo.

Oltre ad usare definizioni di protocolli definiti da Websense, è possibile definire protocolli personalizzati per i filtri. Le definizioni relative a protocolli personalizzati possono essere basate su indirizzi IP o numeri di porta e possono venire modificate.

Per bloccare il traffico in base a una porta specifica, associare il numero della porta a un protocollo personalizzato ed assegnare quindi a quel protocollo un'azione predefinita di Blocco.

Per gestire le definizioni di protocolli personalizzati, andare a Gestione criteri > Componenti filtro e fare quindi clic su Protocolli. Per ulteriori informazioni, vedere Modifica dei protocolli personalizzati, pagina 190 a Creazione di un protocollo personalizzato, pagina 193.

Filtri di protocollo

Argomenti correlati:

- Gestione dei protocolli, pagina 189
- Modifica dei protocolli personalizzati, pagina 190
- Creazione di un protocollo personalizzato, pagina 193
- Aggiunta o modifica degli identificatori dei protocolli, pagina 191
- Aggiunta a un protocollo definito da Websense, pagina 195

Se si è installato Network Agent, il software può bloccare un contenuto Internet trasmesso tramite particolari porte o che usa specifici indirizzi IP o che include determinate firme, indipendentemente dalla natura dei dati. Per predefinizione, il blocco di una porta intercetta tutto il contenuto Internet in entrata nella rete attraverso quella porta, indipendentemente dal suo punto d'origine.



Nota

Il traffico di rete interno, inviato attraverso una particolare porta, potrebbe a volte non venire bloccato anche se il protocollo che usa quella porta è bloccato. Il protocollo potrebbe inviare dati attraverso un server interno molto più rapidamente di quanto Network Agent non sia in grado di catturarli e di elaborarli. Questo non si verifica con i dati originati all'esterno della rete.

Se si inoltra una richiesta di protocollo, il software Websense adotta la procedura seguente per determinare se bloccare o autorizzare la richiesta:

- 1. Determina il nome del protocollo (o l'applicazione Internet).
- 2. Identifica il protocollo in base all'indirizzo di destinazione della richiesta.
- 3. Cerca i relativi numeri di porta o indirizzi IP nelle definizioni dei protocolli personalizzati.
- 4. Cerca i relativi numeri di porta o indirizzi IP o firme nelle definizioni dei protocolli definiti da Websense.

Se il software Websense non è in grado di raccogliere queste informazioni, il contenuto associato al protocollo viene autorizzato.

Modifica dei protocolli personalizzati

Argomenti correlati:

- Gestione dei protocolli, pagina 189
- Creazione di un protocollo personalizzato, pagina 193
- Creazione di un filtro di protocollo
- Modifica di un filtro di protocollo
- *Gestione delle categorie*

Utilizzare la pagina **Gestione criteri > Componenti filtro > Modifica protocolli** per creare e modificare le definizioni dei protocolli personalizzati e per rivalutare le definizioni dei protocolli definiti da Websense. I protocolli definiti da Websense non possono venire modificati.

L'elenco Protocolli include tutti i protocolli personalizzati e quelli definiti da Websense. Fare clic su un protocollo o su un gruppo di protocolli per ottenere informazioni sulla voce selezionata nell'area di destra del riquadro del contenuto.

Per aggiungere un nuovo gruppo personalizzato, fare clic su **Aggiungi protocollo** e procedere quindi alla sezione *Creazione di un protocollo personalizzato*, pagina 193.

Per modificare la definizione di un protocollo:

- 1. Selezionare un protocollo dall'elenco Protocolli. La definizione del protocollo appare a destra dell'elenco.
- 2. Fare clic su **Sovrascrivi azione** per modificare l'azione del filtro applicata a questo protocollo in tutti i filtri di protocollo (vedere *Modifiche globali ai filtri di protocollo*, pagina 192).
- 3. Fare clic su **Aggiungi identificatore** per definire altri identificatori per questo protocollo (vedere *Aggiunta o modifica degli identificatori dei protocolli*, pagina 191).
- 4. Selezionare un identificatore dall'elenco e fare quindi clic su **Modifica** per apportare modifiche alla **Porta**, all'**Intervallo indirizzi IP** o al **Metodo di trasporto** definito dall'identificatore.
- 5. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Per eliminare la definizione di un protocollo, selezionare la relativa voce dall'elenco Protocolli e fare quindi clic su **Elimina**.

Aggiunta o modifica degli identificatori dei protocolli

Usare la pagina **Componenti filtro > Modifica protocolli > Aggiungi identificatore protocollo** per definire altri identificatori per un protocollo personalizzato esistente. Usare la pagina **Modifica identificatore protocollo** per apportare le modifiche necessarie ad un identificatore definito in precedenza.

Prima di creare o modificare un identificatore, verificare che il nome corretto del protocollo appaia accanto a **Protocollo selezionato**.

Quando si gestiscono identificatori di protocollo, ricordare che almeno uno dei criteri applicati (porta, indirizzo IP o tipo di trasporto) deve essere esclusivo di quel protocollo.

- 1. Specificare le **Porte** da includere nell'identificatore.
 - Se si seleziona **Tutte le porte**, questo criterio si sovrappone alle altre porte o indirizzi IP inclusi nelle definizioni di altri protocolli.
 - Gli intervalli dei numeri di porta non vengono considerati esclusivi se si sovrappongono ad altri. Ad esempio, l'intervallo dei numeri di porta 8—6000 si sovrapporrà all'intervallo 4000-9000.
 - Adottare cautela quando si definisce un protocollo con porta 80 o 8080.
 Network Agent rileva le richieste Internet che passano attraverso queste porte.
 Poiché i protocolli personalizzati hanno priorità rispetto ai protocolli definiti da Websense, se si definisce un protocollo personalizzato che usa la porta 80, tutti gli altri protocolli che usano la porta 80 verranno filtrati e registrati come il protocollo personalizzato.
- 2. Specificare gli Indirizzi IP da includere in questo identificatore.

- Se si seleziona **Tutti gli indirizzi IP esterni**, questo criterio si sovrapporrà agli altri indirizzi IP inclusi nelle definizioni di altri protocolli.
- Gli intervalli degli indirizzi IP non vengono considerati esclusivi se si sovrappongono ad altri.
- 3. Specificare il metodo di **Trasporto protocollo** da includere in questo identificatore.
- 4. Fare clic su **OK** per inserire nella cache le modifiche apportate e per ritornare alla pagina Modifica protocolli. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Assegnazione di un nuovo nome a un protocollo personalizzato

Usare la pagina **Componenti filtro > Modifica protocolli > Rinomina protocollo** per modificare il nome assegnato a un protocollo personalizzato oppure spostarlo in un gruppo di protocolli diversi.

• Usare il campo **Nome** per modificare il nome del protocollo. Il nuovo nome non può superare 50 caratteri.

Il nome non può includere i seguenti caratteri:

- * < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,
- Per spostare il protocollo in un gruppo di protocolli diverso, selezionare il nuovo gruppo nel campo **Nel gruppo**.

Una volta terminate le modifiche, fare clic su **OK** per ritornare alla pagina Modifica protocolli. Occorre inoltre fare clic su **OK** nella pagina Modifica protocolli per inserire le modifiche apportate nella cache.

Modifiche globali ai filtri di protocollo

Usare la pagina **Componenti filtro > Modifica categorie > Sovrascrivi azione** per modificare il modo in cui un protocollo viene filtrato in tutti i filtri di protocollo esistenti. Questo determina anche l'azione predefinita applicata al protocollo nei nuovi filtri.

Sebbene questa modifica assuma priorità rispetto all'azione associata a tutti i filtri di protocolli esistenti, gli amministratori potranno in seguito modificare questi filtri per associarvi un'azione diversa.

- 1. Verificare che il nome corretto del protocollo venga visualizzato accanto a **Protocollo selezionato**.
- Scegliere una nuova Azione (Autorizza o Blocca) da applicare a questo protocollo Per predefinizione, l'opzione Nessuna modifica è selezionata. Per ulteriori informazioni, vedere Azioni di filtraggio, pagina 44.
- 3. Specificare nuove opzioni di **Registrazione**. Il traffico basato sui protocolli deve venire registrato affinché possa venire incluso nei report e possa attivare le avvertenze relative all'uso dei protocolli.

4. Specificare se si vuole utilizzare o meno il **Bandwidth Optimizer** per la gestione dell'accesso a questo protocollo. Per ulteriori informazioni, vedere *Uso di Bandwidth Optimizer per la gestione della larghezza di banda*, pagina 195.



 Una volta terminate le modifiche, fare clic su OK per ritornare alla pagina Modifica protocolli (vedere *Modifica dei protocolli personalizzati*, pagina 190). Occorre inoltre fare clic su OK nella pagina Modifica protocolli per inserire le modifiche apportate nella cache.

Creazione di un protocollo personalizzato

Argomenti correlati:

- Gestione dei protocolli, pagina 189
- *Filtri di protocollo*, pagina 189
- Modifica dei protocolli personalizzati, pagina 190
- Aggiunta a un protocollo definito da Websense, pagina 195

Usare la pagina **Componenti filtro > Protocolli > Aggiungi protocollo** per definire un nuovo protocollo personalizzato.

1. Inserire un Nome per il protocollo.

Il nome non può includere i seguenti caratteri:

* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

È possibile assegnare a un protocollo personalizzato lo stesso nome assegnato a un protocollo definito da Websense per estendere il numero di indirizzi IP o di porte associati al protocollo originale. Per ulteriori informazioni, vedere *Aggiunta a un protocollo definito da Websense*, pagina 195.

- 2. Espandere l'elenco a discesa **Aggiungi protocollo a questo gruppo** e selezionare quindi un gruppo di protocolli. Il nuovo protocollo viene visualizzato in tutti gli elenchi e filtri di protocollo di questo gruppo.
- 3. Definire un **Identificatore protocollo** (set di **porte**, **indirizzi IP** e **metodi di trasporto**) per questo gruppo. È possibile aggiungere altri identificatori in seguito, dalla pagina Modifica protocolli.

Adottare le linee guida seguenti per creare gli identificatori dei protocolli:

 Almeno un criterio (porta, indirizzo IP o tipo di trasporto) deve essere esclusivo della definizione di ogni protocollo.

- Se si seleziona **Tutte le porte** o **Tutti gli indirizzi IP esterni**, questo criterio si sovrapporrà alle altre porte e agli altri indirizzi IP inclusi nelle definizioni di altri protocolli.
- Gli intervalli dei numeri di porta o degli indirizzi IP non vengono considerati esclusivi se si sovrappongono ad altri. Ad esempio, l'intervallo dei numeri di porta 8—6000 si sovrapporrà all'intervallo 4000-9000.

Nota

Adottare cautela quando si definisce un protocollo con porta 80 o 8080. Network Agent rileva le richieste Internet che passano attraverso queste porte.

Poiché i protocolli personalizzati hanno priorità rispetto ai protocolli definiti da Websense, se si definisce un protocollo personalizzato che usa la porta 80, tutti gli altri protocolli che usano la porta 80 verranno filtrati e registrati come il protocollo personalizzato.

Le tabelle che seguono offrono esempi di definizioni di protocollo valide e non valide:

Porta	Indirizzo IP	Metodo di trasporto	Combinazione accettata?	
70	QUALSIASI	ТСР	Sì – il numero di porta	
90	QUALSIASI	ТСР	identificatore di protocollo.	

Porta	Indirizzo IP	Metodo di trasporto	Combinazione accettata?
70	QUALSIASI	ТСР	No – Gli indirizzi IP non
70	10.2.1.201	ТСР	è incluso nel set "QUALSIASI".

Porta	Indirizzo IP	Metodo di trasporto	Combinazione accettata?
70	10.2.3.212	ТСР	Sì – Gli indirizzi IP sono
70	10.2.1.201	ТСР	esclusivi.

- 4. In Azioni di filtro predefinite, specificare l'azione predefinita (Autorizza o Blocca) che deve venire applicata a questo protocollo in tutti i filtri di protocollo attivi:
 - Indicare se il traffico che usa questo protocollo debba essere Registrato. Il traffico basato sui protocolli deve venire registrato affinché possa venire incluso nei report e possa attivare le avvertenze relative all'uso dei protocolli.

- Indicare se l'accesso a questo protocollo deve essere determinato dal Bandwidth Optimizer (vedere Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195).
- 5. Una volta terminate le modifiche, fare clic su **OK** per ritornare alla pagina Modifica protocolli. La definizione del nuovo protocollo viene visualizzata nell'elenco Protocolli.
- 6. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta a un protocollo definito da Websense

Non è consentito aggiungere un numero di porta o un indirizzo IP direttamente a un protocollo definito da Websense. È possibile tuttavia creare un protocollo personalizzato con lo stesso nome del protocollo definito da Websense e quindi aggiungere porte o indirizzi IP alla sua definizione.

Se un protocollo personalizzato e un protocollo definito da Websense hanno lo stesso nome, il software Websense cerca il traffico relativo ai protocolli nelle porte e negli indirizzi IP specificati in entrambe le definizioni.

Nei report, i nomi dei protocolli personalizzati hanno un prefisso "U_". Ad esempio, se si crea un protocollo personalizzato per SQL_NET e si specificano altri numeri di porta, il report visualizza U_SQL_NET se il protocollo usa i numeri di porta nel protocollo personalizzato.

Uso di Bandwidth Optimizer per la gestione della larghezza di banda

Argomenti correlati:

- *Gestione delle categorie*, pagina 179
- *Gestione dei protocolli*, pagina 189
- Configurazione delle restrizioni predefinite di Bandwidth Optimizer, pagina 196

Se si crea un filtro di categoria o di protocollo, si può scegliere di limitare l'accesso a una categoria o a un protocollo in base all'uso della larghezza di banda.

- Bloccare l'accesso a categorie o a protocolli in base all'uso totale della larghezza di banda di rete.
- Bloccare l'accesso a categorie in base all'uso totale della larghezza di banda da parte del traffico HTPP.
- Bloccare l'accesso a un protocollo specifico in base all'uso totale della larghezza di banda da parte di quel protocollo.

Ad esempio:

- Bloccare il protocollo della Messaggistica immediata di AOL se l'uso della larghezza di banda di rete supera il 50% della larghezza di banda disponibili o se l'uso della larghezza di banda per AIM supera il 10% della larghezza di banda di rete totale.
- Bloccare la categoria Sport se l'uso totale della larghezza di banda di rete raggiunge il 75% o se l'uso della larghezza di banda da parte di tutto il traffico HTTP raggiunge il 60% della larghezza di banda di rete disponibile.

L'uso della larghezza della banda di rete del protocollo include il traffico attraverso tutte le porte, gli indirizzi IP o le firme definiti per il protocollo. Ciò significa che se un protocollo o un'applicazione Internet utilizza molteplici porte per il trasferimento dei dati, il traffico attraverso tutte le porte incluse nella definizione del protocollo viene calcolato in rapporto all'uso totale della larghezza di banda per quel protocollo. Tuttavia, se un'applicazione Internet usa una porta non inclusa nella definizione del protocollo, il traffico attraverso quella porta non viene incluso nei calcoli dell'uso della larghezza di banda.

Il software Websense registra la larghezza di banda usata dai protocolli filtrati basati su TCP e UDP.

Websense, Inc. aggiorna le definizioni dei protocolli Websense regolarmente per garantire l'accuratezza delle misurazioni relative all'uso della larghezza di banda.

Network Agent invia i dati relativi alla larghezza di banda di rete a Filtering Service in base a un intervallo predefinito. Ciò garantisce che il software Websense monitori con precisione l'uso della larghezza di banda e che riceva le misurazioni più vicine alla media.

Se le opzioni di filtro basate sull'uso della larghezza di banda sono attive, il software Websense inizia l'applicazione dei filtri 10 minuti dopo la configurazione iniziale e 10 minuti dopo ogni riavvio di Websense Policy Server. Questo ritardo garantisce una misurazione precisa dei dati relativi alla larghezza di banda e all'uso di questi dati nell'applicazione dei filtri.

Se una richiesta viene bloccata in base a restrizioni relative alla larghezza di banda, la pagina di blocco di Websense visualizza questa informazione nel campo **Motivo**. Per ulteriori informazioni, vedere *Pagine di blocco*, pagina 87.

Configurazione delle restrizioni predefinite di Bandwidth Optimizer

Argomenti correlati:

- *Modifica di un filtro di categoria*, pagina 50
- Modifica di un filtro di protocollo, pagina 53
- Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195

Prima di specificare le impostazioni relative alla larghezza di banda nei criteri, verificare le soglie che azionano le impostazioni del filtro basate sulla larghezza di banda. I valori definiti da Websense sono:

- Larghezza di banda predefinita per la rete: 50%
- Larghezza di banda predefinita per i protocolli: 20%

I valori di larghezza di banda predefiniti vengono archiviati nel Policy Server e applicati da tutte le relative istanze di Network Agent rilevanti. Se si dispone di molteplici Policy Server, le modifiche apportate ai valori predefiniti per la larghezza di banda in un determinato Policy Server non incidono su altri eventuali Policy Server.

Per modificare i valori predefiniti per la larghezza di banda:

- 1. In Websense Manager, andare a **Impostazioni > Filtri**.
- 2. Inserire le soglie relative all'uso della larghezza di banda che azioneranno i filtri basati sulla larghezza di banda, se questi filtri sono stati attivati.
 - Se una categoria o un protocollo sono bloccati in base al traffico relativo all'intera rete, Larghezza di banda predefinita per la rete definisce la soglia dei filtri predefiniti.
 - Se una categoria o un protocollo sono bloccati in base al traffico relativo al protocollo, l'opzione Larghezza di banda predefinita per la rete definisce la soglia applicabile ai filtri predefiniti.

È possibile ignorare i valori di soglia predefiniti per ciascuna categoria o protocollo in qualsiasi filtro di categoria o di protocollo.

3. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Le modifiche apportate alle predefinizioni possono potenzialmente incidere su qualsiasi filtro di categoria o di protocollo che applica le restrizioni di.

- Per gestire l'uso della larghezza di banda in relazione a un particolare protocollo, modificare il filtro o i filtri di protocollo attivi.
- Per gestire l'uso della larghezza di banda in relazione a una particolare categoria di URL, modificare il relativo filtro o filtri di categoria.

Se si applica un filtro a categorie in base all'uso di una larghezza di banda tramite HTTP, il software Websense misura l'uso totale della larghezza di banda tramite HTTP attraverso tutte le porte specificate come porte HTTP per il software Websense.

Gestione del traffico in base al tipo di file

Se si crea un filtro di categoria, è possibile definire il filtro in base all'estensione di file, limitando l'accesso a tipi di file particolari da siti appartenenti a determinate categorie. Ad esempio, si può autorizzare la categoria Sport ma bloccare i file video dei siti inclusi nella categoria Sport.

Il software Websense dispone di numerosi tipi di file predefiniti o di gruppi di estensioni di file da usare per il medesimo scopo. Le definizioni di questi tipi di file vengono mantenute nel Master Database e possono venire modificate come parte della procedura di aggiornamento del Master Database.

È possibile implementare dei filtri usando i tipi di file predefiniti, modificare le definizioni dei tipi di file esistenti o creare dei nuovi tipi di file. Tenere presente tuttavia, che non è possibile eliminare tipi di file definiti da Websense o eliminare le estensioni di file ad essi associati.

Se un utente richiede l'accesso a un sito, il software Websense determina innanzi tutto la categoria del sito e quindi verifica le estensioni di file da filtrare.

Nota

Per implementare un filtraggio completo per i file Internet video e audio, combinare i filtri basati sui protocolli con i filtri basati sui tipi di file. In questo caso, il filtro di protocollo gestisce lo streaming media, mentre il filtro basato sul tipo di file gestisce i file che possono venire scaricati e quindi riprodotti.

Se un utente cerca di accedere a un file la cui estensione è bloccata, il campo **Motivo** nella pagina di blocco di Websense indica che quel tipo di file è stato bloccato. Per ulteriori informazioni, vedere *Pagine di blocco*, pagina 87.

Nota

La pagina di blocco standard non viene visualizzata se un'immagine GIF o JPEG bloccata include una parte della pagina autorizzata. L'area dell'immagine appare invece vuota. Ciò evita la possibilità di visualizzare una piccola parte di una pagina di blocco in molteplici punti di una pagina altrimenti autorizzata.

Le definizioni relative al tipo di file potrebbero contenere tante estensioni di file quante possono essere utili ai fini del filtraggio. I tipi di file definiti da Websense, ad esempio, includono le seguenti estensioni di file:

Audio	File compressi		Eseguibili	Vic	leo
.aif	.ace	.mim	.bat	.asf	.mpg
.aifc	.arc	.rar	.exe	.asx	.mpv2
.aiff	.arj	.tar		.avi	.qt
.m3u	.b64	.taz		.ivf	.ra
.mid	.bhx	.tgz		.m1v	.ram
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp
.ogg	.gzip	.uue		.mp2v	.wmv

Audio	File cor	npressi	Eseguibili	Vic	leo
.rmi	.hqx	.xxe		.mpa	.wmx
.snd	.iso	.Z		.mpe	.WXV
.wav	.jar	.zip			
.wax	.lzh				
.wma					

Le estensioni di file associate a un tipo di file definito da Websense possono venire aggiunte a un tipo di file personalizzato. L'estensione del file viene quindi filtrata e registrata in base alle impostazioni associate al tipo di file personalizzato.

Per visualizzare le definizioni dei tipi di file, modificare i tipi di file o creare tipi di file personalizzati, andare a **Gestione criteri > Componenti filtro** e fare quindi clic su **Tipi di file**. Per ulteriori informazioni, vedere *Gestione dei tipi di file*, pagina 199.

Gestione dei tipi di file

Argomenti correlati:

- Gestione del traffico in base al tipo di file, pagina 197
- Modifica di un filtro di categoria, pagina 50
- *Filtraggio di un sito*, pagina 83

Usare la pagina **Gestione criteri > Componenti filtro > Modifica tipi di file** per creare e gestire fino a 32 **tipi di file**. I tipi di file sono gruppi di estensioni di file che possono venire esplicitamente bloccati nei filtri di categoria (vedere *Gestione del traffico in base al tipo di file*, pagina 197).

- Fare clic su un tipo di file per visualizzare le estensioni di file associate a quel tipo.
- Per aggiungere estensioni al tipo di file selezionato, fare clic su Aggiungi estensioni e quindi andare alla sezione Aggiunta di estensioni di file a un tipo di file, pagina 200 per ulteriori istruzioni.
- Per creare un nuovo tipo di file, fare clic su **Aggiungi tipo file**, e quindi andare alla sezione *Aggiunta di tipi di file predefiniti*, pagina 200 per ulteriori istruzioni.
- Per eliminare un tipo di file o un'estensione personalizzati, selezionare una voce e fare quindi clic su **Elimina**.

Non è possibile eliminare tipi di file definiti da Websense o eliminare le estensioni di file ad essi associati.

È possibile tuttavia aggiungere a un tipo di file personalizzato, delle estensioni di file associate a un tipo di file definito da Websense. L'estensione del file viene quindi filtrata e registrata in base alle impostazioni associate al tipo di file

personalizzato. Non è possibile aggiungere la stessa estensione a molteplici tipi di file personalizzati.

Una volta terminate le modifiche delle definizioni dei tipi di file, fare clic su **OK**. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta di tipi di file predefiniti

Usare la pagina **Componenti filtro > Modifica tipi di file > Aggiungi tipi di file** per definire i tipi di file personalizzati.

1. Inserire un Nome tipo di file univoco.

È possibile tuttavia creare un tipo di file personalizzato con lo stesso nome del tipo di file definito da Websense se si vogliono aggiungere estensioni di file al tipo di file esistente.

- 2. Inserire le estensioni di file, una riga per volta, nell'elenco **Estensioni di file** definite dall'utente. Non occorre includere il punto (".") prima di ogni estensione.
- 3. Fare clic su **OK** per ritornare alla schermata Modifica tipi di file. Il nuovo tipo di file viene visualizzato nell'elenco Tipi di file.
- 4. Una volta terminate le modifiche delle definizioni dei tipi di file, fare clic su **OK** nella pagina Modifica tipi di file. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta di estensioni di file a un tipo di file

Usare la pagina **Componenti filtro > Modifica tipi di file >Aggiungi tipi di file** per aggiungere estensioni di file al tipo di file selezionato.

- 1. Verificare che il nome del tipo di file previsto venga visualizzato accanto a **Tipo di file selezionato**.
- 2. Inserire le estensioni di file, una riga per volta, nell'elenco **Estensioni di file**. Non occorre includere il punto (".") prima di ogni estensione.
- 3. Fare clic su **OK** per ritornare alla schermata Modifica tipi di file. Le nuove estensioni di file vengono visualizzate nell'elenco Estensioni di file personalizzate.
- 4. Una volta terminate le modifiche delle definizioni dei tipi di file, fare clic su **OK** nella pagina Modifica tipi di file. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Uso delle espressioni regolari

L'espressione regolare è uno schema o un modello usato per creare una corrispondenza tra molteplici stringhe o gruppi di caratteri. È possibile usare espressioni regolari nei filtri per restrizioni di accesso o definire URL o parole chiave

personalizzate. Il filtro Websense cerca di creare quindi una corrispondenza con un modello generico, anziché con un URL o una parola chiave specifica.

Osservare, ad esempio, questa semplice espressione regolare:

dominio.(it|org|net)

Lo schema di questa espressione regolare corrisponde ai seguenti URL:

- dominio.it
- dominio.org
- dominio.net

Usare le espressioni regolari con cautela. Esse costituiscono infatti uno strumento di filtraggio potente, ma possono facilmente comportare il blocco o l'autorizzazione di siti indesiderati. Inoltre, le espressioni regolari non costruite correttamente potrebbero dare come risultato un filtraggio complessivo eccessivo.

Importante

L'uso di espressioni regolari come criteri di filtraggio, possono incrementare l'uso della CPU. I risultati di alcuni test condotti hanno dimostrato che con 100 espressioni regolari, l'uso medio della CPU nel computer in cui è installato Filtering Service, è stato incrementato del 20%.

Il software Websense supporta la maggior parte della sintassi delle espressioni regolari Perl, con alcune eccezioni. Alcune sintassi non supportate non sono utili per creare una corrispondenza di stringhe che possono far parte di un URL.

Le sintassi di espressioni regolari non supportate includono:

(?<=pattern)string	(? pattern)string</th
\N{name}	(?imsx-imsx)
(?(condition)pat1) (?(condition)pat1 pat2)	\pP \PP
(?{code})	??{code})

Per ulteriori informazioni sulle espressioni regolari, vedere:

```
it.wikipedia.org/wiki/Espressioni_regolari
www.regular-expressions.info/
```

Uso della Casella degli strumenti per verificare il comportamento dei filtri

Il riquadro dei collegamenti di destra di Websense Manager include una **Casella degli strumenti** che consente di eseguire delle verifiche rapide delle impostazioni definite per i filtri.

Fare clic sul nome di un filtro per accedere allo strumento. Fare clic ancora sul nome per visualizzare l'elenco degli strumenti. Per ulteriori informazioni sull'uso di uno strumento, vedere .

- *Categoria degli URL*, pagina 202
- *Verifica criterio*, pagina 202
- Verifica filtri, pagina 203
- Accesso URL, pagina 203
- Verifica utente, pagina 203

È anche possibile fare clic su **Portale di supporto** per accedere al sito di assistenza tecnica, Websense Technical Support Web, usando una nuova scheda o finestra del browser. Dal portale di assistenza tecnica si può inoltre accedere alla Knowledge Base, a esercitazioni, suggerimenti, articoli e documentazione.

Categoria degli URL

Per determinare come un sito è categorizzato:

- 1. Fare clic su Categoria URL nella Casella degli strumenti.
- 2. Inserire un URL o un indirizzo IP.
- 3. Fare clic su Vai.

La categoria corrente del sito viene visualizzata in una finestra pop-up. Se la propria organizzazione ha ricategorizzato l'URL, viene visualizzata la nuova categoria.

La categorizzazione del sito può dipendere dalla versione del Master Database (inclusi gli aggiornamenti in tempo reale) che si stanno usando.

Verifica criterio

Usare questo strumento per determinare i criteri da applicare a un client specifico. I risultati sono specifici del giorno e dell'ora correnti.

- 1. Fare clic su Verifica criterio nella Casella degli strumenti.
- 2. Per identificare la directory o il client, inserire:
 - Un nome utente qualificato

Per navigare o condurre una ricerca nella directory al fine di identificare l'utente, fare clic su **Trova utente** (vedere *Identificazione di un utente per verificare criteri o filtri*, pagina 204).

- Un indirizzo IP
- 3. Fare clic su Vai.

Viene visualizzato il nome di uno o più criteri in una finestra pop-up. Vengono visualizzati molteplici criteri soltanto se nessun criterio è stato assegnato all'utente ma sono stati assegnati criteri a molteplici gruppi, domini o unità organizzative alle quali appartiene l'utente.

Anche se vengono visualizzati molteplici criteri, soltanto un criterio può venire applicato a un utente in un determinato momento (vedere *Ordine di filtraggio*, pagina 82).

Verifica filtri

Per determinare quello che accade quando un client specifico richiede l'accesso a un dato sito:

- 1. Fare clic su Verifica filtri nella Casella degli strumenti.
- 2. Per identificare una directory o un computer client, inserire:
 - Un nome utente qualificato

Per navigare o condurre una ricerca nella directory al fine di identificare l'utente, fare clic su **Trova utente** (vedere *Identificazione di un utente per verificare criteri o filtri*, pagina 204).

- Un indirizzo IP
- 3. Inserire l'URL o l'indirizzo IP del sito che si vuole verificare.
- 4. Fare clic su Vai.

La categoria del sito, l'azione applicata alla categoria e il motivo per l'azione vengono visualizzati in una finestra pop-up.

Accesso URL

Per determinare se gli utenti hanno tentato di accedere a un determinato sito nelle ultime 2 settimane; incluso oggi:

- 1. Fare clic su Accesso URL nella Casella degli strumenti.
- 2. Inserire l'URL intero o parziale o l'indirizzo IP del sito che si vuole verificare.
- 3. Fare clic su Vai.

Un report investigativo mostra se e quando si è acceduto al sito.

È possibile usare questo strumento dopo aver ricevuto un avviso di sicurezza al fine di determinare se la propria organizzazione è stata esposta a siti attaccati da phishing o infettati da un virus.

Verifica utente

Per riesaminare la storia dell'uso di Internet di un determinato clientnel corso delle ultime 2 settimane, ad esclusione di oggi:

- 1. Fare clic su Verifica utente nella Casella degli strumenti.
- 2. Inserire il nome utente o l'indirizzo IP del computer, interi o parziali.
- 3. Fare clic su Vai.

Un report investigativo visualizza la cronologia dell'uso da parte del client.

Identificazione di un utente per verificare criteri o filtri

Usare la pagina **Trova utente** per identificare un utente (directory) per lo strumento Verifica criterio o Verifica filtri.

La pagina viene aperta con l'opzione **Utente** selezionata. Espandere la cartella **Voci directory** per navigare all'interno della directory o fare clic su **Cerca**. La funzione di ricerca è disponibile soltanto se si sta usando un servizio di directory LDAP-based.

Per cercare un utente all'interno di una directory:

- 1. Inserire il **Nome** utente, intero o parziale.
- 2. Espandere l'albero **Voci directory** e navigare al suo interno per identificare un contesto di ricerca.

Occorre fare clic su una cartella (DC, OU o CN) nell'albero per specificare il contesto. Questo inserisce automaticamente i dati nel campo sottostante l'albero.

- 3. Fare clic su **Cerca**. Ogni voce che corrisponde alla stringa della ricerca viene elencato in **Risultati ricerca**.
- 4. Fare clic sul nome dell'utente per selezionare un utente o fare clic su **Cerca ancora** per inserire un nuovo termine o contesto di ricerca.

Per ritornare a navigare nella directory, fare clic su Annulla ricerca.

5. Quando il nome utente completo e corretto viene visualizzato nel campo Utente, fare clic su Vai.

Se si sta utilizzando lo strumento Verifica filtri, accertarsi che un URL o un indirizzo IP appaia nel campo URL prima di fare clic su Vai.

Per identificare un computer client anziché un utente, fare clic su Indirizzo IP.

10 Identificazione utente

Per applicare i criteri agli utenti e ai gruppi, il software Websense deve essere in grado di identificare l'utente che ha inviato la richiesta in base all'indirizzo IP d'origine. Sono disponibili vari metodi di identificazione:

- Un dispositivo, o un'applicazione di integrazione, identifica e autentica gli utenti e quindi trasmette le informazioni sull'utente al software Websense. Per ulteriori informazioni, vedere la *Guida all'installazione*.
- Un agente di identificazione trasparente di Websense agisce nel background e comunica con un servizio di directory al fine di identificare gli utenti (vedere *Identificazione trasparente*).
- Il software Websense visualizza un messaggio che richiede agli utenti di inserire le loro credenziali di rete e i loro dati di accesso quando aprono un browser Web (vedere *Autenticazione manuale*, pagina 207).

Identificazione trasparente

Argomenti correlati:

- Autenticazione manuale, pagina 207
- Configurazione dei metodi di identificazione utente trasparente, pagina 208

Normalmente, il termine **identificazione trasparente** descrive il metodo adottato dal software Websense per identificare gli utenti inclusi nel proprio servizio di directory senza dover richiedere i loro dati di accesso. Questo include l'integrazione del software Websense con un dispositivo o un'applicazione che forniscono le informazioni necessarie all'uso dei filtri,oppure l'uso di agenti di identificazione trasparente opzionali di Websense.

 Websense *DC Agent*, pagina 217viene utilizzato con un servizio di directory di ambiente Windows. L'agente conduce periodicamente delle query nei controller dei domini per ottenere informazioni sulle sessioni di collegamento degli utenti e raccoglie dati dai computer client per verificare il loro stato di collegamento. Viene eseguito in un server Windows e può essere installato in qualsiasi dominio della rete.

- Websense Logon Agent, pagina 221 identifica gli utenti nel momento in cui si ٠ collegano ai domini di Windows. L'agente viene eseguito in un server Linux o Windows, ma l'applicazione di accesso ad esso associata può venire eseguita soltanto in un computer dotato del sistema operativo Windows.
- Websense RADIUS Agent, pagina 223 può venire utilizzato insieme a un servizio ٠ di directory basato su Windows o su LDAP. L'agente usa un server e client RADIUS per identificare il collegamento degli utenti da località remote.
- Websense *eDirectory Agent*, pagina 229 viene utilizzato con Novell eDirectory. ٠ L'agente usa l'autenticazione di Novell eDirectory per mappare gli utenti ai loro rispettivi indirizzi IP.

Per istruzioni sull'installazione di ciascun agente, vedere la *Guida all'installazione*. L'agente può essere usato autonomamente o in determinate combinazioni (vedere Configurazione di molteplici agenti, pagina 235).



Nota

Se si utilizza un dispositivo NetCache integrato, NetCache dovrà inviare i nomi degli utenti al software Websense in un formato WinNT, LDAP o RADIUS affinché l'identificazione trasparente possa funzionare.

Se si dispone di un server proxy e si sta usando un agente di identificazione trasparente, è preferibile usare un'autenticazione anonima nel server proxy.

Sia le impostazioni generiche di identificazione dell'utente sia gli agenti di identificazione trasparente specifici vengono configurati in Websense Manager. Fare clic sulla scheda Impostazioni nel riquadro di navigazione di sinistra e fare quindi clic su Identificazione utente.

Per informazioni di configurazione, vedere Configurazione dei metodi di *identificazione utente trasparente*, pagina 208.

In alcune istanze, il software Websense potrebbe non essere in grado di ottenere informazioni da un agente di identificazione trasparente. Ciò si verifica se più di un utente è stato assegnato allo stesso computer o se un utente è un utente anonimo o un ospite, o per altri motivi ancora. In questi casi, è possibile visualizzare un messaggio che richiede all'utente di collegarsi tramite il browser (vedere Autenticazione manuale, pagina 207).

Identificazione trasparente di utenti remoti

In alcune configurazioni, il software Websense è in grado di identificare gli utenti che si collegano alla rete da località remote.

Se si è installato Websense Remote Filtering Server e Client Remote Filtering, il ٠ software Websense può identificare l'accesso in rete dell'utente remoto a un dominio memorizzato nella cache usando un account di dominio. Per ulteriori informazioni, vedere Filtro per i client remoti, pagina 161.

- Se si è installato DC Agent, e gli utenti remoti si collegano direttamente ai domini Windows della propria rete, DC Agent può identificare questi utenti (vedere DC Agent, pagina 217).
- Se si sta usando un server RADIUS per autenticare i collegamenti degli utenti da località remote, RADIUS Agent può identificare in modo trasparente gli utenti e consentire quindi l'applicazione dei criteri di filtro definiti per gli utenti o gruppi di utenti (vedere *RADIUS Agent*, pagina 223).

Autenticazione manuale

Argomenti correlati:

- Identificazione trasparente, pagina 205
- Impostazione delle regole di autenticazione per specifici computer, pagina 210
- Autenticazione manuale sicura, pagina 213
- Configurazione dei metodi di identificazione utente trasparente, pagina 208

L'identificazione trasparente non è sempre disponibile o desiderabile in tutti gli ambienti. Per le organizzazioni che non usano un'identificazione trasparente, o in situazioni in cui l'identificazione trasparente non è disponibile, è possibile comunque applicare un filtro basato su criteri applicabili a utenti o a gruppi usando l'**autenticazione manuale**.

L'autenticazione manuale visualizza un messaggio per gli utenti che richiede loro di inserire il nome utente e la password la prima volta che si collegano ad Internet tramite un browser. Il software Websense conferma la password tramite un servizio di directory supportato e reperisce quindi le informazioni sui criteri relative a quell'utente.

Si può configurare il software Websense in modo che sia possibile eseguire un'autenticazione manuale ogni volta che non è disponibile un'identificazione trasparente (vedere *Configurazione dei metodi di identificazione utente trasparente*, pagina 208) o che sia possibile creare un elenco di computer specifici con impostazioni di autenticazione personalizzate in base alle quali viene richiesto agli utenti, tramite un messaggio, di collegarsi quando aprono un browser (vedere *Impostazione delle regole di autenticazione per specifici computer*, pagina 210).

Se l'autenticazione manuale è attivata, gli utenti potrebbero ricevere errori HTTP e non essere in grado di accedere a Internet se:

- eseguono 3 tentativi non riusciti di inserimento di una password. Questo si verifica se il nome utente o la password non sono validi.
- fanno clic su Annulla per aggirare il messaggio di autenticazione,.

Se l'autenticazione manuale è attivata, gli utenti che non possono venire identificati non saranno autorizzati a navigare in Internet.

Configurazione dei metodi di identificazione utente trasparente

Argomenti correlati:

- *Identificazione trasparente*, pagina 205
- Autenticazione manuale, pagina 207
- Gestione di utenti e gruppi, pagina 64

Usare la pagina **Impostazioni** > **Identificazione utente** per determinare quando e come il software Websense dovrà tentare di identificare gli utenti collegati in rete al fine di applicare i criteri definiti per gli utenti o per i gruppi.

- Configurare il Policy Server in modo che possa comunicare con gli agenti di identificazione trasparente.
- Riesaminare e aggiornare le impostazioni definite per l'agente di identificazione trasparente.
- Definire una regola globale per determinare come il software Websense debba rispondere quando gli utenti non possono venire identificati da un agente o da un dispositivo integrato di identificazione trasparente.
- Identificare i computer su rete ai quali non sono applicabili le regole di identificazione utente globali e specificare se e come gli utenti di questi computer debbano venire autenticati.

Se si stanno usando gli agenti di identificazione trasparente di Websense, questi vengono elencati in **Agenti di identificazione trasparente**:

- Server visualizza l'indirizzo IP o il nome del computer che funge da host per l'agente di identificazione trasparente.
- **Porta** visualizza un elenco delle porte che il software Websense usa per comunicare con l'agente.
- Tipo indica se l'istanza specificata è un DC Agent, Logon Agent, RADIUS Agent o Directory Agent. (Vedere *Identificazione trasparente*, pagina 205 per una descrizione introduttiva di ogni tipo di agente.)

Per aggiungere un agente all'elenco, selezionare un tipo di agente dall'elenco a discesa **Aggiungi agente**. Fare clic su uno dei collegamenti seguenti per istruzioni di configurazione:

- Configurazione di DC Agent, pagina 218
- Configurazione di Logon Agent, pagina 221
- Configurazione di RADIUS Agent, pagina 226
- Configurazione di eDirectory Agent, pagina 231

Per eliminare un'istanza di agente dall'elenco, selezionare la casella di controllo dell'elenco adiacente alle informazioni sull'agente da eliminare e fare quindi clic su **Elimina**.

In **Ulteriori opzioni di autenticazione**, specificare la risposta predefinita del software Websense se gli utenti non vengono identificati in modo trasparente (da un agente o da un dispositivo di integrazione):

- Fare clic su Applica criterio di rete o del computer se si vogliono ignorare i criteri per utenti o per gruppi ed applicare invece i criteri definiti per i computer o per la rete, o i criteri predefiniti.
- Fare clic su Richiedi informazioni di accesso utente per richiedere agli utenti di inserire le credenziali di accesso quando aprono un browser. I criteri per utenti o gruppi possono ora venire applicati (vedere *Autenticazione manuale*, pagina 207).
- Specificare il Contesto di dominio predefinito che il software Websense deve usare ogni volta che visualizza un messaggio che richiede all'utente di inserire le sue credenziali di accesso. Questo è il dominio in cui le credenziali dell'utente sono valide.

Se si usa l'elenco Eccezioni per specificare i computer nei quali viene richiesto agli utenti di inserire le proprie informazioni di accesso, occorre offrire un contesto di dominio predefinito anche se la regola globale è di applicare un criterio designato per i computer o per la rete.

Dopo aver stabilito la regola generale che determina quando e come gli utenti debbano venire identificati dal software Websense, è possibile creare le eccezioni di quella regola.

Ad esempio, se si usa un agente di identificazione trasparente o un prodotto di integrazione per identificare gli utenti o se si è attivata l'autenticazione manuale con visualizzazione del messaggio che richiede agli utenti non identificabili in modo trasparente di inserire le proprie credenziali di accesso, è possibile identificare specifici computer sui quali:

- Agli utenti non identificabili non verrà mai richiesto di inserire le proprie credenziali. In altre parole, quando l'identificazione trasparente non riesce, non si esegue l'autenticazione manuale e si applicano i criteri relativi ai computer o alla rete, o i criteri predefiniti.
- Le informazioni sull'utente vengono sempre ignorate, anche se disponibili, e agli utenti verrà sempre richiesto di inserire le proprie credenziali.
- Le informazioni sull'utente vengono sempre ignorate, anche se disponibili, e agli utenti non verrà mai richiesto di inserire le proprie credenziali (e verranno applicati i criteri definiti per i computer o per la rete, o i criteri predefiniti).

Per creare un'eccezione, fare clic su **Eccezioni** e procedere quindi alla sezione *Impostazione delle regole di autenticazione per specifici computer*, pagina 210.

Una volta terminate le modifiche in questa pagina, fare clic su **OK** per salvarle. Se non si vogliono salvare le modifiche, fare clic su **Annulla**.

Impostazione delle regole di autenticazione per specifici computer

Argomenti correlati:

- Configurazione dei metodi di identificazione utente trasparente, pagina 208
- Autenticazione manuale, pagina 207
- Autenticazione manuale sicura, pagina 213

L'autenticazione selettiva consente di determinare se per gli utenti che richiedono un accesso a Internet da determinati computer client (identificati dal loro indirizzo IP) debba venire visualizzato un messaggio che richiede di inserire le loro credenziali tramite il browser. Questa opzione può essere usata per:

- stabilire regole di autenticazione diverse per il client, ad esempio, di un chiosco pubblico rispetto a quelle definite per i dipendenti dell'organizzazione che offre il chiosco.
- accertare, ad esempio, che gli utenti di un computer installato, ad esempio, nella stanza delle visite di uno studio medico, vengano sempre identificati prima di ottenere l'accesso a Internet.

I computer con impostazioni speciali di identificazione utente vengono inclusi in un elenco della pagina **Impostazioni > Identificazione utente**. Fare clic su **Eccezioni** per stabilire impostazioni specifiche di identificazione utente in relazione ad alcuni computer di rete o per verificare se alcune impostazioni speciali siano state definite per un determinato computer.

Per aggiungere un computer all'elenco, fare clic su **Aggiungi** e quindi, per ulteriori istruzioni, vedere *Definizione delle eccezioni delle impostazioni di identificazione utente*, pagina 210.

Una volta terminata l'aggiunta di intervalli di computer o di rete all'elenco, fare clic su **OK**. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Definizione delle eccezioni delle impostazioni di identificazione utente

Argomenti correlati:

- Identificazione trasparente, pagina 205
- Autenticazione manuale, pagina 207
- Configurazione dei metodi di identificazione utente trasparente, pagina 208

Utilizzare la pagina **Impostazioni > Identificazione utente > Aggiungi indirizzi IP** per identificare i computer ai quali vanno applicate regole di identificazione utente specifiche.

1. Inserire un **indirizzo IP** o un **Intervallo di indirizzi IP** per identificare i computer a cui applicare un metodo di autenticazione specifico e fare quindi clic sul pulsante con la freccia rivolta verso destra per aggiungerli all'elenco **Selezionati**.

Se la stessa regola deve venire applicata a molteplici computer, aggiungerli tutti all'elenco.

- 2. Selezionare una voce dell'elenco **Identificazione utente** per indicare se il software Websense debba cercare di identificare gli utenti di questi computer in modo trasparente.
 - Selezionare Prova a identificare l'utente in maniera trasparente per richiedere le informazioni utente a un agente di identificazione trasparente o a un dispositivo di integrazione.
 - Selezionare **Ignora le informazioni utente** per evitare l'uso di un metodo trasparente per l'identificazione degli utenti.
- 3. Indicare se agli utenti debba venire richiesto, tramite messaggio, di inserire le proprie credenziali di accesso via browser. Questa impostazione viene applicata se le informazioni sull'utente non sono disponibili in quanto un'altra identificazione non è riuscita o le informazioni sull'utente sono state ignorate.
 - Selezionare Richiedi informazioni di accesso utente per richiedere agli utenti di inserire le credenziali di collegamento.

Se anche l'opzione **Prova a identificare l'utente in maniera trasparente** è selezionata, gli utenti riceveranno un messaggio dal browser soltanto se non sono stati identificati in modo trasparente.

• Selezionare **Applica criterio di rete o del computer** per determinare che agli utenti non venga mai richiesto di inserire le loro credenziali.

Se anche l'opzione **Prova a identificare l'utente in maniera trasparente** è selezionata, gli utenti le cui credenziali possono venire verificate in modo trasparente, verranno filtrati dai criteri definiti per gli utenti.

- 4. Fare clic su **OK** per ritornare alla pagina Identificazione utente.
- 5. Al termine della procedura di aggiornamento dell'elenco Eccezioni, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Verifica delle eccezioni delle impostazioni di identificazione utente

Argomenti correlati:

- *Identificazione trasparente*, pagina 205
- Autenticazione manuale, pagina 207
- Configurazione dei metodi di identificazione utente trasparente, pagina 208

Usare la pagina **Impostazioni > Identificazione utente > Modifica indirizzi IP** per modificare le voci dell'elenco Eccezioni. Le modifiche inserite in questa pagina verranno applicate a tutti i computer (identificati in base agli indirizzi IP o a un range di indirizzi IP) visualizzati nell'elenco Selezionati.

- 1. Selezionare una voce dell'elenco **Identificazione utente** per indicare se il software Websense debba cercare di identificare gli utenti di questi computer in modo trasparente.
 - Selezionare **Prova a identificare l'utente in maniera trasparente** per richiedere le informazioni utente a un agente di identificazione trasparente o a un dispositivo di integrazione.
 - Selezionare **Ignora le informazioni utente** per evitare l'uso di un metodo trasparente per l'identificazione degli utenti.
- 2. Indicare se agli utenti debba venire richiesto, tramite messaggio, di inserire le proprie credenziali di accesso via browser. Questa impostazione viene applicata se le informazioni sull'utente non sono disponibili in quanto un'identificazione trasparente non è riuscita o l'identificazione trasparente è stata ignorata.
 - Selezionare **Richiedi informazioni di accesso utente** per richiedere agli utenti di inserire le credenziali di collegamento.

Se anche l'opzione **Prova a identificare l'utente in maniera trasparente** è selezionata, gli utenti riceveranno un messaggio dal browser soltanto se non sono stati identificati in modo trasparente.

Applica criterio di rete o del computer

Se anche l'opzione **Prova a identificare l'utente in maniera trasparente** è selezionata, gli utenti le cui credenziali possono venire verificate in modo trasparente, verranno filtrati dai criteri definiti per gli utenti.

- 3. Fare clic su **OK** per ritornare alla pagina Identificazione utente.
- 4. Al termine della procedura di aggiornamento dell'elenco Eccezioni, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Autenticazione manuale sicura

Argomenti correlati:

- Configurazione dei metodi di identificazione utente trasparente, pagina 208
- Autenticazione manuale, pagina 207
- Impostazione delle regole di autenticazione per specifici computer, pagina 210
- Attivazione dell'autenticazione manuale sicura, pagina 215

L'autenticazione manuale sicura di Websense utilizza il cifraggio Secure Sockets Layer (SSL) per proteggere i dati di autenticazione trasmessi dai computer client e dal software Websense. Un server SSL incorporato in Filtering Service esegue il cifraggio dei nomi utente e password trasmessi dai computer client al Filtering Service e viceversa. Per predefinizione, l'opzione di autenticazione manuale sicura è disattivata.

Nota

L'autenticazione manuale sicura non può venire usata con Remote Filtering. Remote Filtering Server non può visualizzare pagine di blocco nei client se è associato a un'istanza di Filtering Service con attivata un'autenticazione manuale sicura.

Per attivare questa funzione, procedere come segue:

- 1. Generare certificati e codici SSL e posizionarli in una località accessibile dal software Websense e in modo che siano leggibili da Filtering Service (vedere *Generazione di chiavi e di certificati*, pagina 214).
- 2. Attivare un'autenticazione manuale sicura (vedere *Attivazione dell'autenticazione manuale sicura*, pagina 215) e una sicura comunicazione con il servizio di directory.
- 3. Importare i certificati nel browser (vedere *Accettazione del certificato dall'interno del browser del computer client*, pagina 216).

Generazione di chiavi e di certificati

Argomenti correlati:

- *Autenticazione manuale*, pagina 207
- Impostazione delle regole di autenticazione per specifici computer, pagina 210
- Autenticazione manuale sicura, pagina 213
- Attivazione dell'autenticazione manuale sicura, pagina 215
- Accettazione del certificato dall'interno del browser del computer client, pagina 216

Il certificato consiste in una chiave pubblica, utilizzata per cifrare i dati, e una chiave privata utilizzata per decifrare i dati. I certificati vengono rilasciati da una autorità di certificazione (Certificate Authority - CA). È possibile generare un certificato da un server interno per certificazioni oppure ottenerlo da una CA indipendente, come ad esempio VeriSign.

La CA che rilascia il certificato per il client deve essere riconoscibile dal software Websense. Normalmente questo viene determinato da un'impostazione del browser.

- Per ottenere risposte a semplici domande sulle chiavi private, CSR e certificati, vedere <u>httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts</u>.
- Per istruzioni sulla generazione della propria chiave privata, CSR e certificato, vedere www.akadia.com/services/ssh_test_certificate.html.

Sono disponibili numerosi strumenti utilizzati per generare un certificato con firma automatica, inclusa la cassetta per strumenti OpenSSL (disponibili presso www.openssl.org).

Indipendentemente dal metodo scelto per la generazione del certificato, adottare le procedure descritte di seguito.

- 1. Generare una chiave privata (server.key).
- 2. Generare una Certificate Signing Request (CSR) con la chiave privata.

Importante

Quando viene visualizzato un messaggio con la richiesta di inserire il CommonName, inserire l'indirizzo IP di Filtering Server. Se si salta questa operazione, i browser del client visualizzeranno un errore nella certificazione di sicurezza.

- 3. Utilizzare il CSR per creare un certificato con firma automatica (server.crt).
- 4. Salvare il **server.crt** e **server.key** in un percorso a cui il software Websense possa accedere e dal quale Filtering Service possa leggerli.

 \mathbf{P}

Attivazione dell'autenticazione manuale sicura

Argomenti correlati:

- Autenticazione manuale, pagina 207
- Impostazione delle regole di autenticazione per specifici computer, pagina 210
- Autenticazione manuale sicura, pagina 213
- Generazione di chiavi e di certificati, pagina 214
- Accettazione del certificato dall'interno del browser del computer client, pagina 216

1. Chiudere di Websense (vedere Chiusura e riavvio dei servizi di Websense, pagina 290).

- Nel computer con Filtering Service, navigare alla directory di installazione di Websense (per predefinizione C:\Programmi File\Websense\bin oppure /opt/ Websense/bin/)./opt/websense/bin).
- 3. Individuare **eimserver.ini** e creare una copia di backup del file in un'altra directory.
- 4. Apri il file INI originale in un programma di gestione del testo.
- 5. Cercare la sezione [WebsenseServer] ed aggiungere la riga seguente:

SSLManualAuth=on

6. Sotto la riga precedente, aggiungere:

SSLCertFileLoc=[percorso]

Sostituire **[percorso]** con il percorso completo al certificato SSL, incluso il nome di file del certificato (ad esempio, C:\secmanauth\server.crt).

7. Aggiungere inoltre:

```
SSLKeyFileLoc=[percorso]
```

Sostituire **[percorso]** con il percorso completo alla chiave SSL, incluso il nome di file della chiave (ad esempio, C:\secmanauth\server.key).

- 8. Salvare e chiudere il file **eimserver.ini**.
- 9. Avviare di Websense.

Dopo l'avvio, Filtering Service ascolta le richieste inviate attraverso la porta HTTP sicura e predefinita (**15872**).

Le operazioni descritte in precedenza consentono una comunicazione sicura tra il computer client e il software Websense. Per garantire la comunicazione tra il software Websense e il servizio di directory, accertarsi che l'opzione Utilizza SSL sia selezionata nella pagina Impostazioni > Servizi di directory. Per informazioni complete, vedere Impostazioni directory avanzate, pagina 67.

Accettazione del certificato dall'interno del browser del computer

client

Argomenti correlati:

- *Autenticazione manuale*, pagina 207
- Impostazione delle regole di autenticazione per specifici computer, pagina 210
- Autenticazione manuale sicura, pagina 213
- Generazione di chiavi e di certificati, pagina 214
- Attivazione dell'autenticazione manuale sicura, pagina 215

La prima volta che si prova a navigare in un sito Web, il browser visualizza un'avvertenza relativa al certificato di sicurezza. Per evitare la visualizzazione futura di questo messaggio, installare il certificato nell'archivio dei certificati.

Microsoft Internet Explorer (Versione 7)

1. Aprire il browser ed andare a un sito Web.

Viene visualizzata un'avvertenza che indica l'esistenza di un problema con il certificato di sicurezza del sito.

- 2. Fare clic su **Continua a questo sito Web non protetto (non raccomandato)**. Se si vuole che il messaggio di autenticazione venga visualizzato, fare clic su **Annulla**.
- 3. Fare clic sulla casella **Errore certificato** a destra della barra dell'indirizzo (nell'area superiore della finestra del browser) e fare quindi clic su **Visualizza i certificati**.
- 4. Nella scheda Generale della finestra di dialogo Certificato, fare clic su **Installa il** certificato.
- 5. Selezionare Seleziona automaticamente l'archivio dei certificati in base al tipo di certificato e fare quindi clic su Avanti.
- 6. Fare clic su Fine.
- 7. Quando viene visualizzata la richiesta di installazione o non installazione del certificato, fare clic su Sì.

Gli utenti non riceveranno più avvertenze, in questo computer, sul certificato di sicurezza relativamente a Filtering Service.

Mozilla Firefox (Versione 2.x)

1. Aprire il browser ed andare a un sito Web.

Viene visualizzato un messaggio di avvertenza.

- 2. Fare clic su Accetta permanentemente il certificato[
- 3. Inserire le proprie credenziali, se richiesto da un messaggio.
- 4. Andare a **Strumenti > Opzioni** e fare quindi clic su **Avanzate**.
- 5. Selezionare la scheda Cifraggio e fare quindi clic su Visualizza i certificati.
- 6. Selezionare la scheda **Siti Web** e verificare che il certificato faccia parte dell'elenco.

Gli utenti non riceveranno più avvertenze, in questo computer, sul certificato di sicurezza relativamente a Filtering Service.

Mozilla Firefox (Versione 3.x)

1. Aprire il browser ed andare a un sito Web.

Viene visualizzato un messaggio di avvertenza.

- 2. Fare clic su Oppure si può aggiungere un'eccezione.
- 3. Fare clic su Aggiungi l'eccezione.
- 4. Accertarsi che l'opzione Archivia permanentemente questa eccezione sia selezionata e fare quindi clic su Conferma eccezione di sicurezza.

Gli utenti non riceveranno più avvertenze, in questo computer, sul certificato di sicurezza relativamente a Filtering Service.

DC Agent

Argomenti correlati:

- Identificazione trasparente, pagina 205
- Configurazione di DC Agent, pagina 218
- Configurazione di diverse impostazioni per un'istanza di agente, pagina 237

DC Agent di Websense viene eseguito in Windows e rileva gli utenti in una rete Windows con i servizi di rete NetBIOS, WINS DNS in esecuzione.

DC Agent e User Service raccolgono dati sull'utente in rete e li inviano a Filtering Service di Websense. Diverse variabili determinano la velocità della trasmissione dei dati, incluso le dimensioni della propria rete e la quantità di traffico di rete esistente. Per attivare l'identificazione trasparente con DC Agent:

1. Installare DC Agent Per ulteriori informazioni, vedere la sezione *Installing Websense Components Separately* nella *Installation Guide*.



Nota

Eseguire DC Agent usando i privilegi di amministratore del dominio. L'account amministratore del dominio deve essere un membro del gruppo di amministratori del computer in cui è installato DC Agent.

Questo è necessario per consentire a DC Agent di reperire le informazioni di accesso dal controller del dominio. Se non è possibile installare DC Agent con questi privilegi, configurare i privilegi dell'amministratore per questi servizi dopo l'installazione. Per ulteriori informazioni, vedere *Il software Websense non applica i criteri previsti per utenti o gruppi*, pagina 373.

- 2. Configurare DC Agent in modo che comunichi con gli altri componenti Websense e con i controller dei domini su rete (vedere *Configurazione di DC Agent*).
- 3. Usare Websense Manager per aggiungere al filtro utenti e gruppi (vedere *Aggiunta di un client*, pagina 70).

Il software Websense può visualizzare messaggi per gli utenti ai fini della loro identificazione se DC Agent non è in grado di identificarli in modo trasparente. Per ulteriori informazioni, vedere *Autenticazione manuale*, pagina 207.

Configurazione di DC Agent

Argomenti correlati:

- Identificazione trasparente
- Autenticazione manuale
- Configurazione dei metodi di identificazione utente trasparente
- DC Agent
- Configurazione di molteplici agenti

Usare la pagina **Impostazioni > Identificazione utente > DC Agent** per configurare una nuova istanza di DC Agent e per configurare le impostazioni globali da applicare a tutte le istanze di DC Agent.

Per aggiungere una nuova istanza di DC Agent, occorre prima di tutto inserire le informazioni di base relative al percorso di installazione dell'agente e come Filtering Service deve comunicare con DC Agent. Queste impostazioni possono essere esclusive per ciascuna istanza dell'agente.

1. In Configurazione agente di base, inserire l'indirizzo IP o il nome del **Server** in cui è stato installato l'agente.



- 2. Inserire il numero di **Porta** che DC Agent deve usare per comunicare con altri componenti Websense. Il valore predefinito è 30600.
- 3. Per stabilire un collegamento autenticato tra Filtering Service e DC Agent, selezionare l'opzione Abilita autenticazione e quindi inserire la Password per stabilire il collegamento.

Personalizzare quindi le comunicazioni globali e la diagnostica/risoluzione dei problemi di DC Agent nonché il polling del controller del dominio e le impostazioni di polling del computer. Per predefinizione, le modifiche apportate qui potrebbero incidere su tutte le istanze di DC Agent. Le impostazioni contrassegnate con un asterisco (*), tuttavia, possono venire ignorate in un file di configurazione dell'agente se si vuole personalizzare il comportamento di quell'istanza dell'agente (vedere *Configurazione di diverse impostazioni per un'istanza di agente*, pagina 237).

1. In Comunicazione DC Agent, inserire il numero della **Porta di comunicazione** da usare per le comunicazioni tra DC Agent e altri componenti Web. Il valore predefinito è 30600.

A meno che diversamente istruiti dal servizio di assistenza tecnica di Websense, non modificare l'impostazione della **Porta di diagnostica**. Il valore predefinito è 30601.

2. In Polling del controller di dominio, selezionare Attiva il polling del controller del dominio per attivare DC Agent in modo che conduca query nei controller dei domini per le sessioni di accesso dell'utente.

È possibile specificare i controller dei domini in cui ogni istanza di DC Agent deve condurre il polling, nel file di configurazione dell'agente. Per ulteriori dettagli, vedere *Configurazione di molteplici agenti*, pagina 235.

3. Usare il campo **Intervallo query** per specificare la frequenza (in secondi) con la quale DC Agent deve effettuare le query dei controller dei domini.

La riduzione dell'intervallo delle query potrebbe risultare in una maggiore accuratezza nella cattura delle sessioni di accesso ma anche incrementare il traffico complessivo di rete. L'incremento dell'intervallo delle query riduce il traffico di rete, ma potrebbe anche ritardare o impedire la cattura di alcune sessioni di accesso. Il valore predefinito è 10 secondi.

- 4. Usare il campo **Timeout voce utente** per specificare la frequenza (in ore) con la quale DC Agent deve aggiornare le voci utenti nella sua mappa. Il valore predefinito è 24 ore.
- 5. In Polling del controller di dominio, selezionare **Abilita polling del computer** per attivare DC Agent in modo che conduca query nei computer riguardo alle sessioni di accesso dell'utente. Ciò potrebbe includere i computer esterni ai domini in cui l'agente effettua già le query.

DC Agent usa WMI (Windows Management Instruction) per il polling nei computer. Se si attiva l'opzione di polling del computer, occorre configurare il Firewall di Windows nei computer client per consentire la comunicazione attraverso la porta **135**.

6. Inserire un **Intervallo di verifica mappa utenti** per specificare la frequenza con cui DC Agent deve contattare i computer client per verificare gli utenti collegati in rete. Il valore predefinito è 15 minuti.

DC Agent confronta i risultati delle query eseguite con le coppie di nomi utente/ indirizzi IP della mappa utenti che invia a Filtering Service. La riduzione di questo intervallo potrebbe risultare in una maggiore accuratezza della mappa, ma anche in un maggior traffico di rete. L'incremento dell'intervallo riduce il traffico di rete ma potrebbe anche ridurre l'accuratezza.

7. Inserire un periodo di **Timeout voce utente** per specificare la frequenza con la quale DC Agent deve aggiornare i risultati ottenuti tramite il polling dei computer nella sua mappa utenti. Il valore predefinito è 1 ora.

DC Agent elimina i nomi utente/indirizzi IP che sono più vecchi di questo periodo di timeout e che DC Agent non può confermare che siano attualmente collegati. L'incremento di questo intervallo potrebbe ridurre l'accuratezza della mappa utenti in quanto la mappa mantiene possibilmente i vecchi nomi utente per un periodo di tempo più lungo.



Non ridurre l'intervallo di timeout delle voci utente in misura superiore all'intervallo di verifica della mappa degli utenti. Ciò potrebbe causare la rimozione dei nomi utente dalla mappa degli utenti prima che possano venire verificati.

8. Fare clic su **OK** per salvare e implementare immediatamente le modifiche.

Logon Agent

Argomenti correlati:

- Identificazione trasparente, pagina 205
- Configurazione di Logon Agent, pagina 221 ٠
- Configurazione di diverse impostazioni per un'istanza di agente, pagina 237

Websense Logon identifica in tempo reale gli utenti nel momento in cui si collegano ai domini. Questo elimina la possibilità di perdere l'accesso di un utente dovuto a un problema di timing della query.

Logon Agent (chiamato anche Authentication Server) può risiedere in un computer dotato del sistema operativo Windows o Linux. L'agente funziona con Websense Logon Application (LogonApp.exe) installato nei computer client dotati di Windows al fine di identificare gli utenti nel momento in cui si collegano ai domini Windows.

Nella maggior parte dei casi è sufficiente disporre di DC Agent o di Logon Agent, ma è possibile usare entrambi gli agenti. In questo caso, Logon Agent mantiene priorità su DC Agent. DC Agent segnalerà a Filtering Service una sessione di accesso soltanto nella rara eventualità in cui Logon Agent non l'abbia rilevata.

Installare Logon Agent e quindi assegnare Logon Application ai computer client da una postazione centrale. Per ulteriori informazioni, vedere la Installation Guide.

Dopo l'installazione, configurare l'agente in modo che comunichi con i computer client e con Filtering Service di Websense (vedere Configurazione di Logon Agent).



Nota

Se si sta usando Windows Active Directory (in modalità nativa) e se User Service è installato in un computer Linux, vedere User Service in esecuzione su Linux, pagina 380 per una descrizione di altre operazioni di configurazione.

Configurazione di Logon Agent

Argomenti correlati:

- Identificazione trasparente, pagina 205
- Autenticazione manuale, pagina 207
- Configurazione dei metodi di identificazione utente trasparente, pagina 208
- Logon Agent, pagina 221 ٠
- Configurazione di molteplici agenti, pagina 235

Usare la pagina **Impostazioni > Identificazione utente > Logon Agent** per configurare una nuova istanza di Logon Agent e per configurare le impostazioni globali da applicare a tutte le istanze di Logon Agent.

Per aggiungere un'istanza di Logon Agent:

1. In Configurazione agente di base, inserire l'indirizzo IP o il nome del Server in cui è stato installato l'agente.

Nota

I nomi dei computer devono iniziare con un carattere alfanumerico (a-z), non con un carattere numerico o un carattere speciale.

I nomi dei computer che contengono determinati caratteri ASCII potrebbero non venire riconosciuti. Se si sta utilizzando una versione non di lingua inglese del software Websense, inserire un indirizzo IP anziché il nome del computer.

- 2. Inserire il numero di **Porta** che Logon Agent deve usare per comunicare con altri componenti Websense. Il valore predefinito è 30602.
- 3. Per stabilire un collegamento autenticato tra Filtering Service e Logon Agent, selezionare l'opzione **Abilita autenticazione** e quindi inserire la **Password** per stabilire il collegamento.
- 4. Fare clic su **OK** per salvare le modifiche, oppure procedere alla sezione successiva della schermata per inserire ulteriori informazioni di configurazione.

Personalizzare quindi le impostazioni di comunicazione di Logon Agent. Per predefinizione, le modifiche apportate qui potrebbero incidere su tutte le istanze di Logon Agent.

- 1. In Comunicazione Logon Agent, inserire il numero della **Porta comunicazioni** da usare per le comunicazioni tra Logon Agent e altri componenti Web. Il valore predefinito è 30602.
- A meno che diversamente istruiti dal servizio di assistenza tecnica di Websense, non modificare l'impostazione della **Porta di diagnostica**. Il valore predefinito è 30603.
- 3. In Comunicazione applicazione di accesso, specificare la **Porta collegamenti** che l'applicazione degli accessi deve utilizzare per comunicare con Logon Agent. Il valore predefinito è 15880.
- 4. Inserire il **Numero massimo di collegamenti** che ciascuna istanza di Logon Agent permette. Il valore predefinito è 200.

Se si dispone di una rete di grandi dimensioni, è possibile aumentare questo numero. Un numero più alto aumenta il traffico di rete.

5. Fare clic su **OK** per salvare le modifiche, oppure procedere alla sezione successiva della schermata per inserire ulteriori informazioni di configurazione.

Per configurare le impostazioni predefinite usate per determinare la validità di una voce utente, occorre prima di tutto definire se Logon Agent e il client dell'applicazione di accesso funzioneranno in **modalità permanente** o in **modalità non permanente** (predefinita).

La modalità non permanente viene attivata includendo il parametro /NOPERIST quando si lancia **LogonApp.exe**. (Sono disponibili ulteriori informazioni nel file **LogonApp_ReadMe.txt**, incluso con l'installazione del Logon Agent.)

• In modalità permanente, l'applicazione di accesso contatta Logon Agent periodicamente per comunicare le informazioni di accesso dell'utente.

Se ci si trova in modalità permanente, specificare un **Intervallo query** per determinare la frequenza con cui l'applicazione di accesso deve comunicare le informazioni di accesso raccolte.



Nota

Se si modifica questo valore, la modifica non viene applicata fino a quando il periodo di intervallo precedente non è stato superato. Ad esempio, se si modifica l'intervallo da 15 a 5 minuti, l'intervallo di 15 minuti deve terminare prima che la query definita su 5 minuti possa entrare in effetto.

• In modalità non permanente, l'applicazione di accesso invia le relative informazioni a Logon Agent soltanto una volta per ciascun accesso.

Se ci si trova in modalità non permanente, specificare un periodo di tempo per la **Scadenza voce utente**. Alla scadenza di questo periodo di timeout, la voce utente viene eliminata dalla mappa degli utenti.

Una volta terminate le modifiche, fare clic su OK per salvare le impostazioni definite.

RADIUS Agent

Argomenti correlati:

- *Identificazione trasparente*, pagina 205
- Gestione del traffico RADIUS, pagina 224
- *Configurazione dell'ambiente RADIUS*, pagina 225
- Configurazione di RADIUS Agent, pagina 226
- Configurazione del client RADIUS, pagina 227
- Configurazione del server RADIUS, pagina 228
- Configurazione di diverse impostazioni per un'istanza di agente, pagina 237

Websense RADIUS Agent consente di applicare i criteri definiti per utenti e gruppi usando l'autenticazione offerta dal server RADIUS. RADIUS Agent consente un'identificazione trasparente degli utenti che accedono alla rete tramite dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL) o altri tipi di collegamenti remoti (a seconda della propria configurazione).

RADIUS Agent funziona con il Server RADIUS e con il client RADIUS in rete per l'eleborazione e il monitoraggio del traffico via protocollo Remote Access Dial-In User Service (RADIUS). Questo consente di assegnare particolari criteri di filtro sia a utenti e gruppi che accedono alla rete in modalità remota, sia agli utenti locali.



Se si installa RADIUS Agent, l'agente si integra con i componenti di Websense già esistenti. Tuttavia, RADIUS AGENT, il server RADIUS e il client RADIUS devono venire configurati correttamente (vedere *Configurazione di RADIUS Agent*, pagina 226).

Gestione del traffico RADIUS

RADIUS Agent di Websense funziona come un proxy che trasferisce i messaggi RADIUS da un client RADIUS e un server RADIUS (o a molteplici client e server).

RADIUS Agent non autentica gli utenti direttamente. Al contrario, l'agente identifica gli utenti remoti e li associa agli indirizzi IP in modo che il server RADIUS possa autenticare questi utenti. Idealmente, il server RADIUS trasferisce le richieste di autenticazione a un servizio di directory basato su LDAP.

RADIUS Agent archivia l'accoppiamento nome utente-indirizzo IP in una mappa utenti. Se il client RADIUS supporta l'accounting (o la rilevazione degli accessi degli utenti) e l'accounting è attivato, RADIUS Agent reperisce più dettagli sulle sessioni di accesso dai messaggi RADIUS che riceve.

Se correttamente configurato, RADIUS Agent di Websense cattura ed elabora tutti i pacchetti di protocollo RADIUS dei tipi seguenti:

- Access-Request Inviato da un client RADIUS per richiedere l'autorizzazione ad un tentativo di collegamento di accesso alla rete.
- Access-Accept Inviato dal server RADIUS in risposta a un messaggio di Access-Request; informa il client RADIUS che il tentativo di collegamento è stato autorizzato e autenticato.
- Access-Reject Inviato dal server RADIUS in risposta a un messaggio di Access-Request; informa il client RADIUS che il tentativo di collegamento è stato respinto.
- Accounting-Stop-Request: Inviato da un client RADIUS per chiedere al server RADIUS di interrompere la rilevazione delle attività dell'utente.

Configurazione dell'ambiente RADIUS

RADIUS Agent di Websense funziona come un proxy tra un client RADIUS e un server RADIUS. Il diagramma che segue illustra in modo semplificato, come l'uso di RADIUS Agent differisca da una configurazione RADIUS standard.



RADIUS Agent e il server RADIUS vanno installati su computer separati. L'agente e il server non possono avere lo stesso indirizzo IP e devono usare porte diverse.

Dopo aver installato RADIUS Agent, configurarlo in Websense Manager (vedere *Configurazione di RADIUS Agent*, pagina 226). Si deve anche:

- Configurare il client RADIUS (normalmente un Network Access Server [NAS]) per comunicare con RADIUS Agent anziché direttamente con il server RADIUS.
- Configurare il sistema in modo che il server RADIUS utilizzi RADIUS Agent come un proxy (vedere la documentazione del server RADIUS). Se si dispone di molteplici server RADIUS, configurare ciascuno di essi separatamente.

Nota

Se si usa il server Lucent RADIUS e RRAS, occorre configurare il server RADIUS per usare il Password Authentication Protocol (PAP) e il server RRAS per accettare soltanto le richieste PAP. Per ulteriori informazioni, vedere la documentazione di accompagnamento del prodotto.

Configurazione di RADIUS Agent

Argomenti correlati:

- *Identificazione trasparente*, pagina 205
- Autenticazione manuale, pagina 207
- Configurazione dei metodi di identificazione utente trasparente, pagina 208
- *RADIUS Agent*, pagina 223
- Configurazione di molteplici agenti, pagina 235

Usare la pagina **Impostazioni > Identificazione utente > RADIUS Agent** per configurare una nuova istanza di RADIUS Agent e per configurare le impostazioni globali da applicare a tutte le istanze di RADIUS Agent.

Per aggiungere una nuova istanza di RADIUS Agent:

1. In Configurazione agente di base, inserire l'indirizzo IP o il nome del **Server** in cui l'agente è stato installato.



I nomi dei computer devono iniziare con un carattere alfanumerico (a-z), non con un carattere numerico o un carattere speciale.

I nomi dei computer che contengono determinati caratteri ASCII potrebbero non venire riconosciuti. Se si sta utilizzando una versione non di lingua inglese del software Websense, inserire un indirizzo IP anziché il nome del computer.

- 2. Inserire il numero di **Porta** che RADIUS Agent deve usare per comunicare con altri componenti Websense. Il valore predefinito è 30800.
- 3. Per stabilire un collegamento autenticato tra Filtering Service e RADIUS Agent, selezionare l'opzione **Attiva autenticazione** e quindi inserire la **Password** per stabilire il collegamento.
- 4. Fare clic su **OK** per salvare le modifiche, oppure procedere alla sezione successiva della schermata per inserire ulteriori informazioni di configurazione.

Personalizzare quindi le impostazioni globali di RADIUS Agent. Per predefinizione, le modifiche apportate qui potrebbero incidere su tutte le istanze di RADIUS Agent. Le impostazioni contrassegnate con un asterisco (*), tuttavia, possono venire ignorate in un file di configurazione dell'agente se si vuole personalizzare il comportamento di quell'istanza dell'agente (vedere *Configurazione di diverse impostazioni per un'istanza di agente*, pagina 237).

1. Inserire il numero della **Porta** usata per le comunicazioni tra RADIUS Agent e altri componenti Websense. Il valore predefinito è 30800.

- 2. A meno che diversamente istruiti dal servizio di assistenza tecnica di Websense, non modificare l'impostazione della **Porta di diagnostica**. Il valore predefinito è 30801.
- 3. In Server RADIUS, inserire l'**Indirizzo IP o il nome del server RADIUS**. RADIUS Agent inoltra le richieste di autenticazione al server RADIUS e sarà necessario conoscere l'identità di questo computer.
- 4. Se Microsoft RRAS è in esecuzione, inserire l'indirizzo IP del **Computer RRAS** Il software Websense conduce una query in questo computer per identificare le sessioni di accesso dell'utente.
- Inserire un intervallo di valori per Timeout voce utente, usato per specificare la frequenza con la quale RADIUS Agent aggiorna la sua mappa utenti. Normalmente il valore di query predefinito (24 ore) è l'impostazione migliore.
- 6. Usare le **Porte di autenticazione** e le **Porte di accounting** per specificare le porte che RADIUS Agent deve usare per inviare e per ricevere richieste di autenticazione e di accounting. Per ciascun tipo di comunicazione, è possibile specificare la porta utilizzata per le comunicazioni tra:
 - RADIUS Agent e il server RADIUS
 - RADIUS Agent e il client RADIUS
- 7. Al termine della procedura, fare clic su **OK** per salvare immediatamente le impostazioni definite.

Configurazione del client RADIUS

Il client RADIUS deve venire configurato per trasmettere le richieste di autenticazione e di accounting al server RADIUS via RADIUS Agent.

Modificare la configurazione del Client RADIUS in modo che:

- il client RADIUS invii le richieste di autenticazione al computer e alla porta dalla quale RADIUS Agent riceve le richieste di autenticazione. Questa è la Porta di autenticazione specificata durante la procedura di configurazione di RADIUS Agent.
- il client RADIUS invii le richieste di accounting al computer e alla porta dalla quale RADIUS Agent riceve le richieste di accounting. Questa è la Porta di accounting specificata durante la procedura di configurazione di RADIUS Agent.

La procedura esatta per la configurazione di un client RADIUS differisce in base al tipo di client. Per ulteriori informazioni, vedere la documentazione di accompagnamento del client RADIUS.

Nota

Il client RADIUS deve includere gli attributi **Nome utente** e **Framed-IP-Address** nei messaggi di autenticazione e di accounting che invia. RADIUS Agent utilizza i valori di questi attributi per interpretare e per memorizzare le coppie di nome utente/indirizzo IP. Se il client RADIUS non genera questa informazione per predefinizione, configurarla in modo che la generi (vedere la documentazione relativa al client RADIUS).

Configurazione del server RADIUS

Per consentire una comunicazione adeguata tra RADIUS Agent di Websense e il proprio server RADIUS:

- Aggiungere l'indirizzo IP del computer in cui risiede RADIUS Agent all'elenco dei client del server RADIUS. Per istruzioni, vedere la documentazione relativa al server RADIUS.
- Definire i segreti condivisi tra il server RADIUS e tutti i client RADIUS che usano l'agente per comunicare con il server RADIUS. I segreti condivisi vengono normalmente specificati come opzioni di sicurezza dell'autenticazione.

La configurazione di un segreto condiviso per i client RADIUS e il server RADIUS consente una trasmissione sicura dei messaggi RADIUS. Normalmente, il segreto condiviso è una stringa di testo generica. Per istruzioni, vedere la documentazione relativa al server RADIUS.

Nota

Il server RADIUS deve includere gli attributi **Nome utente** e **Framed-IP-Address** nei messaggi di autenticazione e di accounting che invia. RADIUS Agent utilizza i valori di questi attributi per interpretare e per memorizzare le coppie di nome utente/indirizzo IP. Se il server RADIUS non genera questa informazione per predefinizione, configurarlo in modo che la generi (vedere la documentazione relativa al server RADIUS).

eDirectory Agent

Argomenti correlati:

- Identificazione trasparente, pagina 205 ٠
- Configurazione di eDirectory Agent, pagina 231 ٠
- Configurazione di diverse impostazioni per un'istanza di agente, pagina 237 ٠

Websense eDirectory Agent funziona con Novell eDirectory per identificare in modo trasparente gli utenti in modo che il software Websense possa filtrarli in base ai criteri assegnati a utenti, gruppi, domini e unità organizzative.

eDirectory Agent raccoglie informazioni sugli accessi degli utenti da Novell eDirectory che autentica l'accesso degli utenti alla rete. L'agente associa quindi ciascun utente autenticato a un indirizzo IP e registra le coppie di nome utente/ indirizzo IP in una mappa di utenti locali. eDirectory Agent comunica quindi queste informazioni a Filtering Service.



Nota

Da un client Novell dotato del sistema operativo Windows, molteplici utenti possono collegarsi a un server Novell eDirectory. Questo associa un indirizzo IP a molteplici utenti. In questo scenario, la mappa utenti di eDirectory Agent conserva soltanto l'accoppiamento nome utente/ indirizzo IP per l'ultimo utente collegato in base a un determinato indirizzo IP.



Un'istanza di Websense eDirectory Agent può supportare un Novell eDirectory master, più un numero qualsiasi di repliche di Novell eDirectory.

Considerazioni speciali sulla configurazione

- Se si è integrato Cisco Content Engine v5.3.1.5 o versione superiore con il software Websense:
 - Eseguire i seguenti servizi Websense nello stesso computer in cui è installato Cisco Content Engine:

Websense eDirectory Agent Websense User Service Websense Filtering Service Websense Policy Service

- Verificare che tutte le repliche di Novell eDirectory vengano aggiunte al file wsedir.ini nello stesso computer.
- Eliminare il file eDirAgent.bak.

Eseguire Websense Reporting Tools su un computer **separato** dal software Cisco Content Engine e Websense.

• Il software Websense supporta l'uso di NMAS con eDirectory Agent. Per usare eDirectory Agent con NMAS attivato, eDirectory Agent deve essere installato nello stesso computer in cui viene eseguito Novell client.

Configurazione di eDirectory Agent

Argomenti correlati:

- *Identificazione trasparente*, pagina 205
- Autenticazione manuale, pagina 207
- Configurazione dei metodi di identificazione utente trasparente, pagina 208
- *eDirectory Agent*, pagina 229
- Configurazione di eDirectory Agent per usare LDAP, pagina 233
- Configurazione di molteplici agenti, pagina 235

Usare la pagina **Impostazioni > Identificazione utente > eDirectory Agent** per configurare una nuova istanza di eDirectory Agent e per configurare le impostazioni globali da applicare a tutte le istanze di eDirectory Agent.

Per aggiungere una nuova istanza di eDirectory Agent:

1. In Configurazione agente di base, inserire l'indirizzo IP o il nome del **Server** in cui l'agente è stato installato.



Nota

I nomi dei computer devono iniziare con un carattere alfanumerico (a-z), non con un carattere numerico o un carattere speciale.

I nomi dei computer che contengono determinati caratteri ASCII estesi potrebbero non venire riconosciuti. Se si sta utilizzando una versione non di lingua inglese del software Websense, inserire un indirizzo IP anziché il nome del computer.

- 2. Inserire il numero di **Porta** che eDirectory Agent deve usare per comunicare con altri componenti Websense. Il valore predefinito è 30700.
- 3. Per stabilire un collegamento autenticato tra il Filtering Service e eDirectory Agent, selezionare l'opzione Attiva autenticazione e quindi inserire la Password per stabilire il collegamento.
- 4. Fare clic su **OK** per salvare le modifiche, oppure procedere alla sezione successiva della schermata per inserire ulteriori informazioni di configurazione.

Personalizzare quindi le impostazioni di comunicazione di eDirectory Agent. Per predefinizione, le modifiche apportate qui potrebbero incidere su tutte le istanze di eDirectory Agent. Le impostazioni contrassegnate con un asterisco (*), tuttavia, possono venire ignorate in un file di configurazione dell'agente se si vuole personalizzare il comportamento di quell'istanza dell'agente (vedere *Configurazione di diverse impostazioni per un'istanza di agente*, pagina 237).

- 1. Inserire il numero della **Porta di comunicazione** usata per le comunicazioni tra eDirectory Agent e altri componenti Websense. Il valore predefinito è 30700.
- 2. A meno che diversamente istruiti dal servizio di assistenza tecnica di Websense, non modificare l'impostazione della **Porta di diagnostica**. Il valore predefinito è 30701.
- 3. In eDirectory Server, specificare **Base di ricerca** (contesto di base) affinché eDirectory Agent utilizzi un punto di inizio quando si cercano le informazioni per l'utente nella directory.
- 4. Inserire le informazioni relative all'account amministrativo dell'utente che eDirectory Agent deve usare per comunicare con la directory:
 - a. Inserire il **Nome distinto amministratore** per un account amministrativo utente di Novell eDirectory.
 - b. Inserire la **Password** usata per quell'account.
 - c. Specificare un intervallo **Timeout voce utente** per indicare per quanto tempo le voci devono rimanere nella mappa utenti dell'agente.

Questo intervallo deve essere di circa il 30% più lungo rispetto a una sessione di accesso tipica dell'utente. Ciò potrebbe prevenire la rimozione delle voci utente dalla mappa degli utenti prima che questi abbiano completato la navigazione.

Normalmente il valore predefinito (24 ore) è l'impostazione migliore.



In alcuni ambienti, anziché usare l'intervallo di timeout delle voci degli utenti per determinare la frequenza con cui eDirectory Agent aggiorna la sua mappa utenti, potrebbe essere opportuno eseguire una query in eDirectory Server a intervalli regolari per l'aggiornamento degli accessi eseguiti dagli utenti. Vedere *Attivazione di query complete nel server eDirectory*, pagina 234.

5. Aggiungere un server eDirectory master, oltre ad ogni replica, all'elenco **Repliche** eDirectory. Per aggiungere un server eDirectory master o una replica all'elenco, fare clic su **Aggiungi** e quindi seguire le istruzioni della sezione *Definizione delle* eccezioni delle impostazioni di identificazione utente, pagina 210.

Una volta terminate le modifiche, fare clic su OK per salvare le impostazioni definite.

Aggiunta di una replica del server eDirectory

Un'istanza di Websense eDirectory Agent può supportare un Novell eDirectory master, più un numero qualsiasi di repliche di Novell eDirectory installate in diversi computer.

eDirectory Agent deve essere in grado di comunicare con ciascun computer che esegue una replica del servizio di directory. Questo garantisce che l'agente ottenga le informazioni di accesso più recenti il più rapidamente possibile senza attendere il completamento della replica di eDirectory/ Novell eDirectory replica l'attributo che identifica in modo univoco gli utenti collegati, soltanto ogni 5 minuti. Malgrado questo ritardo nella replica, eDirectory Agent rileva le nuove sessioni di accesso non appena un utente si collega a una qualsiasi delle repliche di eDirectory/

Per configurare l'installazione di eDirectory Agent in modo che comunichi con eDirectory:

- 1. Nella schermata di replica Aggiungi eDirectory, inserire l'indirizzo IP o il nome del **Server** eDirectory (master o replica).
- 2. Inserire il numero di **Porta** che eDirectory Agent deve usare per comunicare con il computer di eDirectory.
- 3. Fare clic su **OK** per ritornare alla pagina eDirectory. La nuova voce viene visualizzata nell'elenco Repliche eDirectory.
- 4. Ripetere la procedura descritta sopra per ciascun server eDirectory.
- 5. Fare clic su **OK** per salvare le modifiche nella cache e fare quindi clic su **Salva** tutto.
- 6. Chiudere e riavviare eDirectory Agent in modo che l'agente possa iniziare a comunicare con la nuova replica. Per informazioni, vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290.

Configurazione di eDirectory Agent per usare LDAP

Websense eDirectory Agent può usare Netware Core Protocol (NCP) o Lightweight Directory Access Protocol (LDAP) per ottenere informazioni sull'accesso degli utenti da Novell eDirectory. Per predefinizione, eDirectory Agent in Windows usa NCP. In Linux, eDirectory Agent deve usare LDAP.

Se eDirectory Agent viene eseguito in Windows, ma si vuole che l'agente usi LDAP per eseguire query in Novell eDiretory, occorre definire l'uso di LDAP anziché NCP. In genere, NCP offre un meccanismo di query più efficiente.

Per definire un eDirectory Agent che utilizza LDAP:

- 1. Verificare di disporre di almeno una replica di Novell Directory contenente tutti gli oggetti della directory per monitorare e filtrare la propria rete.
- 2. Interrompere il servizio eDirectory Agent di Websense (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 3. Navigare alla directory di installazione eDirectory Agent (per predefinizione, **Programmi/Websense/bin)** ed aprire quindi il file **wsedir.ini** in un programma di gestione del testo.
- 4. Modificare la voce **QueryMethod** come descritto di seguito:

QueryMethod=0

Questo definisce che l'agente deve usare LDAP per condurre query in Novell eDirectory. (Il valore predefinito è 1, per NCP.)

- 5. Salvare e chiudere il file.
- 6. Riavviare il servizio eDirectory Agent di Websense.

Attivazione di query complete nel server eDirectory

In ambienti di rete di dimensioni limitate, è possibile configurare eDirectory Agent di Websense in modo che, ad intervalli regolari, conduca query nel server eDirectory riguardo a tutti gli utenti collegati. Questo consente all'agente di rilevare sia gli utenti che si sono appena collegati sia gli utenti che si sono scollegati a partire dall'ultima query, nonché di aggiornare di conseguenza la mappa utenti locali.

Importante

Non si consiglia una configurazione di eDirectory Agent per l'uso di query complete nel caso di ambienti di rete di grandi dimensioni in quanto il tempo richiesto per la restituzione dei risultati delle query dipende dal numero di utenti collegati. Più alto è il numero di utenti collegati, più la performance della rete ne subisce l'impatto.

Se si attiva l'opzione di query complete per eDirectory Agent, non si usa l'intervallo del **Timeout voce utente** in quanto gli utenti che sono stati scollegati vengono identificati dalla query. Per predefinizione, la query viene eseguita ogni 30 secondi.

L'attivazione di questa funzione incrementa i tempi di elaborazione di eDirectory Agent in due modi:

- incrementa il tempo necessario a reperire i nomi degli utenti collegati ogni volta che si esegue una query
- incrementa il tempo necessario ad elaborare le informazioni relative al nome utente e a eliminare le voci obsolete dalla mappa utenti locali nonché aggiungere le nuove voci ottenute dalla query più recente

eDirectory Agent esamina la mappa degli utenti locali dopo ogni query anziché identificare soltanto nuovi accessi. Il tempo necessario per l'esecuzione di questa procedura dipende dal numero di utenti restituiti da ogni query. La procedura della query può quindi incidere sui tempi di risposta sia di eDirectory Agent che del server Novell eDirectory

Per attivare le query complete:

- 1. Nel computer con eDirectory Agent, navigare alla directory **bin** di Websense (per predefinizione, C:\Programmi\Websense\bin o /opt/websense/bin).
- 2. Individuare wsedir.ini e creare una copia di backup del file in un'altra directory.
- 3. Aprire **wsedir.ini** in un programma di gestione del testo, come ad esempio Notepad o Vi.
- 4. Andare alla sezione [eDirAgent] del file e cercare la riga seguente:

QueryMethod=<N>

Annotare il valore di QueryMethod nel caso si voglia ritornare, in un secondo tempo, alle impostazioni predefinite .

5. Aggiornare il valore di QueryMethod come descritto di seguito:

- Se il valore corrente è 0 (comunicazione con la directory via LDAP), modificare il valore impostandolo su 2.
- Se il valore corrente è 1 (comunicazione con la directory via LDAP), modificare il valore impostandolo su **3**.

Nota

Se la modifica di questo valore rallenta la performance del sistema, riportare il valore di QueryMethod al suo valore precedente.

6. Se l'intervallo predefinito della query (30 secondi) non è appropriato per il proprio ambiente, modificare il valore **PollInterval** di conseguenza.

Tenere presente che l'intervallo viene impostato su millisecondi.

- 7. Salvare e chiudere il file.
- 8. Riavviare il servizio eDirectory Agent di Websense (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

Configurazione di molteplici agenti

Argomenti correlati:

- ◆ DC Agent, pagina 217
- *Logon Agent*, pagina 221
- *RADIUS Agent*, pagina 223
- *eDirectory Agent*, pagina 229

È possibile combinare molteplici agenti di identificazione trasparente all'interno della stessa rete. Se la propria configurazione di rete richiede molteplici agenti, è consigliabile installare ciascun agente in un computer separato. In alcuni casi, tuttavia, è possibile configurare il software Websense in modo che possa funzionare con molteplici agenti in un unico computer.

Sono supportate le seguenti combinazioni di agenti di identificazione trasparente:

Combinazione	Lo stesso computer?	La stessa rete?	Configurazione prevista
Molteplici DC Agent	No	Sì	Verificare che tutte le istanze di DC Agent possano comunicare con Filtering Service.
Molteplici RADIUS Agent	No	Sì	Configurare ciascuna istanza per una comunicazione con Filtering Service.

Combinazione	Lo stesso computer?	La stessa rete?	Configurazione prevista
Molteplici eDirectory Agent	No	Sì	Configurare ciascuna istanza per una comunicazione con Filtering Service.
Molteplici Logon Agent	No	Sì	Configurare ciascuna istanza per una comunicazione con Filtering Service.
DC Agent + RADIUS Agent	Sì	Sì	Installare questi agenti in directory separate. Configurare ciascun agente per una comunicazione con Filtering Service usando una porta di comunicazione diversa.
DC Agent + eDirectory Agent	No	No	Il software Websense non supporta una comunicazione con i servizi di directory di Windows e di Novel nella medesima implementazione. È possibile tuttavia avere entrambi gli agenti installati, con 1 solo agente attivo.
DC Agent + Logon Agent	Sì	Sì	Configurare ciascun agente per una comunicazione con Filtering Service. Per predefinizione, ciascun agente usa un'unica porta, per cui i conflitti relativi all'uso delle porte non costituiscono un problema a meno che queste porte non vengano modificate.
eDirectory Agent + Logon Agent	No	No	Il software Websense non supporta una comunicazione con i servizi di directory di Windows e di Novel nella medesima implementazione. È possibile tuttavia avere entrambi gli agenti installati, con 1 solo agente attivo.
RADIUS Agent + eDirectory Agent	Sì	Sì	Configurare ciascun agente per una comunicazione con Filtering Service usando una porta di comunicazione diversa.
DC Agent + Logon Agent + RADIUS Agent	Sì	Sì	Sebbene questa combinazione sia usata raramente, è di fatto supportata. Installare ciascun agente in una directory separata. Configurare tutti gli agenti per una comunicazione con Filtering Service usando diverse porte di comunicazione.

Configurazione di diverse impostazioni per un'istanza di agente

Le impostazioni di configurazione degli agenti di identificazione trasparente di Websense Manager vengono definite a livello globale e sono applicabili a tutte le istanze dell'agente installato. Se si dispone di molteplici istanze di ciascun agente, tuttavia, è possibile configurare un'istanza separatamente dalle altre.

Eventuali impostazioni univoche specificate per una particolare istanza di agente prevalgono sulle impostazioni definite nella finestra di dialogo Impostazioni. Le impostazioni su cui si ha priorità sono contrassegnate da un asterisco (*).

- 1. Interrompere il servizio dell'agente di identificazione trasparente (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Nel computer con l'istanza di agente installato, navigare alla directory di installazione dell'agente ed aprire il relativo file nel programma di gestione del testo:
 - per DC Agent: transid.ini
 - per Logon Agent: authserver.ini
 - per eDirectory Agent: wsedir.ini
 - per RADIUS Agent: wsradius.ini
- 3. Identificare il parametro usato per la modifica dell'istanza dell'agente (vedere *Parametri del file INI*, pagina 238).

Ad esempio, è possibili attivare un collegamento autenticato tra questa istanza di agente e altri servizi Websense. Per ottenere questo, inserire un valore per il parametro della **password** nel file INI:

password=[xxxxxx]

- 4. Modificare gli altri valori come necessario.
- 5. Salvare e chiudere il file INI.
- 6. Se si sono modificate le impostazioni di **DC Agent**, occorre eliminare 2 file dalla directory **bin** di Websense (predefinizione: C:\Programmi \Websense\bin.):
 - a. Chiudere tutti i servizi Websense del computer con installato eDirectory Agent (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
 - b. Eliminare i file seguenti:

```
Journal.dat
XidDcAgent.bak
Questi file vengono ricreati quando si avvia il servizio DC Agent di
Websense.
```

- c. Riavviare i servizi di Websense (compreso DC Agent) e procedere quindi al **punto 8**.
- 7. Riavviare il servizio dell'agente di identificazione trasparente.
- 8. Aggiornare le impostazioni dell'agente in Websense Manager:
 - a. Andare a Impostazioni > Identificazione utente.

b. In Agenti di identificazione trasparente, selezionare l'agente e fare quindi clic su Modifica.



- c. Verificare l'**Indirizzo IP o nome del server** e la **Porta** usata da questa istanza di agente. Se si specifica un numero di porta univoco nel file INI, verificare che questa voce corrisponda a quel valore.
- d. Se si specifica una password di autenticazione univoca nel file INI, verificare che la **Password** visualizzata sia corretta.
- e. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Parametri del file INI

Etichetta del campo Websense Manager	nome del parametro .ini	Descrizione
Porta di comunicazione (<i>tutti gli agenti</i>)	porta	La porta attraverso la quale l'agente comunica con gli altri servizi di Websense.
Porta di diagnostica (<i>tutti gli agenti</i>)	DiagServerPort	La porta attraverso la quale lo strumento di diagnostica/risoluzione problemi dell'agente rileva i dati dall'agente.
Password (<i>tutti gli agenti</i>)	password	La password che l'agente utilizza per autenticare i collegamenti ad altri servizi Websense. Specificare una password per attivare l'autenticazione.
Intervallo query (DC Agent)	QueryInterval	L'intervallo in base al quale DC Agent conduce le query nei controller dei domini.
Indirizzo IP o nome del server Porta (<i>eDirectory Agent</i>)	Server=IP:port	L'indirizzo IP e il numero di porta del computer con installato eDirectory Agent.
Base di ricerca (eDirectory Agent)	SearchBase	Il contesto di base del server Novell Directory.

Nome distinto amministratore (<i>eDirectory Agent</i>)	DN	Il nome dell'utente amministrativo per il server Novell eDirectory.
Password (eDirectory Agent)	PW	La password definita per l'utente amministrativo del server Novell eDirectory.
Indirizzo IP o nome del server RADIUS	RADIUSHost	L'Indirizzo IP o il nome del computer del server RADIUS.
Indirizzo IP del computer RRAS (Windows soltanto) (<i>RADIUS Agent</i>)	RRASHost	L'indirizzo IP del computer in cui viene eseguito RRAS. Il software Websense conduce una query in questo computer per rilevare le sessioni di accesso dell'utente.
Porte di autenticazione: tra RADIUS Agent e il server RADIUS	AuthOutPort	La porta attraverso la quale il server RADIUS rileva le richieste di autenticazione.
Porte di autenticazione: tra i client RADIUS e RADIUS Agent	AuthInPort	La porta attraverso la quale RADIUS Agent accetta le richieste di autenticazione.
Porte di accounting: tra RADIUS Agent e il server RADIUS	AccOutPort	La porta attraverso la quale il server RADIUS rileva i messaggi di accounting.
Porte di accounting: tra i client RADIUS e il RADIUS Agent	AccInPort	La porta attraverso la quale RADIUS Agent accetta le richieste di accounting.

Configurazione di un agente affinché ignori determinati nomi utente

È possibile configurare un agente di identificazione trasparente in modo che ignori i nomi non associati agli utenti effettivi. Questa funzione viene spesso usata per gestire il modo in cui i servizi di Windows 200x e XP devono contattare i controller dei domini nella propria rete.

Ad esempio, **user1** si collega in rete e viene identificato dai controller del dominio come **computerA/user1**. Quell'utente viene filtrato da un criterio Websense assegnato a **user1**. Se un servizio viene avviato nel computer di un utente che assume l'identità **computerA/ServiceName** al fine di contattare il controller dei domini, questo può causare dei problemi di filtro. Il software Websense tratta **computerA/ ServiceName** come un nuovo utente senza alcun criterio ad esso assegnato e filtra questo utente in base al criterio assegnato al computer, oppure in base al criterio **Predefinito**.

Per risolvere questo problema:

- 1. Chiudere Agent Service (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Navigare alla directory \Websense\bin\ ed aprire il file ignore.txt in un programma di gestione del testo.
- 3. Inserire ciascun nome utente in una riga separata. Non includere caratteri jolly, come ad esempio "*":

```
maran01
WindowsServiceName
```

Il software Websense ignora i nomi utente indipendentemente dai computer ad essi associati.

Per fare in modo che il software Websense ignori un nome utente nell'ambito di un determinato dominio, usare il formato **nome utente, dominio**

aperez, engineering1

- 4. Una volta terminato, salvare e chiudere il file.
- 5. Riavviare Agent Service.

L'agente ignora i nomi utente specificati e il software Websense non considera questi nomi nel filtro.

11 Amministrazione con delega

Argomenti correlati:

- Introduzione ai ruoli amministrativi, pagina 242
- Introduzione alle funzioni di amministratore, pagina 243
- Concetti di base sui ruoli amministrativi, pagina 247
- Attivazione dell'accesso a Websense Manager, pagina 255
- Uso dell'amministrazione con delega, pagina 259
- Molteplici amministratori in accesso a Websense Manager, pagina 270
- Definizione delle restrizioni di filtraggio per tutti i ruoli, pagina 271

Gli amministratori con delega dispongono di metodi potenti e flessibili per la gestione dei filtri Internet e per la creazione di report per gruppi specifici di client. È un sistema efficace per distribuire responsabilità relative alla gestione degli accessi in Internet e alla creazione di report da inviare ai manager quando tutti gli utenti risiedono in una località centralizzata. È particolarmente efficace in grandi organizzazioni che includono molteplici località e regioni geografiche e consente agli amministratori locali di gestire gli accessi in Internet e generare report sull'attività di filtraggio per gli utenti della loro area.

L'implementazione di un'amministrazione con delega implica la creazione di un ruolo amministrativo per ciascun gruppo di client gestito dagli stessi amministratori. I singoli amministratori, qualunque sia il ruolo a cui sono stati assegnati, possono ottenere le necessarie autorizzazioni per la gestione dei criteri o la creazione di report per i loro client o entrambi. Vedere *Concetti di base sui ruoli amministrativi*, pagina 247.

Il ruolo di Super Administrator è un ruolo pre-installato che include l'utente amministrativo predefinito: WebsenseAdministrator. I Super Administrator hanno accesso a una gamma più ampia di criteri e di impostazioni di configurazione rispetto agli amministratori assegnati ad altri ruoli. Vedere *Super Administrator*, pagina 243.

Introduzione ai ruoli amministrativi

Argomenti correlati:

- Introduzione alle funzioni di amministratore, pagina 243
- Concetti di base sui ruoli amministrativi, pagina 247

Il ruolo amministrativo è costituito da un gruppo di client — utenti, gruppi, domini, unità organizzative, intervalli di computer e di rete — gestiti da uno o più amministratori. È possibile assegnare ai singoli amministratori le autorizzazioni necessarie per l'applicazione di determinati criteri ai client appartenenti a un determinato ruolo o per la creazione di report, o entrambi.

Il software Websense viene inviato con un ruolo di Super Administrator predefinito. Esiste inoltre un utente predefinito, denominatoWebsenseAdministrator, che è automaticamente un membro del ruolo di Super Administrator. È possibile aggiungere altri amministratori a questo ruolo, ma non è possibile eliminare l'amministratore predefinito.

Importante

Non è consentito eliminare il ruolo predefinito di Super Administrator. L'utente predefinito, chiamato
WebsenseAdministrator, è un amministratore nel ruolo di Super Administrator, ma non è incluso nell'elenco di quel ruolo. Non è consentito eliminare o modificare i permessi assegnati a WebsenseAdministrator.

Si possono creare tanti ruoli quanti sono necessari per la propria organizzazione. Ad esempio, si può creare un ruolo per ciascun reparto, con il manager del reparto designato come amministratore e i membri del reparto come client gestiti. In un'organizzazione con sedi in varie località geografiche, è possibile creare un ruolo per ciascuna località e designare tutti gli utenti di una località come client gestiti di quel ruolo. Si può quindi procedere a designare uno o più individui di una determinata località come amministratori.

Per informazioni sulle opzioni disponibili per la definizione degli amministratori, vedere *Introduzione alle funzioni di amministratore*, pagina 243.

Vedere *Uso dell'amministrazione con delega*, pagina 259 per istruzioni sulla creazione di ruoli e sulla configurazione delle autorizzazioni.

Introduzione alle funzioni di amministratore

Gli amministratori sono gli individui che possono accedere a Websense Manager per la gestione dei criteri o la creazione di report per un gruppo di client. Le autorizzazioni disponibili specifiche dipendono dal tipo di ruolo.

- Il Super Administrator è un ruolo speciale predefinito in Websense Manager. Questo ruolo offre la massima flessibilità nella definizione delle autorizzazioni all'accesso. Vedere Super Administrator, pagina 243.
- ◆ I ruoli di amministrazione con delega devono venire creati da un Super Administrator. Gli amministratori di questi ruoli possiedono autorizzazioni di accesso più limitate. Vedere *Amministratori con delega*, pagina 245.

È possibile inoltre creare alcuni ruoli di amministrazione con delega a scopo di creazione di report soltanto, consentendo in tal modo a vari individui di generare dei report senza per questo assegnare loro la responsabilità della gestione dei criteri.

È possibile assegnare gli amministratori a determinati ruoli usando le loro credenziali di accesso alla rete oppure è possibile creare account speciali utilizzati soltanto per accedere a Websense Manager. Vedere *Attivazione dell'accesso a Websense Manager*, pagina 255.

Super Administrator

Argomenti correlati:

- Introduzione alle funzioni di amministratore, pagina 243
- Amministratori con delega, pagina 245
- Amministratori in molteplici ruoli, pagina 246

Il ruolo di Super Administrator viene creato durante la procedura di installazione. L'utente predefinito, WebsenseAdministrator, viene automaticamente assegnato a questo ruolo. Perciò quando ci si collega per la prima volta usando il nome utente e la password impostati durante l'installazione, si ottiene un accesso amministrativo completo a tutti i criteri, alle funzioni di creazione dei report e alle impostazioni di configurazione di Websense Manager.

Per mantenere un accesso completo a questo account, il WebsenseAdministrator non appare nell'elenco degli amministratori con ruolo di Super Administrator. Non può venire eliminato e le autorizzazioni a lui assegnate non possono venire modificate.

È possibile aggiungere amministratori al ruolo di Super Administrator, come necessario. A ciascun amministratore possono venire concesse delle autorizzazioni, come descritto qui di seguito:

• Le autorizzazioni relative ai **Criteri** consentono ai Super Administrator di creare e di modificare i ruoli di amministrazione con delega nonché di copiare i filtri e i criteri in questi ruoli, come necessario. Sono anche autorizzati a creare e modificare i componenti del filtraggio, i filtri e i criteri, e possono applicare dei criteri ai client non gestiti da un altro ruolo.

I Super Administrator, con autorizzazione di gestione dei criteri, possono inoltre visualizzare il registro di controllo e possono accedere alla configurazione di Websense e ad altre opzioni, come descritto qui di seguito:

 L'opzione di autorizzazione totale assegna al Super Administrator un accesso a tutte le impostazioni di configurazione del sistema per l'installazione di Websense, come ad esempio le impostazioni relative agli account, a Policy Server, a Remote Filtering Server, e alle opzioni relative all'assegnazione alle classi di rischio e alla registrazione.

Gli utenti con qualifica totale di Super Administrator hanno la possibilità di creare un Blocco filtro che blocca determinate categorie e protocolli per tutti gli utenti gestiti dai ruoli di amministrazione con delega. Vedere *Definizione delle restrizioni di filtraggio per tutti i ruoli*, pagina 271 per ulteriori informazioni.

Gli utenti con qualifica totale di Super Administrator possono modificare il ruolo di Super Administrator aggiungendo ed eliminando amministratori, come necessario. Possono inoltre eliminare i ruoli di amministrazione con delega o eliminare amministratori o client da questi ruoli.

Tramite le autorizzazioni parziali si può assegnare ai Super Administrator l'accesso al download dei database, ai servizi di directory, all'identificazione utenti e alle impostazioni di configurazione di Network Agent. Gli utenti con qualifica parziale di Super Administrator, che possiedono anche autorizzazioni di creazione dei report, possono accedere alle impostazioni di configurazione degli strumenti di creazione dei report.

Gli utenti con qualifica parziale di Super Administrator possono aggiungere gli account utente ma non possono eliminarli. Possono creare e modificare i ruoli di amministrazione con delega ma non possono eliminare ruoli, eliminare gli amministratori o i client a loro assegnati. Non possono inoltre eliminare amministratori dal ruolo di Super Administrator.

 Le autorizzazioni relative alla Creazione report consentono ai Super Administrator di accedere a tutte le funzioni di creazione dei report nonché di creare report su tutti gli utenti. Agli utenti con qualifica totale di Super Administrator viene automaticamente assegnata l'autorizzazione alla creazione dei report.

Se ad un amministratore è stata assegnata soltanto l'autorizzazione per la creazione di report, le opzioni Crea criterio, Ricategorizza URL e Sblocca URL dell'elenco Operazioni comuni non sono disponibili. Inoltre, l'opzione Verifica criterio della Casella degli strumenti non è disponibile.

La creazione di molteplici utenti con qualifica totale di Super Administrator garantisce che se il Super Administrator principale non è disponibile, un altro amministratore avrà accesso a tutti i criteri e alle impostazioni di configurazione di Websense.

Tenere presente che 2 amministratori non possono collegarsi simultaneamente per gestire i criteri di uno stesso ruolo. Per ulteriori informazioni sulla prevenzione di

eventuali conflitti, vedere *Molteplici amministratori in accesso a Websense Manager*, pagina 270.

I privilegi esclusivi del ruolo di Super Administrator consentono ad un amministratore in quel ruolo di accedere a tutti i ruoli. Per passare a un altro ruolo dopo l'accesso, andare all'elenco **Ruolo**, situato nell'area dell'intestazione, e selezionare il ruolo di interesse.

Dopo essere passati a un altro ruolo, le autorizzazioni relative alla gestione dei criteri sono limitate a quelle assegnate al ruolo di amministratore con delega. I filtri e i criteri che si creano sono disponibili soltanto agli amministratori in quel ruolo. Possono venire applicati soltanto ai client gestiti in quel ruolo. Vedere *Amministratori con delega*, pagina 245.

Le autorizzazioni alla creazione dei report sono cumulative, ossia si ottengono le autorizzazioni combinate di tutti i ruoli dei quali si è amministratore. Gli utenti con qualifica totale di Super Administrator posseggono un'autorizzazione completa alla creazione dei report, indipendentemente dal ruolo a cui hanno acceduto.

Amministratori con delega

Argomenti correlati:

- Introduzione alle funzioni di amministratore, pagina 243
- Super Administrator, pagina 243
- Amministratori in molteplici ruoli, pagina 246

Gli Amministratori con delega gestiscono i client assegnati a un ruolo specifico. Si può assegnare a ciascun amministratore l'autorizzazione alla gestione dei criteri o alla creazione dei report o entrambi.

Gli amministratori con delega che possiedono l'autorizzazione alla gestione dei **criteri**, applicano tali criteri ai client assegnati al loro ruolo e possono quindi determinare l'accesso a Internet disponibile per ogni client. Come parte di questa responsabilità, gli amministratori con delega possono creare, modificare ed eliminare criteri e filtri soggetti alle restrizioni imposte dall'opzione Blocco filtro, definita dal

Super Administrator. Vedere *Definizione delle restrizioni di filtraggio per tutti i ruoli*, pagina 271.



Gli amministratori con delega non possono eliminare i criteri predefiniti.

Gli amministratori con delega possono modificare i componenti dei filtri con alcune limitazioni. Per ulteriori informazioni, vedere *Creazione di criteri e filtri*, pagina 253.

Gli amministratori, con autorizzazione alla gestione dei criteri, che si collegano a Websense Manager con un account utente Websense possono modificare anche la loro password di accesso a Websense. (Vedere *Account utenti Websense*, pagina 257.)

Le opzioni disponibili agli amministratori con delega con autorizzazione alla creazione dei **report** variano in base alla configurazione del ruolo. Potrebbero essere autorizzati a generare dei report soltanto sui client gestiti, in base al loro ruolo, o generare report su tutti i client. Potrebbero avere accesso a tutte le funzioni di creazione dei report o potrebbero avere soltanto un accesso limitato a tali funzioni. Per ulteriori informazioni, vedere *Modifica dei ruoli*, pagina 261.

Un amministratore che possiede soltanto l'autorizzazione alla creazione dei report, dispone di opzioni limitate tra quelle disponibili nel riquadro dei collegamenti di destra (Operazioni comuni e Casella degli strumenti).

Amministratori in molteplici ruoli

Argomenti correlati:

- Introduzione alle funzioni di amministratore, pagina 243
- Super Administrator, pagina 243
- Amministratori con delega, pagina 245

A seconda delle necessità della propria organizzazione, lo stesso amministratore potrebbe venire assegnato a molteplici ruoli. Gli amministratori assegnati a molteplici ruoli devono scegliere, al momento dell'accesso, un solo ruolo da gestire.

Dopo l'accesso, le autorizzazioni sono quelle descritte qui di seguito:

- Criteri È possibile aggiungere e modificare i filtri e i criteri per il ruolo selezionato durante l'accesso ed applicare i criteri ai client gestiti di quel ruolo. La pagina Amministrazione con delega elenca tutti i ruoli ai quali si è stati assegnati, consentendo di visualizzare i client gestiti da ciascun ruolo nonché le autorizzazioni alla creazione dei report.
- Creazione report Si possiedono tutte le autorizzazioni combinate in riferimento alla creazione dei report per tutti i ruoli assegnati. Ad esempio, supponiamo di aver ricevuto l'assegnazione a 3 ruoli, con l'autorizzazione alla creazione dei report, come segue:
 - Ruolo 1: nessuna creazione di report
 - Ruolo 2: creazione dei report soltanto per i client gestiti e soltanto per i report investigativi
 - Ruolo 3: creazione dei report per tutti i client, completo accesso a tutte le funzioni relative alla creazione dei report

In questa situazione, indipendentemente dal ruolo scelto durante l'accesso, si è autorizzati a visualizzare i report nelle pagine Oggi e Cronologia, a creare report per tutti i client e a usare tutte le funzioni relative ai report.

Se si è acceduto soltanto a scopo di creazione dei report, il campo Ruolo, nella barra dell'intestazione, indica se si possiede l'autorizzazione ad una Creazione completa dei report (report su tutti i client) o ad una Creazione limitata dei report (report soltanto sui client gestiti).

Concetti di base sui ruoli amministrativi

Argomenti correlati:

- Introduzione ai ruoli amministrativi, pagina 242
- Notifica agli Amministratori, pagina 250
- *Operazioni degli amministratori con delega*, pagina 251

Tenere presente innanzi tutto che l'amministrazione con delega richiede che il Super Administrator completi le seguenti operazioni:

- Determinare come gli amministratori devono accedere a Websense Manager. Vedere Attivazione dell'accesso a Websense Manager, pagina 255.
- Aggiungere i ruoli e configurarli. Vedere *Uso dell'amministrazione con delega*, pagina 259.
- Informare gli amministratori delle loro responsabilità e delle opzioni a loro disponibili. Vedere *Notifica agli Amministratori*, pagina 250.

In aggiunta a queste operazioni necessarie, esistono altre operazioni facoltative associate all'amministrazione con delega.

Creazione di un Blocco filtro

Gli utenti con qualifica parziale di Super Administrator hanno la possibilità di creare un Blocco filtro che determini il blocco di alcune categorie e protocolli per tutti gli utenti gestiti in tutti i ruoli di amministrazione con delega. Queste restrizioni vengono automaticamente imposte a tutti i filtri creati o copiati in un ruolo di amministrazione con delega e non possono venire modificate dall'amministratore con delega.

Nota

Il Blocco filtro non viene applicato ai client gestiti dal ruolo di Super Administrator.

Il Blocco filtri può inoltre bloccare i tipi di file e le parole chiave associate alle categorie selezionate e forzare la registrazione dei protocolli selezionati. Vedere *Creazione di un Blocco filtro*, pagina 272.

Spostamento dei client

L'aggiunta di un client alla pagina dei Client mentre si è collegati come Super Administrator assegna automaticamente quel client al ruolo di Super Administrator. Quel client non può venire aggiunto a un ruolo di amministrazione con delega nella pagina Modifica ruolo. Idealmente, i client andrebbero aggiunti direttamente al ruolo anziché assegnare un criterio dal ruolo di Super Administrator. Tuttavia, questo non è sempre possibile.

Per trasferire i client dal ruolo di Super Administrator a un altro ruolo, usare l'opzione **Passa al ruolo** nella pagina Client. Vedere *Spostamento dei client a ruoli diversi*, pagina 72.

Come parte dello spostamento, il criterio applicato al ruolo di Super Administrator, viene copiato nel ruolo di amministrazione con delega. Vengono copiati anche i filtri applicati in base a quel criterio. Durante questa procedura di copia, i filtri vengono aggiornati per imporre le restrizioni dell'opzione Blocco filtro, se necessario.

Nel ruolo di destinazione, il tag "(copiato)" viene aggiunto alla fine del nome del filtro o del criterio. Gli amministratori di quel ruolo possono identificare in modo immediato la nuova voce ed aggiornarla come necessario.

Nota

Ogni volta che un filtro o un criterio viene copiato nello stesso ruolo, il tag (Copiato) riceve un numero progressivo per ogni nuova copia. (copiato 1), (copiato2) e così via. Ciascuno di essi diventa un filtro o un criterio separato nell'ambito di quel ruolo.

Incoraggiare gli amministratori di quel ruolo ad assegnare un nuovo nome ai filtri e ai criteri e a modificarli come necessario, per rendere più chiare le proprie impostazioni e minimizzare i duplicati. Queste modifiche possono semplificare eventuali operazioni di manutenzione successive. I filtri di Autorizza sempre del ruolo di Super Administrator consentono di accedere a tutte le categorie o protocolli e non possono venire modificati. Per preservare la capacità del Super Administrator di implementare un Blocco filtro, questi filtri non possono venire copiati nel ruolo di amministrazione con delega.

Se il criterio assegnato al client in corso di spostamento impone l'applicazione del filtro Autorizza sempre, il client non può venire spostato fino a quando non si applica un criterio che non usa il filtro Autorizza sempre.

Dopo che il client è stato spostato al nuovo ruolo, soltanto un amministratore in quel ruolo potrà modificare i criteri o i filtri applicati al client. Le modifiche apportate ai criteri o ai filtri originali nel ruolo di Super Administrator non incidono sulle copie dei criteri o dei filtri nei ruoli di amministrazione con delega.

Copia di filtri e criteri

Inizialmente i filtri e i criteri creati da un Super Administrator sono disponibili soltanto per gli amministratori con il ruolo di Super Administrator. Si può usare l'opzione **Copia nel ruolo** per copiare filtri e criteri nel ruolo di amministrazione con delega senza spostare un client in quel ruolo. Vedere *Copia di filtri e criteri nei ruoli*, pagina 177.

Se si copiano filtri e criteri direttamente, vengono applicate le stesse restrizioni di quando i filtri e i criteri vengono copiati come parte dello spostamento di un client.

- La restrizioni di Blocca filtro vengono implementate durante la procedura di copia.
- I filtri di categoria e di protocollo di Autorizza sempre non possono venire copiati.
- I filtri e i criteri copiati vengono identificati nel ruolo per mezzo del tag (Copiato) accanto al loro nome.

Valutare la possibilità di modificare la descrizione dei criteri, prima di iniziare la copia, per essere certi che siano facilmente comprensibili per gli amministratori nei ruoli di destinazione.

Applicazione dei ruoli ai client rimasti

I client che non vengono specificatamente assegnati a un ruolo di amministrazione con delega vengono gestiti dai Super Administrator. Non esiste un elenco di Client gestiti per il ruolo di Super Administrator.

Per applicare i criteri a questi client, aggiungerli alla pagina Gestione criteri > Client. Vedere *Aggiunta di un client*, pagina 70. I client che non sono stati assegnati a un criterio specifico sono soggetti alle regole definite dai criteri predefiniti per quel ruolo.

Potrebbe a volte accadere che non è possibile aggiungere client alla pagina Client. Questo potrebbe essere dovuto al fatto che il client è un membro della rete, del gruppo, del dominio o dell'unità organizzativa assegnata a un altro ruolo. Se l'amministratore di quest'altro ruolo ha applicato un criterio ai singoli membri di una rete o di un gruppo, quei client non possono venire aggiunti al ruolo di Super Administrator.

Notifica agli Amministratori

Argomenti correlati:

- Introduzione ai ruoli amministrativi, pagina 242
- Concetti di base sui ruoli amministrativi, pagina 247

Dopo aver assegnato ad alcuni individui il ruolo di amministratore, verificare che vengano loro inviate le informazioni seguenti.

• L'URL usato per collegarsi a Websense Manager. Predefinizione:

```
https://<ServerIP>:9443/mng/
```

Sostituire <ServerIP> con l'indirizzo IP del computer in cui è installato Websense Manager.

- Il Policy Server da scegliere durante l'accesso, se applicabile. In un ambiente con molteplici Policy Server, gli amministratori devono scegliere un Policy Server durante l'accesso. Devono scegliere un Policy Server configurato in modo da comunicare con il servizio di directory che autentica i client da loro gestiti.
- Se si deve usare il proprio account di accesso in rete o un account utente di Websense quando si accede a Websense Manager. Se gli amministratori accedono tramite un account utente di Websense, fornire il nome utente e la password.
- Le loro autorizzazioni, sia in termini di creazione e applicazione dei criteri ai client di quel ruolo, che in termini di creazione dei report, o entrambi.

Consigliare agli amministratori che possiedono l'autorizzazione di gestione sia dei criteri che dei report a tenere presente le attività che intendono eseguire durante la sessione. Se intendono soltanto creare dei report, consigliare loro di andare al campo **Ruolo** nell'intestazione e di scegliere **Rilascio autorizzazione criterio**. Questo rende disponibile l'autorizzazione di gestione dei criteri per il ruolo consentendo a un altro amministratore di accedere a Websense Manager e di gestire i criteri per quel ruolo.

- Come trovare l'elenco dei client gestiti da quel ruolo. Gli amministratori possono andare a Gestione criteri > Amministrazione con delega e quindi fare clic sul nome del loro ruolo per visualizzare la pagina Modifica ruolo, che include un elenco di client gestiti.
- Le restrizioni imposte da Blocca filtro, se alcune categorie o alcuni protocolli sono stati bloccati.
- Le operazioni normalmente eseguite dagli amministratori. Vedere *Operazioni degli amministratori con delega*, pagina 251.

Accertare che gli amministratori con delega vengano notificati quando si aggiungono o si modificano dei tipi di file e dei protocolli personalizzati. Questi componenti vengono automaticamente visualizzati nei filtri e nei criteri di tutti i ruoli, per cui è importante che questi amministratori siano al corrente quando vengono apportate modifiche.

Operazioni degli amministratori con delega

Argomenti correlati:

- Introduzione ai ruoli amministrativi, pagina 242
- Concetti di base sui ruoli amministrativi, pagina 247
- Notifica agli Amministratori, pagina 250

Gli amministratori con delega che possiedono l'autorizzazione di gestione dei **criteri** possono eseguire le operazioni seguenti.

- Visualizzazione dell'account utente, pagina 251
- Visualizzazione della definizione del proprio ruolo, pagina 252
- Aggiunta di client alla pagina Client, pagina 252
- Creazione di criteri e filtri, pagina 253
- Applicazione di criteri ai client, pagina 254

L'autorizzazione alla **Creazione report** può venire attivata o disattivata per i vari componenti dei report. Autorizzazioni specifiche alla creazione dei report assegnate al proprio ruolo determinano quali delle seguenti operazioni sono disponibili per gli amministratori con autorizzazione alla creazione dei report. Vedere *Generazione di report*, pagina 255.

Visualizzazione dell'account utente

Argomenti correlati:

- Operazioni degli amministratori con delega, pagina 251
- Visualizzazione della definizione del proprio ruolo, pagina 252
- Aggiunta di client alla pagina Client, pagina 252
- Creazione di criteri e filtri, pagina 253
- Applicazione di criteri ai client, pagina 254

Se si accede a Websense Manager con le credenziali di rete, eventuali modifiche apportate alle password vengono gestite dal servizio di directory della rete. Per assistenza, contattare il proprio amministratore di sistema.

Se si è ricevuta l'assegnazione di un nome utente e password per accedere a Websense, visualizzare le informazioni relative al proprio account e modificare la propria password all'interno di Websense Manager.

- 1. Andare a Gestione criteri > Amministrazione con delega.
- 2. Fare clic su Gestisci account utente Websense nell'area superiore della pagina.

- 3. Fare clic su **Modifica password** se si vuole modificarla. Vedere *Modifica della password utente di Websense*, pagina 258.
- 4. Fare clic su **Visualizza** per visualizzare un elenco di ruoli di cui si è amministratore.

Visualizzazione della definizione del proprio ruolo

Argomenti correlati:

- Operazioni degli amministratori con delega, pagina 251
- Visualizzazione dell'account utente, pagina 251
- Aggiunta di client alla pagina Client, pagina 252
- Creazione di criteri e filtri, pagina 253
- Applicazione di criteri ai client, pagina 254

Aprire la pagina Amministrazione con delega e fare clic sul nome del ruolo per visualizzare la pagina Modifica ruolo, che include un elenco di client gestiti in funzione di quel ruolo. Questa pagina visualizza anche le opzioni di creazione dei report disponibili per gli amministratori che possiedono le autorizzazioni di Creazione report assegnate a questo ruolo.

Gli amministratori che possiedono soltanto autorizzazioni per la creazione dei report non possono visualizzare questa pagina. Per questi amministratori sono disponibili soltanto le funzioni specificate per la creazione dei report.

Aggiunta di client alla pagina Client

Argomenti correlati:

- Operazioni degli amministratori con delega, pagina 251
- Visualizzazione dell'account utente, pagina 251
- Visualizzazione della definizione del proprio ruolo, pagina 252
- Creazione di criteri e filtri, pagina 253
- Applicazione di criteri ai client, pagina 254

I Super Administrator assegnano i client gestiti a un determinato ruolo, ma gli amministratori con delega devono aggiungerli alla pagina Client prima di poter applicare i relativi criteri. Per istruzioni, vedere *Aggiunta di un client*, pagina 70.

Non appena si aggiungono dei client all'elenco dei client gestiti da un determinato ruolo, i client aggiunti vengono filtrati dai criteri predefiniti assegnati al ruolo. I client che sono stati spostati al ruolo dalla pagina Client del Super Administrator sono soggetti ai criteri applicati dai Super Administrator e che erano stati copiati nel ruolo quando il client era stato spostato.
I client inseriti nell'elenco della pagina Amministrazione con delega > Modifica ruolo per il proprio ruolo, possono venire aggiunti alla pagina Client e può venire loro assegnato un criterio. È anche possibile aggiungere singoli utenti o computer membri di un gruppo, di un dominio o di un'unità organizzativa o di un intervallo di rete, assegnati al proprio ruolo come client gestiti.

Poiché un utente può far parte di molteplici gruppi, domini o unità organizzative, l'aggiunta di individui da un gruppo di client più esteso, può potenzialmente creare dei conflitti quando diversi ruoli gestiscono gruppi, domini o unità organizzative con membri in comune. Se degli amministratori assegnati a diversi ruoli accedono simultaneamente a Websense Manager, potrebbero aggiungere lo stesso client (ad esempio, un membro di un gruppo) alla loro pagina Client. In questo caso, il filtro di accesso a Internet per quel client è soggetto ai diritti di priorità definiti per quel ruolo. Vedere *Gestione dei conflitti di ruolo*, pagina 268.

Creazione di criteri e filtri

Argomenti correlati:

- Operazioni degli amministratori con delega, pagina 251
- Visualizzazione dell'account utente, pagina 251
- Visualizzazione della definizione del proprio ruolo, pagina 252
- Aggiunta di client alla pagina Client, pagina 252
- Applicazione di criteri ai client, pagina 254

Al momento della creazione di un ruolo, questo eredita automaticamente il criterio, il filtro di categoria e il filtro di protocollo predefiniti e preinstallati, così come erano definiti in quel particolare momento. Potrebbero anche esistere criteri e filtri che il Super Administrator ha copiato in quel ruolo.

Oltre ai criteri e ai filtri, è anche possibile ereditare tipi di file e protocolli personalizzati, creati dal Super Administrator.

Si è tuttavia liberi di modificare i criteri e i filtri ereditati dal Super Administrator. Le modifiche apportate incidono soltanto sul ruolo. Qualsiasi modifica che il Super Administrator apporta a criteri e filtri che si sono ereditati in precedenza, non ha alcun impatto sul ruolo.

Nota

Qualsiasi modifica applicata dal Super Administrator a tipi di file e protocolli personalizzati ha un impatto automatico sui filtri e sui criteri di quel ruolo.

Se si viene informati dal Super Administrator delle modifiche apportate a questi componenti, riesaminare i filtri e i criteri per essere certi di gestirli correttamente. È anche possibile creare il numero di filtri e criteri necessari. I filtri e i criteri creati da un amministratore con delega sono disponibili soltanto per gli amministratori che hanno acceduto al proprio ruolo. Per istruzioni sulla creazione dei criteri, vedere *Gestione dei criteri*, pagina 77. Per istruzioni sulla creazione dei filtri, vedere *Gestione dei filtri*, pagina 48.

È possibile modificare i componenti dei filtri per il proprio ruolo, con alcune limitazioni.

- Categorie Si possono aggiungere categorie personalizzate e modificare sia il Master Database sia le categorie personalizzate, definendo gli URL ricategorizzati e le parole chiave per l'uso all'interno del proprio ruolo, modificare l'azione e l'opzione di filtraggio avanzato applicati per predefinizione ai filtri di categoria creati. (Le modifiche apportate a un'azione predefinita di una categoria vengono implementate soltanto se la categoria non è stata bloccata dal Blocco filtro.)
- Protocolli Si possono modificare l'azione o le opzioni di filtri avanzati applicate, per predefinizione, ai filtri di protocollo che si creano. (Le modifiche apportate all'azione predefinita di un protocollo vengono implementate soltanto se il protocollo non è bloccato dal Blocco filtro.) Gli amministratori con delega non possono aggiungere o eliminare le definizioni di un protocollo.
- **Tipi di file** Si possono visualizzare le estensioni di file assegnate ad ogni tipo di file. Gli amministratori con delega non possono aggiungere tipi di file o modificare le estensioni assegnate a un tipo di file.
- URL non filtrati Si possono aggiungere gli URL e le espressioni regolari che rappresentano i siti con accesso autorizzato per tutti i client gestiti nel loro ruolo soltanto.

Per ulteriori informazioni, vedere Definizione dei Componenti filtro, pagina 178.

Se un Super Administrator ha implementato restrizioni del tipo Blocco filtro, potrebbero esserci categorie o protocolli che vengono automaticamente bloccati e che non possono venire modificati nei filtri successivamente creati e modificati. Vedere *Definizione delle restrizioni di filtraggio per tutti i ruoli*, pagina 271.

Applicazione di criteri ai client

Argomenti correlati:

- Operazioni degli amministratori con delega, pagina 251
- Visualizzazione dell'account utente, pagina 251
- Visualizzazione della definizione del proprio ruolo, pagina 252
- Aggiunta di client alla pagina Client, pagina 252
- Creazione di criteri e filtri, pagina 253

Dopo aver creato un criterio, è possibile applicare quel criterio direttamente ai client che sono stati già aggiunti alla pagina dei Client facendo clic sul pulsante **Applica ai client**. Vedere *Assegnazione dei criteri ai client*, pagina 81.

In alternativa, è possibile andare alla pagina Client e aggiungere i client a cui va applicato questo criterio. Vedere *Gestione dei client*, pagina 62.

Generazione di report

Se si possiede l'autorizzazione alla creazione dei report, le opzioni specifiche disponibili vengono definite dal Super Administrator. Per vedere le opzioni disponibili, andare alla pagina Amministrazione con delega e fare clic sul nome del ruolo. Viene visualizzata la pagina Modifica ruolo con le opzioni di creazione dei report che si è autorizzati ad usare. Per ulteriori informazioni, vedere *Modifica dei ruoli*, pagina 261.

Attivazione dell'accesso a Websense Manager

Quando si configurano i ruoli dell'amministrazione con delega, occorre determinare le funzioni di Websense Manager a cui gli amministratori possono accedere. Per essere certi che le opzioni corrette siano disponibili agli individui che accedono a Websense Manager, ciascuna persona deve accedere con un nome utente e una password specifici. Si possono usare due tipi di account:

- Account di rete usa le credenziali già definite nel servizio di directory della rete (vedere Account di directory, pagina 255).
- Account utente Websense consente di creare un nome utente e una password da usare specificatamente all'interno di Websense Manager (vedere Account utenti Websense, pagina 257).

Account di directory

Argomenti correlati:

- Attivazione dell'accesso a Websense Manager, pagina 255
- Account utenti Websense, pagina 257

Gli utenti con qualifica totale di Super Administrator possono usare la pagina Impostazioni > Generale > Directory di accesso per inserire le informazioni relative al servizio di directory necessarie che consentono agli amministratori di accedere a Websense Manager con le proprie credenziali di rete.

Nota

Queste informazioni vengono usate per l'autenticazione degli utenti di Websense Manager soltanto. Non sono applicabili al filtraggio dei client. Le informazioni relative al servizio di directory dei client vengono configurate tramite la pagina Impostazioni > Servizi di directory (vedere *Servizi di directory*, pagina 65). Le credenziali di rete degli utenti di Websense Manager devono venire autenticate in base a un unico servizio di directory. Se la rete include molteplici servizi di directory, deve esistere un rapporto "trusted" tra il servizio di directory di accesso configurato in Websense Manager e gli altri servizi.

Se non è possibile definire un singolo servizio di directory da usare con Websense Manager, considerare la possibilità di creare degli account utenti di Websense per gli amministratori (vedere *Account utenti Websense*, pagina 257).

Per definire il servizio di directory che Websense Manager deve usare per autenticare gli amministratori, verificare innanzi tutto di aver selezionato la casella di controllo relativa all'uso di un servizio di directory per l'autenticazione degli amministratori e selezionare quindi il tipo di **Servizio di directory** dall'apposito elenco.

Se si seleziona l'opzione predefinita, **NT Directory / Active Directory di Windows** (**Mixed Mode**), non sarà necessario eseguire un'altra configurazione. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Se si seleziona Active Directory (Native Mode) o Altre directory LDAP, inserire le seguenti informazioni supplementari:

1. Inserire l'indirizzo IP o il nome del computer in cui è installato il servizio di directory.

Se si sta invece usando Active Directory (Native Mode) e si sono configurati i server di catalogo globale per il failover, si può inserire il nome del dominio DNS.

- 2. Inserire la Porta usata per la comunicazione con il servizio di directory.
- 3. Per cifrare la comunicazione con il servizio directory, selezionare Utilizza SSL.
- 4. Inserire un **Nome distinto utente** e una **Password** che Websense deve usare per collegarsi al servizio di directory.
- 5. Inserire il **Contesto dominio predefinito** che il software Websense deve usare per l'autenticazione degli amministratori.
 - Se si sta usando Active Directory (Native Mode), la configurazione è completa. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.
 - Se si sta usando un altro servizio di directory LDAP, continuare.
- 6. Inserire l'**Attributo ID di accesso utente** e il **Filtro di ricerca utente**, se necessario, che il software Websense deve usare per rendere più rapida l'autenticazione dell'utente.

Queste informazioni vengono anche visualizzate nella pagina **Impostazioni** > **Servizi di directory**, nella sezione **Impostazioni directory avanzate**. È possibile copiare e incollare i valori, se necessario.

- 7. In Opzioni di gruppo, specificare se lo schema LDAP deve includere o meno l'attributo **memberOf**:
 - Se l'attributo memberOf non viene utilizzato, specificare il Filtro di ricerca gruppo utente che il software Websense deve usare per l'autenticazione degli amministratori.

- Se si usa l'attributo memberOf, specificare l'**Attributo di gruppo** da applicare.
- 8. Se lo schema LDAP usato include gruppi nidificati, selezionare **Esegui ulteriore** ricerca di gruppo nidificato.
- 9. Se il servizio di directory usa i riferimenti LDAP, indicare se il software Websense deve usare o ignorare i riferimenti.
- 10. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Account utenti Websense

Argomenti correlati:

- Attivazione dell'accesso a Websense Manager, pagina 255
- Aggiunta di un account utente di Websense, pagina 258

I Super Administrator usano la pagina **Amministrazione con delega > Gestisci account utente Websense** per creare gli account che gli amministratori devono usare per accedere a Websense Manager senza dover inserire le credenziali della directory di rete. Questa pagina consente anche ai Super Administrator di modificare la password per gli account utente di Websense e per visualizzare i ruoli ai quali l'utente di Websense viene assegnato come amministratore.

Gli utenti con qualifica totale di Super Administrator possono eliminare gli account utente da questa pagina.

Gli amministratori con delega usano questa pagina per modificare la loro password di accesso a Websense e per visualizzare i ruoli ai quali sono stati assegnati come amministratori.

Opzione	Descrizione
Aggiungi	Apre la pagina per la creazione di un nuovo account utente di Websense. Vedere <i>Aggiunta di un account utente di</i> <i>Websense</i> , pagina 258.
Modifica password	Apre la pagina per la modifica della password per l'account ad essa associato. Vedere <i>Modifica della password utente di</i> <i>Websense</i> , pagina 258.
Visualizza	Visualizza un elenco di ruoli ai quali questo utente è stato assegnato come amministratore.
Elimina	Selezionare la relativa casella di controllo per visualizzare uno o più account utente obsoleti e fare quindi clic su questo pulsante per eliminarli.
Chiudi	Ritornare alla pagina Amministrazione con delega.

Aggiunta di un account utente di Websense

Argomenti correlati:

- Attivazione dell'accesso a Websense Manager, pagina 255
- Account utenti Websense, pagina 257
- Modifica della password utente di Websense, pagina 258

Usare la pagina **Amministrazione con delega > Gestisci account utente Websense** per aggiungere gli account utente di Websense .

1. Inserire un Nome utente univoco della lunghezza massima di 50 caratteri.

Il nome deve contenere da 1 a 50 caratteri e non può includere i caratteri seguenti:

* < > ' { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

I nomi utente possono includere spazi e trattini.

- 2. Inserire e confermare una **Password** (da 4 a 255 caratteri) per questo utente. Si consiglia l'uso di password difficili da identificare: lunghezza minima di 8 caratteri che devono comprendere almeno uno dei seguenti caratteri:
 - lettera maiuscola
 - lettera minuscola
 - numero
 - carattere speciali (tra cui trattino, segno di sottolineatura o spazio)
- 3. Una volta terminate le modifiche, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Gestisci account utente Websense. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Modifica della password utente di Websense

Argomenti correlati:

- Attivazione dell'accesso a Websense Manager, pagina 255
- Account utenti Websense, pagina 257
- Aggiunta di un account utente di Websense, pagina 258

La pagina Amministrazione con delega > Gestisci account utente di Websense > Modifica password consente agli amministratori con delega di modificare la password al loro account utente di Websense. Il Super Administrator può usare questa pagina per modificare la password a un account utente qualsiasi di Websense.

- 1. Verificare che il **Nome utente** corretto sia visualizzato nell'area superiore della pagina.
- 2. Inserire e confermare la nuova **Password** (da 4 a 255 caratteri) per questo utente.

Si consiglia l'uso di password difficili da indovinare: lunghezza minima di 8 caratteri che devono comprendere almeno uno dei seguenti caratteri:

- lettera maiuscola
- lettera minuscola
- numero
- carattere speciali (tra cui trattino, segno di sottolineatura o spazio)
- 3. Una volta terminate le modifiche, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Gestisci account utente Websense. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Uso dell'amministrazione con delega

Argomenti correlati:

- Introduzione ai ruoli amministrativi, pagina 242
- Gestione dei conflitti di ruolo, pagina 268

La pagina **Gestione criteri > Amministrazione con delega** offre diverse opzioni a seconda che venga visualizzata da un Super Administrator o da un amministratore con delega.

I Super Administrator possono visualizzare un elenco di tutti i ruoli correntemente definiti e dispongono delle opzioni descritte qui di seguito.

Opzione	Descrizione
Aggiungi	Fare clic su questa opzione per aggiungere un nuovo ruolo. Vedere <i>Aggiunta di ruoli</i> , pagina 260.
Ruolo	Fare clic su questa opzione per visualizzare o configurare il ruolo. Vedere <i>Modifica dei ruoli</i> , pagina 261.
Elimina	Fare clic su questa opzione per eliminare i ruoli selezionati nell'elenco. Questa opzione è disponibile soltanto per gli utenti con qualifica totale di Super Administrator.
	Vedere la sezione <i>Considerazioni speciali</i> , pagina 268 per informazioni su come i client di un ruolo vengono gestiti dopo l'eliminazione del ruolo.
Avanzate	Fare clic su questa opzione per accedere alla funzione Gestisci priorità di ruolo.
Gestisci priorità di ruolo	Fare clic su questa opzione per specificare le impostazioni di criterio del ruolo che vengono usate se lo stesso client esiste in molteplici gruppi gestiti da diversi ruoli. Vedere <i>Gestione dei conflitti di ruolo</i> , pagina 268.

Opzione	Descrizione
Gestisci account utente Websense	Fare clic su aggiungi, modifica e elimina i nomi utente e le password per gli account usati soltanto per accedere a Websense Manager. Vedere <i>Account utenti Websense</i> , pagina 257.
Gestisci gruppi LDAP personalizzati	Fare clic su aggiungi, modifica e elimina i gruppi LDAP personalizzati che possono venire assegnati come client gestiti ai ruoli di amministrazione con delega. Vedere <i>Gestione di gruppi LDAP personalizzati</i> , pagina 68. Questa opzione non è disponibile se il servizio di directory configurato è Windows NT/Active Directory (Mixed Mode).

Gli amministratori con delega visualizzano soltanto i ruoli ai quali sono stati designati come amministratori ed hanno anche accesso ad altre opzioni limitate.

Opzione	Descrizione
Ruolo	Fare clic su questa opzione per visualizzare i client assegnati al ruolo e le specifiche autorizzazioni di creazione dei report concesse. Vedere <i>Modifica dei ruoli</i> , pagina 261.
Gestisci account utente Websense	Fare clic su questa opzione per accedere alle opzioni che consentono di modificare la propria password a Websense Manager e per visualizzare i ruoli a cui si è stati assegnati. Vedere <i>Account utenti Websense</i> , pagina 257.

Aggiunta di ruoli

Argomenti correlati:

- Modifica dei ruoli, pagina 261
- Considerazioni speciali, pagina 268

Usare la pagina > Amministrazione con delega > Aggiungi ruolo per assegnare un nome e una descrizione al nuovo ruolo.

1. Inserire un Nome per il nuovo ruolo.

Il nome deve contenere da 1 a 50 caratteri e non può includere i caratteri seguenti:

* < > ' { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,

I nomi dei ruoli possono includere spazi e trattini.

2. Inserire una **Descrizione** per il nuovo ruolo.

La descrizione può contenere fino a un massimo di 255 caratteri. Le restrizioni relative ai caratteri usati per i nomi dei ruoli sono anche applicabile alle descrizioni, con due eccezioni: le descrizioni possono includere punti (.) e virgole (,).

3. Fare clic su **OK** per visualizzare la pagina **Modifica ruolo** e definire le caratteristiche di questo ruolo.. Vedere *Modifica dei ruoli*, pagina 261.

Il nuovo ruolo viene aggiunto all'elenco a discesa Ruolo, nell'intestazione, la volta successiva che ci si collega a Websense Manager.

Modifica dei ruoli

Argomenti correlati:

- Uso dell'amministrazione con delega, pagina 259
- Aggiunta di ruoli, pagina 260
- Gestione dei conflitti di ruolo, pagina 268

Gli amministratori con delega possono usare la pagina **Amministrazione con delega > Modifica ruolo** per visualizzare l'elenco dei client gestiti in base al ruolo a loro assegnato e le specifiche autorizzazioni di creazione di report concesse.

I Super Administrator possono usare questa pagina per selezionare gli amministratori e i client da assegnare a un ruolo e per definire le autorizzazioni per gli amministratori, come descritto di seguito. Soltanto gli utenti con qualifica totale di Super Administrator possono eliminare amministratori e client da un ruolo.

1. Modificare il ruolo Nome e Descrizione, come necessario.



2. Aggiungere ed eliminare gli amministratori per questo ruolo. (Questa sezione, disponibile soltanto ai Super Administrator, viene visualizzata se ci si collega come amministratore con delega.)

Opzione	Descrizione
Nome utente	Il nome utente dell'amministratore.
Tipo account	Indica se l'utente è stato definito nel servizio di directory della rete (Directory) o come account utente di Websense (Websense).
Creazione report	Selezionare questa casella di controllo per concedere all'amministratore i permessi relativi all'uso degli strumenti di creazione dei report.
Criterio	Selezionare questa casella di controllo per concedere all'amministratore l'autorizzazione a creare filtri e criteri e per assegnare i criteri necessari ai client gestiti dal ruolo. Nel ruolo di Super Administrator, gli amministratori con autorizzazione alla gestione dei criteri possono gestire anche determinate impostazioni di configurazione Websense. Vedere <i>Super Administrator</i> , pagina 243.

Opzione	Descrizione
Totale	Selezionare questa casella di controllo, disponibile soltanto per il ruolo di Super Administrator, per concedere all'amministratore l'autorizzazione a gestire tutte le impostazioni di configurazione di Websense, oltre alla funzione Blocco filtro. Soltanto gli utenti con qualifica totale di Super Administrator possono concedere autorizzazioni totali a un nuovo amministratore.
Aggiungi	Apre la pagina Aggiungi amministratore . Vedere <i>Aggiunta di amministratori</i> , pagina 264.
Elimina	Elimina dal ruolo gli amministratori selezionati nell'elenco Amministratori. (Disponibile soltanto per l'utente con qualifica totale di Super Administrator.)

3. Aggiungere ed eliminare i **Client gestiti** per quel ruolo. (Disponibile soltanto per i Super Administrator. Gli amministratori con delega possono visualizzare i client assegnati al loro ruolo.)

Opzione	Descrizione
<nome></nome>	Visualizza il nome di ciascun client esplicitamente assegnato al ruolo. Gli amministratori in quel ruolo devono aggiungere i client alla pagina Client prima che i criteri possano venire applicati. Vedere <i>Operazioni degli amministratori con</i> <i>delega</i> , pagina 251.
Aggiungi	Apre la pagina Aggiungi client gestiti . Vedere <i>Aggiunta di client gestiti</i> , pagina 266.
Elimina	Questo pulsante, disponibile soltanto per gli utenti con qualifica totale di Super Administrator, elimina da ciascun ruolo i client selezionati nell'elenco dei client gestiti.
	Alcuni client non possono venire eliminati direttamente dall'elenco dei client gestiti. Per ulteriori informazioni, vedere <i>Considerazioni speciali</i> , pagina 268.

4. Usare l'area **Autorizzazioni creazione report** per selezionare le funzioni disponibili per gli amministratori assegnati a questo ruolo e che possiedono l'accesso alle funzioni di creazione report.

Opzione	Descrizione
Crea report su tutti i client	Selezionare questa opzione per concedere agli amministratori l'autorizzazione necessaria a generare report su tutti gli utenti di rete.
	Usare le opzioni rimanenti dell'area Autorizzazioni creazione report per definire le autorizzazioni specifiche da concedere agli amministratori assegnati a questo ruolo.
Crea report solo sui client gestiti	Selezionare questa opzione per limitare gli amministratori ad una funzione di creazione dei report soltanto in relazione ai client gestiti assegnati a questo ruolo. Selezionare quindi le opzioni relative alla creazione dei report investigativi a cui questi amministratori possono accedere.
	Gli amministratori limitati alla creazione dei report relativi ai client gestiti non possono accedere ai report di presentazione o ai report sugli utenti delle pagine Oggi e Cronologia. Viene anche loro impedito di gestire le impostazioni del database di registrazione.

a. Scegliere il livello generale di autorizzazione alla creazione di report :

b. Selezionare la casella di controllo per ciascuna opzione di creazione dei report che gli amministratori assegnati al ruolo sono autorizzati ad usare.

Opzione	Descrizione
Accedi report di presentazione	Consente di accedere alle opzioni relative ai report di presentazione. Questa opzione è disponibile soltanto se gli amministratori sono autorizzati a creare report su tutti gli utenti. Vedere <i>Report di</i> <i>presentazione</i> , pagina 100.
Visualizza report nelle pagine Oggi e Cronologia	Consente di visualizzare in queste pagine i grafici che illustrano l'attività svolta in Internet. Vedere <i>Oggi: integrità, sicurezza e risultati a partire dalla</i> <i>mezzanotte</i> , pagina 22 e <i>Cronologia: ultimi 30</i> <i>giorni</i> , pagina 25.
	Se questa opzione non è selezionata, gli amministratori possono visualizzare soltanto le aree Avvisi di integrità e Valore della pagina Oggi e Stime dei risultati della pagina Cronologia.
Accedi report investigativi	Consente di accedere alle opzioni di base dei report investigativi. Se questa opzione è selezionata, è possibile selezionare anche altre opzioni relative ai report investigativi. Vedere <i>Report investigativi</i> , pagina 119.

Opzione	Descrizione
Visualizza nomi utente in report investigativi	Consente agli amministratori in questo ruolo di visualizzare i nomi utente, se registrati. Vedere <i>Configurazione di Filtering Service per la</i> <i>registrazione</i> , pagina 314.
	Deselezionare questa opzione per visualizzare soltanto i codici di identificazione generati dal sistema anziché i nomi.
	Questa opzione è disponibile soltanto se gli amministratori sono autorizzati ad accedere ai report investigativi.
Salva report investigativi come preferiti	Consente agli amministratori in questo ruolo di creare report investigativi preferiti. Vedere <i>Report investigativi preferiti</i> , pagina 138.
	Questa opzione è disponibile soltanto se gli amministratori sono autorizzati ad accedere ai report investigativi.
Pianifica report investigativi	Consente agli amministratori in questo ruolo di pianificare la creazione dei report investigativi in base a tempi futuri specifici o in un ciclo ripetitivo.
	Vedere <i>Pianificazione dei report investigativi</i> , pagina 141.
	Questa opzione è disponibile soltanto se gli amministratori sono autorizzati a salvare i report investigativi come preferiti.
Gestisci database di registrazione	Consente agli amministratori di accedere alla pagina Impostazioni >Database di registrazione. Vedere Impostazioni dell'amministrazione del database di registrazione, pagina 330.
	Questa opzione è disponibile soltanto se gli amministratori sono autorizzati a creare report su tutti i client.

5. Una volta terminate le modifiche, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Amministrazione con delega. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta di amministratori

Argomenti correlati:

- Modifica dei ruoli, pagina 261
- Attivazione dell'accesso a Websense Manager, pagina 255

I Super Administrator possono usare la pagina Amministrazione con delega > Modifica ruolo > Aggiungi amministratori per specificare gli individui designati come amministratori per un determinato ruolo.



Gli amministratori possono venire aggiunti a molteplici ruoli. Questi amministratori devono scegliere un ruolo in fase di accesso al software. In questo caso, l'amministratore riceve le autorizzazioni combinate di creazione dei report per tutti i ruoli.

Gli amministratori con delega mantengono un controllo significativo sulle attività svolte in Internet dai client da loro gestiti. Per garantire che questo controllo venga gestito responsabilmente e in conformità con i criteri stabiliti dalla propria organizzazione, il Super Administrator può usare la pagina Registro di controllo per monitorare le modifiche apportate dagli amministratori. Vedere *Visualizzazione ed esportazione del registro di controllo*, pagina 289.

 Se si prevede di aggiungere degli account di directory come amministratori con delega, accertarsi di essere collegati al Policy Server la cui configurazione di servizio di directory (vedere *Servizi di directory*, pagina 65) corrisponde alla configurazione della directory di accesso (vedere *Account di directory*, pagina 255).

Se si aggiungono soltanto degli account utente di Websense come amministratori, è possibile collegarsi a qualsiasi Policy Server.

2. Nell'area Account di directory, selezionare la casella di controllo adiacente ad uno o più utenti e fare quindi clic sul pulsante con freccia rivolta verso destra (>) per spostare gli utenti nell'elenco Selezionati.



Se il proprio ambiente informatico usa Active Directory (Native Mode) o un altro servizio di directory basato su LDAP, è possibile condurre una ricerca nella directory per trovare il nome specifico di un utente, un gruppo, un dominio o un'unità organizzativa. Vedere *Ricerca nel service di directory*, pagina 71.

3. Nell'area Account utente Websense, selezionare la casella di controllo adiacente ad uno o più utenti e fare quindi clic sul pulsante con freccia rivolta verso destra per spostare gli utenti evidenziati nell'elenco Selezionati.

Opzione	Descrizione
Criterio	Selezionare questa opzione per consentire agli amministratori in questo ruolo di applicare i criteri ai loro client gestiti. Questo consente anche l'accesso a determinate impostazioni di configurazione di Websense.
Totale	Selezionare questa opzione per concedere l'accesso a tutte le impostazioni di configurazione di Websense.
	Questa opzione è disponibile soltanto se un utente con qualifica totale di Super Administrator aggiunge degli amministratori al ruolo di Super Administrator, con l'autorizzazione alla gestione dei criteri.
Creazione report	Selezionare questa opzione per concedere l'accesso a tutti gli strumenti di creazione dei report. Usare la pagina Modifica ruolo per impostare le opzioni di autorizzazione alla creazione dei report.

4. Definire le Autorizzazioni per gli amministratori in questo ruolo.

- 5. Una volta terminate le modifiche, fare clic su **OK** per ritornare alla pagina Modifica ruolo.
- Fare clic su OK nella pagina Modifica ruolo per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su Salva tutto.

Aggiunta di client gestiti

Argomenti correlati:

- Uso dell'amministrazione con delega, pagina 259
- Modifica dei ruoli, pagina 261

I client gestiti sono gli utenti e i computer assegnati a un determinato ruolo i cui criteri vengono definiti dagli amministratori assegnati a quel ruolo. I client della directory (utenti, gruppi, domini e unità organizzative), computer e reti possono venire tutti definiti come client gestiti.

I Super Administrator possono usare la pagina **Amministrazione con delega** > **Modifica ruolo** > **Aggiungi clienti gestiti** per aggiungere il numero desiderato di client a un ruolo, come necessario. Ciascun client può essere assegnato ad un solo ruolo.

Se si assegna un intervallo di rete come client gestito a un ruolo, non è possibile assegnare i singoli indirizzi IP, inclusi in quell'intervallo, a un altro ruolo. Non è inoltre possibile assegnare specificatamente un utente, un gruppo, un dominio o un'unità organizzativa a 2 ruoli diversi. È tuttavia possibile assegnare un utente a un ruolo e quindi assegnare un gruppo, un dominio o un'unità organizzativa di cui l'utente è membro, a un ruolo diverso.



Quando si aggiungono dei client gestiti, valutare i tipi di client che si vuole includere. Se si aggiungono indirizzi IP a un ruolo, gli amministratori assegnati a quel ruolo possono generare report su **tutte** le attività svolte da specifici computer. Se si aggiungono degli utenti a un ruolo, gli amministratori possono generare dei report su tutte le attività svolte da quegli utenti, indipendentemente dal computer da cui erano state svolte.

Gli amministratori non vengono inclusi automaticamente come client gestiti nei ruoli che amministrano, in quanto ciò consentirebbe loro di definire i criteri a loro applicati. Per consentire agli amministratori di visualizzare il loro uso di Internet, attivare la funzione Attività utente (vedere *Attività utente*, pagina 346).

Se l'organizzazione ha implementato molteplici Policy Server e i Policy Server comunicano con diverse directory, accertarsi di selezionare il Policy Server collegato alla directory contenente i client da aggiungere.

Nota

Le migliori pratiche indicano che tutti i client gestiti nello stesso ruolo dovrebbero far parte dello stesso servizio di directory.

- 1. Selezionare i client da includere nel ruolo:
 - In Directory, selezionare le caselle di controllo di uno o più utenti.

Se il proprio ambiente usa Active Directory (Native Mode) o un altro servizio di directory basato su LDAP, è possibile condurre una ricerca nella directory per trovare il nome specifico di un utente, un gruppo, un dominio o un'unità organizzativa. Vedere *Ricerca nel service di directory*, pagina 71.

- In **Computer** inserire l'indirizzo IP di un computer da aggiungere a questo ruolo.
- In Rete, inserire il primo e l'ultimo indirizzo IP di un gruppo di computer da aggiungere come un'unità singola.
- 2. Fare clic sul pulsante freccia verso destra (>), adiacente al tipo di client, per spostare i client nell'elenco **Selezionati**.
- 3. Una volta terminate le modifiche, fare clic su **OK** per ritornare alla pagina Modifica ruolo.
- Fare clic su OK nella pagina Modifica ruolo per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su Salva tutto.

Gestione dei conflitti di ruolo

Argomenti correlati:

- Uso dell'amministrazione con delega, pagina 259
- Aggiunta di client gestiti, pagina 266

I servizi di directory consentono allo stesso utente di appartenere a molteplici gruppi. Ne risulta che un singolo utente può esistere in gruppi gestiti da diversi ruoli di amministrazione con delega. La stessa situazione è applicabile ai domini e alle unità organizzative.

È inoltre possibile che un utente venga gestito da un certo ruolo sebbene appartenga a un determinato gruppo, dominio o unità organizzativa gestiti da un ruolo diverso. Se gli amministratori di entrambi questi ruoli si collegano al sistema simultaneamente, potrebbe accadere che l'amministratore responsabile per l'utente applichi un criterio a quell'utente nello stesso tempo in cui l'amministratore responsabile per il gruppo applichi un criterio ai singoli membri del gruppo.

Usare la pagina **Amministrazione con delega > Gestisci priorità di ruolo** per indicare al software Websense quello che occorre fare se diversi criteri vengono applicati allo stesso utente a causa di una sovrapposizione di ruoli. Se si verifica un conflitto, il software Websense applica i criteri di filtro del ruolo che appare in testa all'elenco.

1. Selezionare un ruolo dall'elenco, ad eccezione del ruolo di Super Administrator.



Il ruolo di Super Administrator è sempre in testa all'elenco e non può essere spostato.

- 2. Fare clic su Sposta su o Sposta giù per cambiare la sua posizione nell'elenco.
- 3. Ripetere le operazioni descritte ai punti 1 e 2 fino a quando tutti i ruoli non stati priorizzati correttamente.
- 4. Una volta terminate le modifiche, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Amministrazione con delega. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Considerazioni speciali

Argomenti correlati:

- Uso dell'amministrazione con delega, pagina 259
- *Modifica dei ruoli*, pagina 261

Riesaminare le informazioni seguenti prima di eliminare i ruoli dell'amministrazione con delega o eliminare dei client gestiti da un ruolo.

Eliminazione dei ruoli

Nella pagina **Amministrazione con delega**, gli utenti con qualifica totale di Super Administrator possono eliminare i ruoli determinati come obsoleti.

L'eliminazione di un ruolo elimina anche tutti i client che gli amministratori assegnati a quel ruolo avevano aggiunto alla pagina Client. Una volta eliminato il ruolo, se quei client appartengono a reti, gruppi o domini gestiti da altri ruoli, verranno assoggettati ai criteri applicati da quei ruoli (vedere *Ordine di filtraggio*, pagina 82). In caso contrario, saranno soggetti ai criteri predefiniti di Super Administrator.

1. Nella pagina **Amministrazione con delega**, selezionare la casella di controllo adiacente a ciascun ruolo da eliminare.



Non è consentito eliminare il ruolo di Super Administrator.

- 2. Fare clic su Elimina.
- 3. Confermare la richiesta di rimozione dei ruoli selezionati dalla pagina di Amministrazione con delega. Le modifiche non sono permanenti fino a quando non si fa clic su **Salva tutto**.

Il ruolo eliminato apparirà cancellato dall'elenco a discesa Ruolo, nell'intestazione, la prossima volta che ci si collega a Websense Manager.

Eliminazione client gestiti

I client non possono venire eliminati direttamente dall'elenco dei client gestiti (Amministrazione con delega > Modifica ruolo) se:

- l'amministratore ha applicato un criterio al client
- l'amministratore ha applicato un criterio a uno o più membri di una rete, di un gruppo, di un dominio o di un'unità organizzativa

Potrebbero anche insorgere problemi se, durante il collegamento con Websense Manager, il Super Administrator sceglie un Policy Server diverso da quello che comunica con il servizio di directory contenente i client da eliminare. In questo caso, il Policy Server e il servizio di directory non riconoscono i client.

Un utente con qualifica totale di Super Administrator può accertare che i client corretti vengano eliminati, procedendo come segue:

- 1. Collegarsi a Websense Manager selezionando il Policy Server il cui servizio di directory contiene i client gestiti da eliminare. Occorre collegarsi con l'autorizzazione di utente con qualifica totale di Super Administrator.
- 2. Aprire l'elenco **Ruolo** nell'intestazione, e selezionare il ruolo dal quale si vogliono eliminare i client gestiti.
- 3. Andare a **Gestione criteri** > **Client** per visualizzare un elenco di tutti i client ai quali l'amministratore con delega ha esplicitamente assegnato un criterio.

Questo potrebbe includere sia i client specificatamente identificati nell'elenco dei client gestiti del ruolo, sia i client membri di reti, gruppi, domini o unità organizzative inclusi nell'elenco dei client gestiti.

- 4. Eliminare i client appropriati.
- 5. Fare clic su **OK** per inserire le modifiche nella cache.
- 6. Aprire l'elenco **Ruolo** nell'intestazione e selezionare il ruolo di **Super Administrator**.
- 7. Andare a Gestione criteri > Amministrazione con delega >Modifica ruolo.
- 8. Eliminare i client appropriati dall'elenco di client gestiti e fare quindi clic su **OK** per confermare la richiesta di eliminazione.
- 9. Fare clic su **OK** nella pagina Modifica ruolo per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Molteplici amministratori in accesso a Websense Manager

Argomenti correlati:

- Introduzione alle funzioni di amministratore, pagina 243
- Attivazione dell'accesso a Websense Manager, pagina 255

Gli amministratori con diversi ruoli possono accedere simultaneamente a Websense Manager per eseguire le attività autorizzate in base al loro ruolo. Ad esempio, gli amministratori con Ruolo A e con Ruolo B, che possiedono l'autorizzazione alla gestione dei criteri, possono collegarsi simultaneamente a Websense Manager. Poiché gestiscono diversi client, possono creare ed applicare criteri senza generare per questo dei conflitti.

La situazione è diversa se gli amministratori autorizzati alla gestione dei criteri in base a uno stesso ruolo accedono simultaneamente a Websense Manager. Per preservare l'integrità della struttura dei criteri e della loro assegnazione, soltanto un amministratore che condivide lo stesso ruolo con altri amministratori può accedere a Websense Manager con autorizzazione alla gestione dei criteri. Se un secondo amministratore con autorizzazione alla gestione dei criteri in base allo stesso ruolo di altri tenta di collegarsi mentre il primo amministratore è ancora collegato, potrà scegliere di:

- collegarsi soltanto per la creazione dei report, se ne possiede la necessaria autorizzazione.
- collegarsi ad un ruolo diverso se è stato assegnato anche a un altro ruolo.
- riprovare più tardi, dopo che il primo amministratore si è scollegato.

Se gli amministratori con autorizzazione sia alla creazione di report che alla gestione dei criteri si collegano per generare dei report, dovranno immediatamente rinunciare alla propria autorizzazione di gestione dei criteri in modo che altri amministratori con quel ruolo possano svolgere questa attività.

 Aprire l'elenco a discesa Ruolo nell'intestazione e selezionare Rilascio autorizzazione criterio.

In alternativa, è possibile creare un account utente speciale di Websense (vedere *Account utenti Websense*, pagina 257) per ciascun ruolo, e concedere all'utente soltanto l'autorizzazione alla creazione dei report. Occorre fornire tali credenziali di accesso (nome utente e password) agli amministratori con quel ruolo, che possiedono l'autorizzazione sia alla gestione dei criteri che alla creazione dei report. Se gli amministratori hanno bisogno di generare dei report, possono collegarsi come amministratore autorizzato alla creazione dei report, lasciando aperto ad un altro amministratore l'accesso ai criteri .

Definizione delle restrizioni di filtraggio per tutti i ruoli

Argomenti correlati:

- Introduzione alle funzioni di amministratore, pagina 243
- Creazione di un Blocco filtro, pagina 272

Il software Websense consente agli utenti con qualifica totale di Super Administrator di stabilire un Blocco filtro che blocchi categorie e protocolli per tutti i client gestiti dai ruoli di amministrazione con delega. Per ulteriori informazioni, vedere *Creazione di un Blocco filtro*, pagina 272.

Gli amministratori di questi ruoli possono applicare l'azione di filtro ad altre categorie e ad altri protocolli associati ai loro criteri, ma non alle categorie e ai protocolli bloccati dal Blocco filtro.

Le modifiche apportate al Blocco filtro vengono implementate per tutti i client gestiti non appena le modifiche vengono salvate. Gli amministratori con delega che stanno lavorando in Websense Manager quando le modifiche entrano in effetto, non vedranno le modifiche applicate ai filtri fino al loro prossimo collegamento.



Se un filtro viene copiato da un ruolo di Super Administrator a un altro ruolo, alla copia vengono applicate le restrizioni definite dal Blocco filtro.

I Super Administrator non vengono limitati dal Blocco filtro. I Super Administrator possono definire i criteri che consentono l'accesso alle categorie e ai protocolli bloccati per i ruoli di amministrazione con delega. Di conseguenza gli individui che

necessitano di diritti di accesso speciali devono venire gestiti dal ruolo di Super Administrator.

Creazione di un Blocco filtro

Argomenti correlati:

- Definizione delle restrizioni di filtraggio per tutti i ruoli, pagina 271
- *Blocco delle categorie*, pagina 272
- Blocco dei protocolli, pagina 273

La pagina **Gestione criteri > Blocco filtro** consente di scegliere se fissare il blocco delle categorie o dei protocolli per tutti i client gestiti dai ruoli di amministrazione con delega. Le opzioni relative alle categorie o ai protocolli che sono stati bloccati dal Blocco filtro, vengono considerate **bloccate**.

- Fare clic sul pulsante **Categorie** per bloccare specifiche categorie o specifici elementi delle categorie (parole chiave e tipi di file). Vedere *Blocco delle categorie*, pagina 272.
- Fare clic sul pulsante Protocolli per bloccare dei protocolli o per bloccare l'accesso ai protocolli. Vedere *Blocco dei protocolli*, pagina 273.

Blocco delle categorie

Argomenti correlati:

- Definizione delle restrizioni di filtraggio per tutti i ruoli, pagina 271
- Creazione di un Blocco filtro, pagina 272
- *Blocco dei protocolli*, pagina 273

Usare la pagina **Gestione criteri > Blocco filtro > Categorie** per selezionare le categorie che si vogliono bloccare per tutti i membri dei ruoli di amministrazione con delega. È anche possibile bloccare le parole chiave e i tipi di file associati ad una data categoria.

1. Selezionare una categoria dall'apposito albero.

I ruoli di amministrazione con delega non hanno accesso alle categorie personalizzate create dai Super Administrator. Di conseguenza le categorie personalizzate non sono incluse in questo albero. 2. Definire le restrizioni da applicare a questa categoria nell'area disponibile accanto all'albero delle categorie.

Opzione	Descrizione
Blocca categoria	Blocca l'accesso a tutti i siti che fanno parte di questa categoria.
Blocca parole chiave	Blocca l'accesso in base alle parole chiave definite per questa categoria in ciascun ruolo.
Blocca tipi file	Blocca i tipi di file selezionati per i siti associati a questa categoria.
	Contrassegnare la casella di controllo per ciascun tipo di file da bloccare.
	I tipi di file creati dal Super Administrator sono inclusi in questo elenco in quanto sono disponibili per i ruoli di amministrazione con delega.
Applica a sottocategorie	Applica le stesse impostazioni alle sottocategorie di questa categoria.

È possibile bloccare simultaneamente gli elementi selezionati per tutte le categorie, se necessario. Selezionare **Tutte le categorie** incluse nell'albero e selezionare quindi gli elementi da bloccare per tutte le categorie. Fare clic su **Applica alle sottocatgorie**.

3. Una volta terminate le modifiche, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Blocca filtro. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Blocco dei protocolli

Argomenti correlati:

- Definizione delle restrizioni di filtraggio per tutti i ruoli, pagina 271
- Creazione di un Blocco filtro, pagina 272
- *Blocco delle categorie*, pagina 272

Usare la pagina **Gestione criteri > Blocco filtro > Protocolli** per bloccare l'accesso o la registrazione dei protocolli selezionati per tutti i client gestiti dai ruoli di amministrazione con delega.



Nota

La registrazione del Protocollo è associata alle avvertenze relative all'uso del protocollo. Non è possibile generare avvertenze sull'uso di un protocollo a meno che la sua registrazione non sia stata definita almeno in un filtro di protocollo. L'attivazione dell'opzione **Blocca registrazione protocollo** tramite Blocco filtro garantisce che le avvertenze sull'uso possano venire generate per quel protocollo. Vedere *Configurazione degli avvisi di utilizzo di un protocollo*, pagina 297.

1. Selezionare un protocollo dall'apposito albero.

I ruoli di amministrazione con delega non hanno accesso ai protocolli personalizzati creati dal Super Administrator. Di conseguenza i protocolli personalizzati non vengono inclusi in questo albero.

2. Definire le restrizioni da applicare a questa categoria nell'area disponibile accanto all'albero delle categorie.

Opzione	Descrizione
Blocca protocollo	Blocca l'accesso alle applicazioni e ai siti Web che usano questo protocollo.
Blocca registrazione protocollo	Registra le informazioni relative all'accesso a questo protocollo e impedisce agli amministratori con delega di disattivare la registrazione.
Applica a gruppo	Applica le stesse impostazioni a tutti i protocolli del gruppo.

3. Una volta terminate le modifiche, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Blocca filtro. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

12 Amministrazione del server Websense

Argomenti correlati:

- Componenti dei prodotti Websense, pagina 276
- *Gestione di Policy Server*, pagina 282
- Visualizzazione ed esportazione del registro di controllo, pagina 289
- Chiusura e riavvio dei servizi di Websense, pagina 290
- Avvisi su schermo, pagina 292
- Esecuzione di backup e ripristino dei dati Websense, pagina 300

Le funzioni di filtraggio dell'uso di Internet richiedono un'interazione tra vari componenti software di Websense.

- Le richieste di accesso a Internet da parte degli utenti vengono ricevute da Network Agent o da un prodotto di integrazione sviluppato da terzi.
- Le richieste vengono inviate a Websense Filtering Service per l'elaborazione.
- Filtering Service comunica con Policy Server e Policy Broker per l'applicazione dei criteri appropriati in risposta alla richiesta.

Nella maggior parte degli ambienti informatici, un unico Policy Database include client, filtri, criteri e informazioni di configurazione generale, sia che si tratti di un solo Policy Server o di molteplici Policy Server.

Ciascuna istanza di Websense Manager è associata ad un unico Policy Database e può essere utilizzata per configurare ciascun Policy Server associato a quel database.

Poiché la configurazione dei criteri eseguita in Websense Manager è archiviata nel database centrale, le informazioni sui criteri diventano automaticamente disponibili a tutti i Policy Server associati a quel Policy Database.

Componenti dei prodotti Websense

Argomenti correlati:

- Componenti per il filtraggio, pagina 277
- Componenti dei report, pagina 280
- Componenti dell'identificazione utenti, pagina 281
- *Gestione di Policy Server*, pagina 282
- Chiusura e riavvio dei servizi di Websense, pagina 290
- Revisione dello stato del sistema in uso, pagina 299

Il software Websense comprende vari componenti integrati che offrono funzioni di identificazione utente, di filtraggio dell'accesso a Internet e di creazione dei report. Questa sezione offre una descrizione generale di ciascun componente al fine di facilitare la comprensione e la gestione dell'ambiente dei filtri.

I componenti Websense primari includono:

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- Master Database
- Websense Manager
- Usage Monitor
- User Service
- Log Server
- Database di registrazione

Il software Websense include inoltre degli agenti di identificazione trasparente, facoltativi.

- DC Agent
- RADIUS Agent
- eDirectory Agent
- Logon Agent

Altri componenti facoltativi includono:

- Remote Filtering Server
- Remote Filtering Client
- Websense Content Gateway

Componenti per il filtraggio

Componente	Descrizione
Policy Database	Memorizza le impostazioni del software Websense e le informazioni sui criteri.
Policy Broker	Gestisce le richieste inviate dai componenti Websense per informazioni sui criteri e sulla configurazione in generale.
Policy Server	 Identifica e monitora il percorso e lo stato di altri componenti Websense. Archivia informazioni di configurazione specifiche di un'istanza di Policy Server. Comunica dati di configurazione a Filtering Service da utilizzare nei filtri applicati alle richieste di accesso a Internet. Configura le impostazioni di Policy Server in Websense Manager (vedere <i>Gestione di Policy Server</i>, pagina 282). I criteri e la maggior parte delle impostazioni di configurazione vengono condivise tra i Policy Server che
	usano lo stesso Policy Database (vedere Ambiente con molteplici Policy Server, pagina 284).
Filtering Service	 Svolge funzioni di filtraggio applicati agli accessi a Internet insieme a Network Agent o a un prodotto di integrazione sviluppato da terzi. Quando un utente richiede l'accesso a un sito, Filtering Service riceve la richiesta e determina i criteri da applicare. Filtering Service deve essere in esecuzione affinché le
	richieste di accesso a Internet vengano filtrate e registrate.
	Ciascuna istanza di Filtering Service scarica la propria copia del Master Database di Websense.
	Il comportamento dei filtri e di Filtering Service vanno configurati in Websense Manager (vedere <i>Filtri per l'uso di</i> <i>Internet</i> , pagina 37 e <i>Configurazione delle impostazioni di</i> <i>filtraggio di Websense</i> , pagina 57).
Network Agent	Potenzia le funzioni di filtro e di registrazione
	Consente la gestione dei protocolli
	Consente l'azione di filtraggio in un ambiente stand- alone
	Per ulteriori informazioni, vedere <i>Configurazione della rete</i> , pagina 349.

Componente	Descrizione
Master Database	• Include oltre 36 milioni di siti Web, suddivisi in più di 90 categorie e sottocategorie.
	Contiene più di 100 definizioni di protocollo da usare nei filtri applicati ai protocolli.
	Scaricare Websense Master Database per attivare i filtri di accesso ad Internet ed accertarsi che il database sia sempre mantenuto aggiornato. Se il Master Database non è stato aggiornato da oltre 2 settimane, non verrà svolta alcune attività di filtraggio. Per ulteriori informazioni, vedere <i>Websense Master Database</i> , pagina 32.
Websense Manager	Funge da interfaccia con il software Websense per le funzioni di configurazione e di gestione.
	Usa Websense Manager per definire e personalizzare i criteri di accesso a Internet, per aggiungere o eliminare i filtri applicati ai client, per configurare i componenti del software Websense ed altro ancora.
	Per ulteriori informazioni, vedere Utilizzo di Websense Manager, pagina 17.
Usage Monitor	Consente la visualizzazione di avvisi relativi all'uso di Internet.
	Usage Monitor rileva gli accessi alle categorie e ai protocolli degli URL e genera avvisi in base alla configurazione definita.
	Per ulteriori informazioni, vedere <i>Avvisi su schermo</i> , pagina 292.
Remote Filtering Client	 Risiede nei computer client al di fuori del firewall di rete. Identifica i computer come client da filtrare e comunica con Remote Filtering Server.
	Per ulteriori informazioni, vedere <i>Filtro per i client remoti</i> , pagina 161.
Remote Filtering Server	• Consente l'applicazione di filtri ai client al di fuori del firewall di rete.
	Comunica con Filtering Service per la gestione degli accessi a Internet da parte di computer remoti.
	Per ulteriori informazioni, vedere <i>Filtro per i client remoti</i> , pagina 161.

Componente	Descrizione
Websense Content Gateway	Offre una piattaforma robusta relativamente ai server proxy e alla cache.
	• Può analizzare in tempo reale il contenuto dei siti e dei file disponibili nei siti Web al fine di categorizzare i siti non categorizzati in precedenza.
	Vedere Analisi del contenuto con le opzioni di Tempo reale, pagina 149.
Websense Content Gateway	Oltre a svolgere la funzione standard di Websense Content Gateway:
	 Analizza il codice HTML per rilevare la presenza di minacce alla sicurezza (ad esempio, phishing [falsificazione di pagine Web], ridirezionamento dell'URL, minacce Web e proxy avoidance [elusione via Proxy])
	• Ispeziona il contenuto dei file per assegnare una categoria di minaccia (ad esempio, virus, cavallo di Troia o worm).
	Elimina contenuti attivi dalle pagine Web.
	Vedere Analisi del contenuto con le opzioni di Tempo reale, pagina 149.

Componenti dei report

Componente	Descrizione
Log Server	Registra i dati relativi alle richieste di accesso a Internet, tra cui:
	L'origine della richiesta
	La categoria o il protocollo associati alla richiesta
	Se la richiesta è stata autorizzata o bloccata
	• Se il blocco in base alle parole chiave, il blocco in base ai tipi di file, le assegnazioni di tempo, i livelli della larghezza di banda o la protezione della password sono stati applicati.
	Con Network Agent e alcuni prodotti di integrazione, Log Server archivia anche le informazioni relative all'uso della larghezza di banda.
	Log Server deve venire installato in un computer dotato del sistema operativo Windows per consentire la creazione di report investigativi e di presentazione nonché la visualizzazione dei grafici delle pagine Oggi e Cronologia, in Websense Manager.
	Dopo aver installato Log Server, configurare Filtering Service in modo che trasferisca i dati di registrazione ai percorsi corretti (vedere <i>Configurazione di Filtering Service</i> <i>per la registrazione</i> , pagina 314).
Database di registrazione	Archivia i dati sulle richieste di accesso a Internet raccolti da Log Server affinché vengano usati dagli strumenti di creazione dei report di Websense.

Componenti dell'identificazione utenti

Componente	Descrizione
User Service	 Comunica con il proprio servizio di directory. Inoltra informazioni relative all'utente, nonché ai report utente-gruppo e utente-dominio, a Policy Server e a Filtering Server, affinché vengano usate nell'applicazione dei criteri di filtraggio.
	Se si è installato e configurato un agente di identificazione trasparente di Websense (vedere <i>Identificazione trasparente</i> , pagina 205), User Service aiuta ad interpretare le informazioni sulle sessioni di accesso dell'utente, ed utilizza queste informazioni per fornire a Filtering Service le associazioni rilevate tra nome utente-indirizzo IP.
	Se si aggiungono utenti e gruppi, come client di Websense (vedere <i>Aggiunta di un client</i> , pagina 70), User Service inoltra le informazioni sul nome e sul percorso dal servizio di directory a Websense Manager.
	Per informazioni sulla configurazione dell'accesso ai servizi di directory, vedere <i>Servizi di directory</i> , pagina 65.
DC Agent	• Offre un'identificazione utente trasparente per gli utenti di un servizio di directory basato su Windows.
	Comunica con User Service per fornire informazioni aggiornate sulle sessioni di accesso dell'utente al software Websense affinché vengano usate per l'applicazione dei filtri.
	Per ulteriori informazioni, vedere <i>DC Agent</i> , pagina 217.
Logon Agent	Offre un'accuratezza insuperabile nell'identificazione trasparente dell'utente nelle reti Linux e Windows.
	• Non si affida a un servizio di directory o ad altri intermediari per catturare le sessioni di accesso dell'utente.
	• Rileva le sessioni di accesso dell'utente nel momento in cui si verificano.
	Logon Agent comunica con l'applicazione di accesso installata nel computer client per assicurare che le sessioni di accesso del singolo utente vengano catturate ed elaborate direttamente dal software Websense.
	Per ulteriori informazioni, vedere Logon Agent, pagina 221.

Componente	Descrizione
eDirectory Agent	• Funziona con Novell eDirectory per identificare gli utenti in modo trasparente.
	• Raccoglie informazioni sulle sessioni di accesso degli utenti da Novell Directory che autentica l'accesso in rete degli utenti.
	 Associa ciascun utente autenticato a un indirizzo IP e collabora quindi con User Service per inoltrare le informazioni necessarie a Filtering Service.
	Per ulteriori informazioni, vedere <i>eDirectory Agent</i> , pagina 229.
RADIUS Agent	Consente un'identificazione trasparente degli utenti che accedono alla rete tramite dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL) o altri tipi di collegamenti remoti.
	Per ulteriori informazioni, vedere <i>RADIUS Agent</i> , pagina 223.

Funzionamento di Policy Database

Websense Policy Database archivia sia i dati relativi ai criteri (comprese le impostazioni definite per i client, i componenti dei filtri e l'amministrazione con delega) sia le impostazioni di configurazione globali specificate in Websense Manager. Le impostazioni specifiche di un'istanza di Policy Server vengono archiviate separatamente.

Nella maggior parte degli ambienti con molteplici Policy Server, un solo Policy Database mantiene i criteri e i dati di configurazione generale di molteplici Policy Server.

- 1. All'avvio, ciascun componente di Websense richiede le informazioni di configurazione applicabili dal Policy Database tramite Policy Broker.
- 2. I componenti in esecuzione verificano spesso la presenza di modifiche apportate a Policy Database.
- 3. Policy Database viene aggiornato ogni volta che gli amministratori apportano modifiche a Websense Manager e fanno clic su Salva tutto.
- 4. Dopo aver apportato una modifica a Policy Database, ogni componente richiede e riceve le modifiche che potrebbero avere un impatto sulle rispettive funzioni.

Accertarsi di eseguire regolarmente un backup del Policy Database per salvaguardare importanti dati di configurazione e informazioni sui criteri definiti. Per ulteriori informazioni, vedere *Esecuzione di backup e ripristino dei dati Websense*, pagina 300.

Gestione di Policy Server

Policy Server è il componente del software Websense che gestisce le informazioni relative ai criteri e che comunica con Filtering Service per aiutare nell'applicazione dei

criteri. Policy Server è anche responsabile dell'identificazione di altri componenti e del rilevamento del loro percorso e stato.

Quando ci si collega a Websense Manager, ci si collega a un'interfaccia grafica in comunicazione con Policy Server.

- Non è possibile collegarsi a Websense Manager fino a quando questo non viene configurato per la comunicazione con Policy Server.
- Se la configurazione del software Websense include molteplici Policy Server, è possibile scegliere tra le varie istanze di Policy Server al momento dell'accesso.
- È possibile aggiungere ed eliminare istanze di Policy Server dall'interno di Websense Manager.

Per predefinizione, la comunicazione tra Websense Manager e un'istanza centrale di Policy Server viene stabilita durante l'installazione di Websense Manager.

La maggior parte degli ambienti richiede soltanto un Policy Server. Un singolo Policy Server può comunicare con molteplici istanze di Filtering Service e Network Agent per un bilanciamento del carico. In organizzazioni di grandi dimensioni (10.000 e più utenti), potrebbe tuttavia essere utile installare molteplici istanze di Policy Server. Se si stanno installando altri Policy Server, aggiungere ciascuna istanza a Websense Manager (vedere *Aggiunta e modifica delle istanze di Policy Server*, pagina 283).

Aggiunta e modifica delle istanze di Policy Server

Usare la pagina **Impostazioni > Policy Server** per aggiungere a Websense Manager istanze di Policy Server o per configurare o eliminare i Policy Server esistenti.

Per aggiungere istanze di Policy Server

- 1. Fare clic su Aggiungi. Viene visualizzata la pagina Aggiungi Policy Server.
- 2. Inserire l'indirizzo IP o il nome host del computer in cui è installato Policy Server nel campo IP o nome del server.
- 3. Inserire il numero di **Porta** che Websense Manager deve usare per comunicare con quell'istanza di Policy Server. Il valore predefinito è **55806**.
- 4. Fare clic su **OK** per ritornare alla pagina Policy Server. La nuova istanza di Policy Server viene visualizzata nell'elenco.
- 5. Fare clic su **OK** per inserire nella cache le modifiche apportate alla pagina Policy Server. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Per modificare un'istanza di Policy Server (ad esempio, se il nome o l'indirizzo IP del computer in cui è installato Policy Server viene modificato), selezionare un indirizzo IP o il nome host dall'elenco del Policy Server e fare quindi clic su **Modifica**.

Per eliminare un'istanza di Policy Server, selezionare un indirizzo IP o un nome host dall'elenco del Policy Server e fare quindi clic su **Elimina**. Facendo clic su Elimina si elimina l'istanza di Policy Server da Websense Manager ma non si disinstalla o chiude il servizio Policy Server di Websense. Se esiste una sola istanza di Policy Server nell'elenco, questa istanza non può essere eliminata.

Ambiente con molteplici Policy Server

In alcuni ambienti distribuiti con un grande numero di utenti, potrebbe essere utile installare molteplici Policy Server. Questo comporta la considerazione di alcuni fattori.

- Se si implementa una configurazione che consente allo stesso client di essere gestito da vari Policy Server, a seconda del carico corrente, si consiglia di **non** implementare le azioni associate a un criterio basato sul tempo:
 - Accedi con password
 - Conferma
 - Assegna durata

Le informazioni sui tempi, associate a queste funzioni, non vengono condivise dai Policy Server e i client potrebbero ricevere un permesso di accesso a Internet più o meno limitato rispetto alla loro richiesta.

Tenere presente che i criteri predefiniti vengono applicati nel caso nessun altro criterio fosse applicabile a un client. Se i client possono essere soggetti alle regole di più di un Policy Server, potrebbe essere utile assicurarsi che il criterio predefinito non imponga filtri di categoria con azioni basate sul tempo.

- Poiché le informazioni sui criteri vengono archiviate nel Policy Database, le modifiche apportate ai criteri vengono automaticamente condivise da tutti i Policy Server quando si fa clic su Salva tutto.
- Molte impostazioni di configurazione globale (come ad esempio le definizioni delle classi di rischio e le opzioni di avviso) vengono condivise dai Policy Server.
- Le impostazioni di configurazione specifiche di un singolo Policy Server (come ad esempio i suoi collegamenti con Filtering Service e Network Agent) vengono archiviate localmente da ciascun Policy Server e non vengono distribuite.

Per passare da un Policy Server ad un altro in Websense Manager al fine di verificare o configurare le impostazioni da applicare a una singola istanza di Policy Server:

- 1. Nell'intestazione di Websense, espandere l'elenco di **Policy Server** e selezionare un indirizzo IP.
- 2. Se esistono modifiche non salvate nell'istanza corrente di Policy Server, viene visualizzato un messaggio di avvertenza. Eseguire una delle operazioni seguenti:
 - Fare clic su **Annulla** per rimanere collegati al Policy Server in uso in modo da poter salvare le modifiche.
 - Fare clic su **OK** per abbandonare le modifiche e collegarsi al Policy Server successivo.
 - Fare clic su **Indietro** per proseguire con la configurazione del Policy Server in uso.

Se non esistono modifiche non salvate, l'utente viene riportato direttamente alla schermata di accesso.

3. Alla schermata di accesso, inserire un nome utente e una password per collegarsi al Policy Server selezionato e fare quindi clic su **Inizia sessione**.

Modifica dell'indirizzo IP del Policy Server

Prima di modificare l'indirizzo IP del computer in cui è installato Policy Server, chiudere tutti i servizi Websense nel computer. Se Websense Manager è installato nello stesso computer, questo include i servizi di Apache2Websense e di ApacheTomcatWebsense.

Dopo aver modificato l'indirizzo IP, occorre aggiornare manualmente i file di configurazione di Websense usati da Websense Manager, Policy Server e altri servizi Websense, prima di poter riprendere ad applicare i filtri.

Punto 1: Aggiornare la configurazione di Websense Manager

Aggiornare Websense Manager per usare il nuovo indirizzo IP per il collegamento con Policy Server.

1. Nel computer in cui è installato Websense Manager, interrompere i servizi Apache2Websense e ApacheTomcatWebsense (se necessario).

Se Websense Manager e Policy Server sono stati installati nello stesso computer, i servizi Apache dovrebbero essere già stati chiusi.

- 2. Navigare alla directory seguente:
 - Windows:

C:\Programmi\Websense EUSM Backup\UserList.bak

Linux:

/opt/Websense/tomcat/conf/Catalina/localhost/

- 3. Individuare il file **mng.xml** e creare una copia di backup del file in un'altra directory.
- Aprire mng.xml in un programma di gestione del testo (come Notepad o Vi) e sostituire ogni istanza del vecchio indirizzo IP di Policy Server con quello nuovo. L'indirizzo IP di Policy Server appare due volte: come valore ps/default/host e come valore psHosts.
- 5. Una volta terminato, salvare e chiudere il file.

Non riavviare i servizi Apache fino a quando non si sono completati gli aggiornamenti di configurazione rimasti in questa sezione.

Punto 2: Aggiornare la configurazione di Policy Server

Aggiornare il file di configurazione Policy Server e il file di inizializzazione utilizzato per configurare la comunicazione tra i vari componenti di Websense.

- 1. Chiudere tutti servizi Websense del computer in cui è installato Policy Server, se non si è ancora provveduto a farlo (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Navigare alla directory bin di Websense.
 - Windows:

C:\Programmi\Websense\bin

- Linux /opt/Websense/bin
- 3. Individuare il file **config.xml** e creare una copia di backup del file in un'altra directory.
- 4. Aprire **config.xml** in un programma di gestione del testo e sostituire ogni istanza del vecchio indirizzo IP del Policy Server con l'indirizzo nuovo.
- 5. Una volta terminato, salvare e chiudere il file.
- 6. Nella directory **bin**, individuare il file **websense.ini** ed eseguire quindi una copia di backup in un'altra directory.
- 7. Aprire **websense.ini** in un programma di gestione del testo e sostituire ogni istanza del vecchio indirizzo IP del Policy Server con quello nuovo.
- 8. Una volta terminato, salvare e chiudere il file.

Punto 3: Verificare la connessione con il database di registrazione.

Usare Windows ODBC Data Source Administrator del computer in cui è installato Policy Server per verificare il collegamento ODBC al database di registrazione.

- 1. Andare a Start > Impostazioni > Pannello di controllo > Strumenti di amministrazione > Origine dati (ODBC).
- 2. Nella scheda **DSN di sistema**, selezionare il nome appropriato per l'origine dei dati (per predefinizione, **wslogdb70**) e fare clic su **Configura**.
- 3. Verificare di aver selezionato il computer server del database corretto e fare quindi clic su **Avanti**.
- 4. Inserire le credenziali utilizzate per collegarsi al database e fare quindi clic su **Avanti**.
- 5. Accettare le impostazioni predefinite delle 2 schermate successive e fare quindi clic su **Test Data Source [Prova origine dati]**

Nota

Se la prova non riesce, verificare il nome del computer server del database e riprovare.

Se il nome del computer è corretto ma la prova non riesce ancora, verificare che la porta di collegamento utilizzata sia quella corretta e che il firewall consenta la comunicazione attraverso la porta selezionata.

Punto 4: Riavviare dei servizi Websense

1. Riavviare il computer Policy Server. Accertarsi che i servizi di Websense del computer siano stati riavviati normalmente.

2. Se Websense Manager, usato per configurare questo Policy Server, è stato installato in un altro computer, riavviare i servizi **Apache2Websense** e **ApacheTomcatWebsense** in quel computer.



Se Websense Manager è stato installato nello stesso computer di Policy Server, gli amministratori dovranno usare il nuovo indirizzo IP per collegarsi.

Gestione di Filtering Service

Filtering Service è il componente del software Websense che collabora con Network Agent o con un prodotto di integrazione di terzi per filtrare l'attività svolta in Internet. Se un utente richiede l'accesso a un sito, Filtering Service riceve la richiesta, determina il criterio da applicare ed usa il criterio applicabile per determinare come filtrare il sito.

Ciascuna istanza di Filtering Service scarica la propria copia del Master Database di Websense da usare per la determinazione di come filtrare le richieste di accesso a Internet.

Filtering Service invia al Log Server anche le informazioni sulle attività in Internet in modo che queste possano venire registrate e usate per la creazione dei report.

Se ci si collega a Websense Manager, un **Filtering Service Summary** della pagina Stato > Oggi includerà un elenco con gli indirizzi IP e lo stato corrente di ciascuna istanza di Filtering Service, associata al Policy Service in uso. Fare clic sull'indirizzo IP di Filtering Service per visualizzare informazioni sul Filtering Service selezionato.

Revisione dei dati di Filtering Service

Usare la pagina **Stato > Oggi > Dettagli di Filtering Service** per verificare lo stato di una singola istanza di Filtering Service.

La pagina elenca:

- Indirizzo IP di Filtering Service
- Se l'istanza selezionata è in esecuzione o meno
- La versione di Filtering Service

Il numero di versione deve corrispondere al numero di versione del software Websense, tenendo in considerazione possibili aggiornamenti correttivi.

- Il sistema operativo in esecuzione nel computer con installato Filtering Service
- La piattaforma del software Websense

Questo indica se il software Websense è in esecuzione in modalità stand-alone o è integrato con un prodotto sviluppato da terzi.

• L'indirizzo IP e lo stato di qualsiasi istanza di Network Agent con la quale Filtering Service comunica.

Fare clic su Chiudi per ritornare alla pagina Oggi.

Verifica dello stato di download del Master Database

Ciascuna istanza di Filtering Service nella propria rete scarica la propria copia del Master Database. Quando si lavora inWebsense Manager, Riepilogo avviso di integrità della pagina Stato > Oggi visualizza un messaggio di stato quando il download di un Master Database è in corso oppure se un tentativo di download non è riuscito.

Per informazioni dettagliate su un download recente o in corso del database, fare clic su **Download database** nella casella degli strumenti della pagina Oggi. La pagina di Download database include una voce per ciascuna istanza di Filtering Service associata al Policy Server in uso.

Inizialmente, la pagina Download database visualizza un riepilogo rapido del download indicando dove il database è stato scaricato, la versione del database scaricato e se lo scaricamento è stato completato. Da questo riepilogo, è possibile:

- Iniziare il download del database da un Filtering Service (fare clic su Aggiorna).
- Iniziare il download del database da un'istanza di Filtering Service (fare clic su Aggiorna tutto).
- Annullare uno o tutti gli aggiornamenti

Fare clic su un indirizzo IP dell'elenco a destra per verificare in dettaglio lo stato di scaricamento del database per l'istanza di Filtering Service selezionata.

- Se l'istanza di Filtering Service selezionata ha incontrato un problema di scaricamento, potrebbe venire visualizzato un messaggio con le istruzioni necessarie.
- Per avviare manualmente il download del database per l'istanza di Filtering Service selezionata, fare clic su **Aggiorna**.

Durante lo scaricamento del database, la schermata dello stato visualizza informazioni sullo stato di avanzamento di ciascuna fase del processo di download. Fare clic su **Chiudi** per nascondere le informazioni di avanzamento e per continuare a lavorare in Websense Manager.

Ripresa del download del Master Database

Se il download di un Master Database viene interrotto, il software Websense tenta di riprendere automaticamente il download. Se Filtering Service è in grado di ricollegarsi con il server del download, il download riprende dal punto in cui era stato interrotto.

È possibile riavviare manualmente un download non riuscito o interrotto. In questo caso, il download non riprende dal punto di interruzione ma riavvia invece la procedura dall'inizio.

 In Websense Manager, andare a Stato > Oggi e fare clic su Download del database.
- 2. Fare clic su **Interrompi tutti gli aggiornamenti** per chiudere il processo interrotto.
- 3. Selezionare un'istanza di Filtering Service e fare clic su **Aggiorna** oppure fare clic su **Aggiorna tutto**, per riavviare la procedura di download dall'inizio.

Visualizzazione ed esportazione del registro di controllo

Il software Websense dispone di una funzione di analisi retrospettiva che indica gli amministratori che hanno acceduto a Websense Manager, nonché tutte le modifiche apportate ai criteri e alle impostazioni. Queste informazioni sono disponibili soltanto ai Super Administrator autorizzati alla gestione dei criteri (vedere *Super Administrator*, pagina 243).

Gli amministratori con delega mantengono un controllo significativo sulle attività svolte in Internet dai client da loro gestiti. Il monitoraggio delle modifiche per mezzo del registro di controllo consente di accertare che questo controllo sia gestito in modo responsabile e in conformità con i criteri d'uso approvati dalla propria organizzazione.

Usare la pagina **Stato > Registro di controllo** per visualizzare il registro di controllo e per esportare le parti selezionate in un foglio di Excel (XLS), se necessario.

I registri di controllo vengono conservati per 60 giorni. Per conservare i record del registro di controllo oltre 60 giorni, usare l'opzione di esportazione per esportare il registro ad intervalli regolari. L'esportazione non elimina i record dal registro di controllo.

Quando la pagina del Registro di controllo è aperta, vengono visualizzati i record più recenti. Usare la barra di scorrimento e i pulsanti di navigazione situati sopra il registro per visualizzare i record più vecchi.

Il registro visualizza le informazioni seguenti: Se una voce è troncata, fare clic sulla voce parziale per visualizzare l'intero record in una finestra di dialogo popup.

Colonna	Descrizione
Data	La data e l'ora della modifica, in conformità con il fuso orario.
	Per garantire dati coerenti nel registro di controllo, accertarsi che tutti i computer con i componenti di Websense installati, siano sincronizzati in termini di data e ora.
Utente	Il nome dell'amministratore che ha eseguito la modifica.
Server	L'indirizzo IP o il nome del computer in cui Policy Server è installato e su cui la modifica ha agito.
	Viene visualizzato soltanto per le modifiche che incidono su Policy Server, come ad esempio le modifiche apportate alla scheda Impostazioni.

Colonna	Descrizione
Ruolo	Il ruolo di amministrazione con delega su cui la modifica ha agito.
	Se una modifica agisce su un client che è stato assegnato come "client gestito" al ruolo di amministratore con delega, la modifica apportata agirà anche nei confronti del ruolo di Super Administrator. Se la modifica agisce su un client che fa parte di un intervallo di rete, di un gruppo, di un dominio o di un'unità organizzativa assegnati al ruolo, la modifica agirà sul ruolo di amministratore con delega.
Tipo	L'elemento di configurazione modificato, come ad esempio un criterio, un filtro di categoria, o un accesso/disconnessione.
Elemento	L'identificatore di un oggetto modificato come ad esempio il nome di un filtro di categoria o il nome di un ruolo.
Azione	Il tipo di modifica apportata, come ad esempio un'aggiunta, un'eliminazione, un accesso e così via
Precedente	Il valore definito prima della modifica.
Corrente	Il nuovo valore dopo la modifica.

Non tutte le voci vengono visualizzate per tutti i record. Ad esempio, il ruolo non viene visualizzato per i record relativi a un accesso o a una disconnessione.

Per esportare i record del registro di controllo:

1. Selezionare un periodo di tempo dall'elenco Esporta intervallo.

Scegliere Ultimi 60 giorni per esportare l'intero file del registro di controllo.

2. Fare clic su Vai.

Se Microsoft Excel è installato nel computer con Websense Manager in esecuzione, il file esportato viene aperto. Usare le opzioni di Excel per salvare o stampare il file.

Se Microsoft Excel non è stato installato nel computer di Websense Manager, seguire le istruzioni su schermo per individuare il software o per salvare il file.

Chiusura e riavvio dei servizi di Websense

I servizi di Websense vengono configurati per un riavvio automatico ad ogni riavvio del computer. A volte potrebbe essere tuttavia necessario chiudere o riavviare uno o più componenti del prodotto indipendentemente dal riavvio del computer.

Nota

Se Filtering Service sta scaricando il Master Database, non si chiuderà fino a quando il download non è stato completato. Se si chiudono tutti i servizi di Websense, terminare sempre con i servizi seguenti, nelll'ordine qui riportato:

- 1. Websense Filtering Service
- 2. Websense Policy Broker
- 3. Websense Policy Database

Tenere presente che a meno che non sia insorto un problema specificatamente correlato a Policy Broker o a Policy Database, è molto improbabile che si debbano riavviare questi servizi. Evitare di riavviare questi servizi, se possibile.

Se si riavviano tutti i servizi di Websense, iniziare sempre dai servizi seguenti, nell'ordine qui riportato:

- 1. Websense Policy Database
- 2. Websense Policy Broker
- 3. Websense Filtering Service

Windows

- 1. Aprire la finestra di dialogo Servizi di Windows Start > Impostazioni > Pannello di controllo > Strumenti di amministrazione > Servizi.
- 2. Fare clic con il pulsante destro del mouse sul nome del servizio di Websense e selezionare quindi **Interrompi** o **Start**.

Linux

Nei computer con sistema operativo Linux, tutti i servizi vengono interrotti e avviati simultaneamente quando si usa questa procedura.

- 1. Andare alla directory /opt/Websense.
- 2. Verificare lo stato dei servizi Websense mediante il comando seguente:
 - ./WebsenseAdmin status
- 3. Chiudere, avviare o riavviare tutti i servizi di Websense mediante i comandi seguenti:
 - ./WebsenseAdmin stop
 - ./WebsenseAdmin start
 - ./WebsenseAdmin restart



1

Non usare il comando **kill** per chiudere un servizio di Websense in quanto potrebbe danneggiare il servizio.

Avvisi su schermo

Argomenti correlati:

- Prevenzione di un numero eccessivo di avvisi, pagina 292
- Configurazione delle opzioni generali degli avvisi, pagina 293
- Configurazione degli avvisi del sistema, pagina 295
- Configurazione degli avvisi di utilizzo di una categoria, pagina 296
- Configurazione degli avvisi di utilizzo di un protocollo, pagina 297

Per facilitare il monitoraggio e la gestione sia del software Websense che delle attività Internet dei client, i Super Administrator possono configurare dei messaggi di avvertenza da visualizzare al verificarsi di determinati eventi.

- Avvisi di sistema: Le notifiche riguardanti lo stato della sottoscrizione e l'attività del Master Database.
- Avvisi di utilizzo: Le notifiche visualizzate quando l'attività di Internet riguardo a determinate categorie o protocolli raggiunge le soglie configurate.

Gli avvisi possono venire inviati a specifici destinatari via e-mail, come messaggi su schermo (messaggistica **net send** di Windows) o come messaggi SNMP.

Nota

Gli avvisi popup su schermo non possono essere inviati dai computer con sistema operativo Linux. Possono tuttavia essere inviati da un computer Linux, con Policy Server installato, ai computer con sistema operativo Windows purché il client Samba sia stato installato nel computer Linux. Vedere *Guida di distribuzione*.

Gli avvisi di utilizzo possono venire generati per le categorie e i protocolli definiti da Websense o personalizzati dall'utente.

Prevenzione di un numero eccessivo di avvisi

Argomenti correlati:

- Avvisi su schermo, pagina 292
- Configurazione delle opzioni generali degli avvisi, pagina 293
- Configurazione degli avvisi di utilizzo di una categoria, pagina 296
- Configurazione degli avvisi di utilizzo di un protocollo, pagina 297

Sono disponibili delle funzioni di controllo incorporate per evitare la generazione di un numero eccessivo di avvisi. Usare l'impostazione **Numero massimo di avvisi** giornalieri per tipo di utilizzo per specificare il numero massimo di avvisi che si possono inviare in risposta alle richieste degli utenti riguardo a determinate categorie o protocolli. Per ulteriori informazioni, vedere *Configurazione delle opzioni generali degli avvisi*, pagina 293.

Si possono anche definire dei limiti di soglia degli avvisi di utilizzo per ogni categoria e protocollo. Ad esempio, se si imposta la soglia per il numero massimo di avvisi su 10 per una determinata categoria, viene generato un avviso dopo 10 richieste ricevute per quella categoria (provenienti da una combinazione qualsiasi di client). Per ulteriori informazioni, vedere *Configurazione degli avvisi di utilizzo di una categoria*, pagina 296 e *Configurazione degli avvisi di utilizzo di un protocollo*, pagina 297.

Supponiamo che il numero massimo di avvisi giornalieri sia impostato su 20 e la soglia di avvisi per una determinata categoria sia impostata su 10. Gli amministratori vengono avvertiti soltanto le prime 20 volte che le richieste di una categoria superano la soglia definita. Ciò significa che soltanto le prime 200 ricorrenze generano un avviso di avvertenza (soglia di 10 moltiplicata per il limite massimo di avvisi di 20).

Configurazione delle opzioni generali degli avvisi

Argomenti correlati:

- Avvisi su schermo, pagina 292
- Configurazione degli avvisi del sistema, pagina 295
- Configurazione degli avvisi di utilizzo di una categoria, pagina 296
- Configurazione degli avvisi di utilizzo di un protocollo, pagina 297

Il software Websense può notificare gli amministratori al verificarsi di vari tipi di eventi di sistema, quali l'aggiornamento delle categorie del Master Database o i problemi di sottoscrizione, oppure quando l'utilizzo di Internet supera il limite di soglia definito.

Usare la pagina **Impostazioni > Avvisi e notifiche > Avvisi** per selezionare e configurare i metodi di notifica più indicati, come descritto sopra. Usare quindi le altre pagine della sezione Impostazioni > Avvisi e notifiche per attivare gli avvisi che si vogliono ricevere.

1. Inserire un numero nel campo **Numero massimo di avvisi giornalieri per tipo di utilizzo** per limitare il numero di avvisi generati giornalmente per ciascun avviso di utilizzo riguardante categorie o protocolli.

Ad esempio, si può configurare il sistema in modo che gli avvisi di utilizzo vengano inviati ogni 5 volte (soglia) che qualcuno richiede di accedere a un sito della categoria Sport. A seconda del numero di utenti e delle loro abitudini di uso di Internet, ciò potrebbe generare centinaia di avvisi ogni giorno. Se si inserisce 10 come numero massimo di avvisi giornalieri in base al tipo di utilizzo, verranno generati soltanto 10 avvisi giornalieri per la categoria Sport. In questo esempio, gli avvisi avvertono riguardo alle prime 50 richieste di siti di Sport (5 richieste per avviso moltiplicato per 10 avvisi).

2. Selezionare la casella di controllo **Abilita avvisi mediante e-mail** affinché avvisi e notifiche vengano inviati tramite e-mail. Configurare quindi le impostazioni relative alle e-mail.

IP o nome del server SMTP	L'indirizzo IP o il nome del server SMTP attraverso il quale passano gli avvisi inviati tramite e-mail.
Indirizzo e-mail	Indirizzo e-mail da usare come mittente per gli avvisi
mittente	inviati tramite e-mail.
Indirizzo e-mail	L'indirizzo e-mail del destinatario principale delle e-
amministratore (A):	mail di avviso.
Indirizzo e-mail destinatari (Cc):	L'indirizzo e-mail fino a un massimo di altri 50 destinatari. Ciascun indirizzo deve essere in una riga separata.

3. Selezionare la casella di controllo **Abilita avvisi pop-up** affinché i messaggi popup vengano visualizzati in determinati computer. Inserire quindi l'indirizzo IP o il nome del computer di un massimo di 50 **Destinatari**, ciascuno su una riga separata.



Nota

Gli avvisi pop-up non possono essere inviati dai computer con sistema operativo Linux. Possono tuttavia essere inviati da un computer Linux, con Policy Server installato, ai computer con sistema operativo Windows purché il client Samba sia stato installato nel computer Linux. Vedere *Guida di distribuzione*.

4. Selezionare la casella di controllo **Abilita avvisi SNMP** affinché gli avvisi vengano inviati tramite un sistema SNMP Trap, installato in rete. Fornire quindi le informazioni necessarie sul sistema SNMP Trap.

Nome comunità	Nome della comunità trap nel server SNMP Trap.
IP o nome del server	L'Indirizzo IP o il nome del server SNMP Trap.
Porta	Il numero di porta usato dal messaggio SNMP.

5. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Configurazione degli avvisi del sistema

Argomenti correlati:

- Avvisi su schermo, pagina 292
- Configurazione delle opzioni generali degli avvisi, pagina 293
- Revisione dello stato del sistema in uso, pagina 299

Websense Manager visualizza la pagina **Stato > Avvisi** (informazioni dettagliate) descritta in *Revisione dello stato del sistema in uso*, pagina 299.

Per accertare che gli amministratori vengano notificati riguardo importanti eventi relativi al sistema, come ad esempio la non riuscita del download del database o una sottoscrizione di prossima scadenza, mentre non sono collegati a Websense Manager, configurare il sistema di generazione degli avvisi di Websense in modo che gli avvisi vengano inviati via e-mail, tramite messaggi pop-up o tramite il sistema SNMP Trap.

Nella scheda Impostazioni, usare la pagina **Avvisi e notifiche > Sistema** per selezionare il metodo con cui inviare questi avvisi agli amministratori di Websense, e per definire il tipo di avvisi da inviare.

 Per ciascun avviso, selezionare il metodo di invio. A seconda dei metodi disponibili nella pagina Avvisi, è possibile scegliere il metodo E-mail, Pop-up e SNMP.



Nota

Oltre alla generazione di un avviso, le informazioni sui download non riusciti e sui livelli di sottoscrizione superati, vengono registrate nel visualizzatore degli eventi di Windows (soltanto per Windows) e nel file Websense.log (Windows e Linux).

Sono disponibili degli avvisi in risposta ai seguenti eventi:

- La sottoscrizione scade tra una settimana.
- I motori di ricerca supportati da Search Filtering sono stati modificati.
- Download di un Websense Master Database non riuscito.
- Una categoria o un protocollo è stato aggiunto al, o rimosso dal, Master Database.
- Il numero di utenti attuali supera il livello di sottoscrizione.
- Il numero di utenti correnti ha raggiunto il 90% del livello di sottoscrizione.
- La sottoscrizione scade tra un mese.
- Websense Master Database è stato aggiornato.
- Al termine della procedura, fare clic su OK per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su Salva tutto.

Configurazione degli avvisi di utilizzo di una categoria

Argomenti correlati:

- Avvisi su schermo, pagina 292
- Prevenzione di un numero eccessivo di avvisi, pagina 292
- Configurazione delle opzioni generali degli avvisi, pagina 293
- Aggiunta di avvisi di utilizzo di una categoria, pagina 296

Il software Websense può inviare una notifica nel caso l'attività in Internet per particolari categorie di URL dovesse raggiungere una soglia predefinita. È possibile definire gli avvisi relativi a richieste autorizzate o a richieste bloccate riguardo a una determinata categoria.

Ad esempio, potrebbe essere utile venire avvertiti al raggiungimento di 50 autorizzazioni di richieste di accesso ai siti della categoria Acquisti in linea, per determinare se applicare o meno delle restrizioni a questa categoria. Oppure potrebbe essere utile ricevere un avviso ogni volta che 100 richieste per i siti della categoria Intrattenimento vengono bloccate, per determinare se gli utenti si sono abituati a un nuovo criterio d'uso di Internet.

Nella scheda Impostazioni, usare la pagina **Avvisi e notifiche > Utilizzo categoria** per visualizzare gli avvisi già definiti e per aggiungere o eliminare gli avvisi di utilizzo di una categoria.

- 1. Visualizzare i due elenchi **Avvisi di utilizzo categoria autorizzati** e **Avvisi di utilizzo categoria bloccati** per istruzioni sulle categorie da configurare per l'invio di avvisi, la soglia definita per ciascuna delle categorie e i metodi selezionati per l'invio degli avvisi.
- Fare clic su Aggiungi sotto l'apposito elenco per aprire la pagina Aggiungi avvisi di utilizzo categoria (vedere *Aggiunta di avvisi di utilizzo di una categoria*, pagina 296) e configurare altre categorie di URL per l'invio di avvisi.
- 3. Selezionare la casella di controllo per le categorie che si vuole eliminare dall'elenco e fare quindi clic su **Elimina** sotto l'apposito elenco.
- 4. Una volta terminato, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Utilizzo categoria. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta di avvisi di utilizzo di una categoria

Argomenti correlati:

- Avvisi su schermo, pagina 292
- Configurazione delle opzioni generali degli avvisi, pagina 293
- Configurazione degli avvisi di utilizzo di una categoria, pagina 296

La pagina **Aggiungi avvisi di utilizzo categoria** viene visualizzata quando si fa clic su Aggiungi nella pagina Avvisi di utilizzo categoria. È possibile selezionare qui nuove categorie per gli avvisi di utilizzo, stabilire la soglia di questi avvisi e selezionare i metodi di invio degli avvisi.

- 1. Selezionare la casella di controllo adiacente ad ogni categoria affinché questa venga aggiunta mantenendo le definizioni di soglia e di metodo di invio degli avvisi.
 - Nota Non è possibile aggiungere avvisi di utilizzo per le categorie escluse dalla registrazione nel log. Vedere *Configurazione di Filtering Service per la registrazione*, pagina 314.
- 2. Definire la **Soglia** tramite la selezione del numero di richieste che devono comportare la generazione di un avviso.
- 3. Selezionare la casella di controllo del metodo desiderato per l'invio degli avvisi (E-mail, Pop-up, SNMP) per queste categorie.

Soltanto i metodi di invio degli avvisi attivati nella pagina Avvisi (vedere *Configurazione delle opzioni generali degli avvisi*, pagina 293) sono disponibili per la selezione.

4. Fare clic su **OK** per inserire nella cache le modifiche apportate e per ritornare alla pagina Avvisi di utilizzo categoria. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Configurazione degli avvisi di utilizzo di un protocollo

Argomenti correlati:

- Avvisi su schermo, pagina 292
- Prevenzione di un numero eccessivo di avvisi, pagina 292
- Configurazione delle opzioni generali degli avvisi, pagina 293
- Aggiunta degli avvisi di utilizzo protocollo, pagina 298

Il software Websense può inviare una notifica nel caso l'attività in Internet relativa ad un determinato protocollo dovesse raggiungere una soglia predefinita. È possibile definire gli avvisi relativi a richieste autorizzate o a richieste bloccate riguardo al protocollo selezionato.

Ad esempio, potrebbe essere utile venire avvertiti al raggiungimento di 50 richieste del protocollo di una determinata messaggistica immediata, per determinare se applicare o meno delle restrizioni a quel protocollo. Oppure potrebbe essere utile ricevere un avviso ogni volta che 100 richieste del protocollo per lo scambio di un file peer-to-peer vengono bloccate, per determinare se gli utenti si sono abituati a un nuovo criterio d'uso di Internet.

Nella scheda Impostazioni, usare la pagina **Avvisi e notifiche > Utilizzo protocollo** per visualizzare gli avvisi già definiti e per aggiungere o eliminare i protocolli relativi agli avvisi di utilizzo.

- 1. Visualizzare i due elenchi **Avvisi di utilizzo protocolli autorizzati** e **Avvisi di utilizzo protocolli bloccati** per istruzioni sui protocolli da configurare per l'invio di avvisi, la soglia di ciascun protocollo e i metodi selezionati per l'invio degli avvisi.
- Fare clic su Aggiungi sotto l'apposito elenco per aprire la pagina Aggiungi avvisi di utilizzo protocollo (vedere *Aggiunta degli avvisi di utilizzo protocollo*, pagina 298) e configurare altri protocolli per l'invio di avvisi.
- 3. Selezionare la casella di controllo per i protocolli che si vuole eliminare e fare quindi clic su **Elimina** sotto l'apposito elenco.
- 4. Una volta terminato, fare clic su **OK** per inserire le modifiche nella cache e per ritornare alla pagina Avvisi di utilizzo protocollo. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta degli avvisi di utilizzo protocollo

Argomenti correlati:

- Avvisi su schermo, pagina 292
- Configurazione delle opzioni generali degli avvisi, pagina 293
- Configurazione degli avvisi di utilizzo di un protocollo, pagina 297

Usare la pagina **Avvisi di utilizzo protocolli autorizzati > Aggiungi protocollo Avvisi di utilizzo** per selezionare i nuovi protocolli per gli avvisi di utilizzo, per stabilire la soglia di ciascun avviso e selezionare i metodi per l'invio degli avvisi.

1. Selezionare la casella di controllo adiacente a ciascun protocollo da aggiungere insieme alla definizione della soglia e del metodo di invio degli avvisi.



Nota

Non è possibile selezionare un protocollo per gli avvisi a meno che questo non sia stato configurato per la registrazione in uno o più filtri di protocollo.

Gli avvisi di protocollo riflettono soltanto l'uso da parte dei client soggetti alle regole di un filtro di protocollo che prevede la registrazione del protocollo.

- 2. Definire la **Soglia** selezionando il numero di richieste che devono comportare la generazione di un avviso.
- 3. Selezionare i metodi desiderati per l'invio degli avvisi (E-mail, Pop-up, SNMP) riguardo a questi protocolli.

Soltanto i metodi di invio degli avvisi attivati nella pagina Avvisi (vedere *Configurazione delle opzioni generali degli avvisi*, pagina 293) sono disponibili per la selezione.

4. Fare clic su OK per inserire nella cache le modifiche apportate e per ritornare alla pagina Avvisi di utilizzo protocollo (vedere *Configurazione degli avvisi di utilizzo di un protocollo*, pagina 297). Le modifiche non vengono implementate fino a quando non si fa clic su Salva tutto.

Revisione dello stato del sistema in uso

Usare la pagina **Stato > Avvisi** per reperire informazioni relative ai problemi che incidono sulla performance del software Websense, per ottenere assistenza nella diagnostica e risoluzione problemi, e per verificare i dettagli degli aggiornamenti recenti di Websense Master Database, eseguiti in tempo reale .

L'elenco Avvisi attivi include lo stato dei componenti software di Websense monitorati.

- Per informazioni dettagliate sui componenti da monitorare, fare clic su **Elementi** sottoposti a monitoraggio sopra l'elenco dei messaggi di avviso.
- Per diagnosticare e risolvere un problema, fare clic sul pulsante Soluzioni accanto al messaggio d'errore o di avvertenza.
- Per nascondere un messaggio di avvertenza, fare clic su Avanzate. Se la propria organizzazione non usa Log Server, Network Agent o User Service, o se non si intende attivare WebCatcher, contrassegnare una casella di controllo per nascondere il relativo avviso. Al termine della procedura, fare clic su OK per applicare le modifiche.

Fare clic su Avanzate per nascondere le opzioni avanzate.

L'elenco **Aggiornamenti del database in tempo reale** contiene informazioni sugli aggiornamenti di emergenza del Websense Master Database, che riportano:

- Quando è avvenuto l'aggiornamento
- Il tipo di aggiornamento
- Il nuovo numero di versione del database
- La ragione dell'aggiornamento
- L'indirizzo IP dell'istanza di Filtering Service che ha ricevuto l'aggiornamento

Questi aggiornamenti supplementari si verificano in aggiunta agli aggiornamenti regolari e pianificati del Master Database e potrebbero venire usati, ad esempio, per ricategorizzare un sito che è stato temporaneamente categorizzato in modo erroneo. Il software Websense controlla ad ogni ora la disponibilità di nuovi aggiornamenti del database.

Per gli utenti di Websense Web Security, la pagina Avvisi include un terzo elenco: Aggiornamenti di sicurezza in tempo reale. Questo elenco ha lo stesso formato dell'elenco Aggiornamenti del database in tempo reale ma mostra in modo specifico gli aggiornamenti in tempo reale associati alla sicurezza.

L'installazione di questi aggiornamenti di sicurezza, non appena disponibili, eliminano la vulnerabilità ad attacchi phishing, a rogue application e a codici dannosi che attaccano siti o applicazioni Web di uso frequente.

Per ulteriori informazioni sugli aggiornamenti in tempo reale, vedere *Real-Time Security Updates*TM, pagina 33.

Usare il pulsante **Stampa**, sopra la pagina, per aprire una finestra secondaria con una versione stampabile dell'area degli Avvisi. Utilizzare le opzioni offerte dal browser per stampare questa pagina che non dispone di tutte le opzioni di navigazione disponibili nella finestra principale di Websense Manager.

Esecuzione di backup e ripristino dei dati Websense

Argomenti correlati:

- Pianificazione del backup, pagina 302
- Esecuzione immediata dei backup, pagina 303
- Manutenzione dei file di backup, pagina 304
- Ripristino dei dati Websense, pagina 305
- Cancellazione della pianificazione dei backup, pagina 306
- Opzioni di comando, pagina 306

L'utilità di Backup di Websense semplifica la procedura di backup delle impostazioni e dei criteri definiti nel software Websense, nonché il ripristino di una configurazione definita in precedenza. I dati salvati dall'utilità possono anche venire usati per importare le informazioni di configurazione di Websense dopo un aggiornamento.

L'utilità di Backup salva:

- Le informazioni di configurazione globali, inclusi i dati sui client e sui criteri, archiviate nel Policy Database;
- Le informazioni di configurazione locale, come ad esempio le impostazioni di Filtering Service e Log Server, archiviate da ciascun Policy Server.
- I file di inizializzazione e configurazione dei componenti Websense.

Il processo di backup funziona come segue:

- 1. Inizializzare un backup immediato (vedere *Esecuzione immediata dei backup*, pagina 303) o definire una pianificazione dei backup (vedere *Pianificazione del backup*, pagina 302).
 - Lanciare manualmente un backup, in qualsiasi momento.

- I file di backup vengono archiviati in una directory specifica quando si esegue o si pianifica un backup.
- L'utilità di Backup controlla tutti i componenti di Websense installati nel computer, raccoglie i dati di cui eseguire il backup e crea un file di archiviazione. Il nome del file riflette il formato:

wsbackup_yyyy-mm-dd_hhmmss.tar.gz

In questo caso, *yyyy-mm-dd_hhmmss* rappresenta la data e l'ora del backup, mentre **tar.gz** è un formato di file compresso.

Soltanto i membri principali (Linux) e i membri del gruppo di amministratori (Windows) possono accedere ai file di backup.

Eseguire l'utilità di Backup di Websense di ciascun computer che include i componenti di Websense. Lo strumento identifica e salva tutti i file seguenti che trova nel computer in uso:

Percorso	Nome del file
\Programmi \Websense\bin or	authserver.ini
/opt/Websense/bin	BrokerService.cfg
	config.xml
	eimserver.ini
	LogServer.ini
	netcache.conf
	securewispproxy.ini
	transid.ini
	upf.conf
	websense.ini
	WebUI.ini
	wsauthserver.ini
	wscitrix.ini
	WSE.ini
	wsedir.ini
	wsradius.ini
	wsufpserver.ini
bin/i18n	i18n.ini
bin/postgres/data	postgresql.conf
	pg_hba.conf
BlockPages/*/Custom	Tutte le impostazioni della pagina di blocco
tomcat/conf/Catalina/ Localhost	mng.xml
Windows\system32	isa_ignore.txt
Windows\system32\bin	ignore.txt
/etc/wsLib	wsSquid.ini

Archiviare i file di backup di Websense in un percorso protetto e sicuro. Questi file devono far parte delle procedure di backup normale della propria organizzazione.

Per ripristinare una configurazione precedente:

- 1. Reperire i file di backup dal sito di archiviazione.
- 2. Copiare i file di backup nel computer con Websense nel quale erano stati creati.
- 3. Eseguire l'utilità di Backup in modalità di ripristino.

Importante

Usare sempre l'utilità di Backup per ripristinare una configurazione precedente del software Websense. Non estrarre i file dall'archivio usando altre utilità di estrazione.

Se il file di backup è danneggiato, non sarà possibile ripristinare le impostazioni archiviate.

Durante la procedura di ripristino, qualsiasi messaggio di errore o di avvertenza viene visualizzato nel computer in cui si sta eseguendo il ripristino.

Pianificazione del backup

Argomenti correlati:

- Esecuzione immediata dei backup, pagina 303
- Manutenzione dei file di backup, pagina 304
- Ripristino dei dati Websense, pagina 305
- Cancellazione della pianificazione dei backup, pagina 306
- Opzioni di comando, pagina 306

Per pianificare i backup, aprire il comando Shell e navigare alla directory bin di Websense (C:\Programmi\Websense\bin o opt/Websense/bin, per predefinizione). Digitare il seguente comando.

wsbackup -s -t "<m> <h> <giorno_del_mese> <mese>
 <giorno della settimana>" -d <directory>

Tenere presente che le informazioni sui tempi utilizzano un formato **crontab** e i punti interrogativi e gli spazi sono obbligatori.

Variabile	Informazioni
<m></m>	0 - 59
	Specificare il minuto preciso in cui si vuole iniziare il backup.
<h></h>	0 - 23
	Specificare l'ora precisa del giorno in cui si vuole iniziare il backup.
<giorno_del_mese></giorno_del_mese>	1 - 31
	Specificare la data di esecuzione del backup. Se si pianifica un backup per i giorni 29-31, l'utilità usa la procedura di sostituzione standard del sistema operativo per i mesi che non includono quella data.
<mese></mese>	1 - 12
	Specificare il mese di esecuzione del backup.
<giorno_della_settimana></giorno_della_settimana>	0 - 6
	Specificare un giorno della settimana. 0 rappresenta la domenica.

Per la sostituzione delle variabili mostrate nell'esempio, fornire le informazioni seguenti:

Ogni campo può contenere un numero, un asterisco o un elenco di parametri. Fare riferimento alle istruzioni relative al comando **crontab**.

Esecuzione immediata dei backup

Argomenti correlati:

- *Pianificazione del backup*, pagina 302
- Manutenzione dei file di backup, pagina 304
- *Ripristino dei dati Websense*, pagina 305
- Cancellazione della pianificazione dei backup, pagina 306
- *Opzioni di comando*, pagina 306

Per lanciare l'esecuzione immediata di un backup, aprire il comando Shell e navigare alla directory bin di Websense (C:\Programmi\Websense\bin o opt/Websense/bin, per predefinizione). Digitare il seguente comando.

wsbackup -b -d <directory>

In questo caso, *directory* indica la directory di destinazione per l'archivio di backup.



Attenzione

Non archiviare i file di backup nella directory **bin** di Websense. Questa directory viene eliminata se si disinstalla il software Websense.

Se si avvia un backup immediato, eventuali messaggi di errore e notificche vengono visualizzate nella console del computer in cui è in esecuzione il backup.

Manutenzione dei file di backup

Argomenti correlati:

- *Pianificazione del backup*, pagina 302
- Esecuzione immediata dei backup, pagina 303
- *Ripristino dei dati Websense*, pagina 305
- Cancellazione della pianificazione dei backup, pagina 306
- *Opzioni di comando*, pagina 306

Quando si esegue un backup, si crea automaticamente un file di configurazione (**WebsenseBackup.cfg**) il quale viene successivamente memorizzato nell'archivio di backup. Questo file di configurazione specifica:

- La durata di archiviazione dei backup nella directory di backup
- La massima quantità di spazio su disco che può essere usata da tutti i file di backup contenuti nella directory.

Modificare il file **WebsenseBackup.cfg** in un programma di gestione del testo per modificare uno o entrambi questi parametri:

Parametro	Valore
KeepDays	Il numero di giorni in cui i file di archivio devono rimanere nella directory di backup. Il valore predefinito è 365.
KeepSize	Il numero di byte allocati per i file di backup. Il valore predefinito è 10857600.

Tutti i file più vecchi del valore definito in **KeepDays** vengono eliminati dalla directory di backup. Se si supera la quantità di spazio su disco assegnato, i file più vecchi vengono eliminati dalla directory di backup per fare spazio per i nuovi file.

Ripristino dei dati Websense

Argomenti correlati:

- Pianificazione del backup, pagina 302
- Esecuzione immediata dei backup, pagina 303
- *Manutenzione dei file di backup*, pagina 304
- Cancellazione della pianificazione dei backup, pagina 306
- Opzioni di comando, pagina 306

Quando si ripristinano i dati di configurazione di Websense, accertarsi di aver ripristinato i dati relativi ai componenti installati nel computer corrente.

Per iniziare il processo di ripristino, aprire il comando Shell di Websense (C:\Programmi\Websense\bin o opt/Websense/bin, per predefinizione). Digitare il seguente comando.

wsbackup -r -f archive_file.tar.gz

Importante

La procedura di ripristino potrebbe richiedere diversi minuti. Non interrompere la procedura mentre il ripristino è in corso.

Durante la procedura di ripristino, l'utilità di Backup interrompe tutti i servizi di Websense. Se l'utilità non può interrompere i servizi, invia un messaggio chiedendo all'utente di interromperli manualmente. I servizi vanno interrotti nell'ordine riportato nella sezione *Chiusura e riavvio dei servizi di Websense*, pagina 290.

L'utilità di Backup salva alcuni file usati per la comunicazione con i prodotti di integrazione sviluppati da terzi. Poiché questi file risiedono al di fuori della struttura delle directory di Websense, occorre ripristinarli manualmente copiando ciascun file nella directory corretta.

I file da ripristinare manualmente includono:

Nome del file	Ripristinare in
isa_ignore.txt	Windows\system32
ignore.txt	Windows\system32\bin
wsSquid.ini	/etc/wsLib

Cancellazione della pianificazione dei backup

Argomenti correlati:

- Pianificazione del backup, pagina 302
- Esecuzione immediata dei backup, pagina 303
- Manutenzione dei file di backup, pagina 304
- Ripristino dei dati Websense, pagina 305
- *Opzioni di comando*, pagina 306

Per cancellare la pianificazione dei backup e interrompere l'esecuzione in corso dei backup, aprire il comando Shell e navigare alla directory bin di Websense (C:\Programmi\Websense\bin o opt/Websense/bin, per predefinizione). Digitare il seguente comando.

wsbackup -u

Opzioni di comando

Argomenti correlati:

- Pianificazione del backup, pagina 302
- Esecuzione immediata dei backup, pagina 303
- Manutenzione dei file di backup, pagina 304
- *Ripristino dei dati Websense*, pagina 305
- Cancellazione della pianificazione dei backup, pagina 306

Soltanto i membri principali (Linux) o i membri del gruppo di amministratori (Windows) possono gestire l'utilità di Backup.

Per visualizzare un elenco completo delle opzioni di comando dell'utility di Backup in qualsiasi momento, inserire:

```
wsbackup -h
oppure
wsbackup --help
```

Il comando wsbackup usa le opzioni seguenti:

- ♦ -b 0 --backup
- -d directory_path oppure --dir directory_path
- -f full_file_name or --file full_file_name
- ♦ -h oppure --help oppure -?

- ♦ -r oppure --restore
- ◆ -s *oppure* --schedule
- ♦ -t oppure --time
- ♦ -u oppure --unschedule
- -v *oppure* --verbose [0...3]

13 Amministrazione della creazione dei report

Argomenti correlati:

- *Pianificazione della configurazione*, pagina 310
- Gestione dell'accesso ai Reporting Tools., pagina 310
- Configurazione di base, pagina 311
- Utilità Configurazione di Log Server, pagina 316
- Amministrazione del database di registrazione, pagina 330
- Configurazione dei report investigativi, pagina 341
- *Attività utente*, pagina 346

Per usare le funzioni relative ai report di presentazione e ai report investigativi di Websense, occorre installare sia Websense Manager sia i componenti per la creazione dei report in un server Windows. Occorre anche configurare il software Websense in modo che registri le attività di filtraggio degli accessi in Internet.

La registrazione invia i record al database di registrazione di Websense che li inoltra ad un database di registrazione che deve essere installato in un motore di database supportato: Microsoft SQL Server Desktop Engine (a cui ci si riferisce in questo documento come MSDE) oppure Microsoft SQL Server Enterprise o Standard Editions (a cui ci si riferisce come Microsoft SQL Server). Per istruzioni sull'installazione dei componenti, vedere la *Guida all'installazione*.

Quando si genera un report, Websense Manager visualizza informazioni ricavate dal database di registrazione in base al filtro definito nel report.

Le organizzazioni che installano Websense Manager in un server Linux, o che preferiscono usare Linux per la creazione dei report, possono installare separatamente il prodotto Websense Explorer per Linux per generare i report. Questo prodotto funziona separatamente da Websense Manager. Vedere *Explorer for Linux Administrator's Guide* per informazioni sull'installazione e sull'uso del programma.

Pianificazione della configurazione

A seconda del volume di traffico Internet nella propria rete, le dimensioni del database di registrazione possono incrementare significativamente. Al fine di definire una strategia efficace di registrazione e creazione di report per la propria organizzazione, porsi le domande seguenti:

• Quando è più intenso il traffico di rete?

Cercare di pianificare i processi più laboriosi relativi al database e alla creazione di report quando il traffico è meno intenso. Questo migliorerà la performance della funzione di registrazione e di creazione di report durante i periodi di punta. Vedere *Configurazione delle opzioni sui tempi di navigazione in Internet*, pagina 334 e *Configurazione delle opzioni di manutenzione del database di registrazione*, pagina 335.

• Per quanto tempo si devono conservare i dati per disporre di una cronologia di report adeguata?

Valutare la possibilità di un'eliminazione automatica delle partizioni che hanno raggiunto una determinata età. Questo riduce la quantità di spazio su disco necessario al database di registrazione. Vedere *Configurazione delle opzioni di manutenzione del database di registrazione*, pagina 335.

• Quale livello di dettagli è effettivamente necessario?

Valutare le opzioni di registrazione da attivare: la registrazione di URL completi e dei relativi accessi aumenta le dimensioni del database di registrazione. Per ridurre le dimensioni del database di registrazione, considerare quanto segue:

- la disattivazione della registrazione di URL completi (vedere Configurazione della registrazione di URL completi, pagina 333)
- registrazione delle visite anziché degli accessi (vedere *Configurazione dei file cache di registro*, pagina 321)
- attivazione del consolidamento (vedere *Configurazione delle opzioni di consolidamento*, pagina 322)
- disattivazione della registrazione di alcune categorie (vedere *Configurazione* di Filtering Service per la registrazione, pagina 314)

Un'implementazione efficace della creazione dei report viene realizzata con un hardware che soddisfa o eccede i requisiti relativi al carico previsto e alla conservazione di dati storici.

Gestione dell'accesso ai Reporting Tools.

Se Websense Manager e i componenti per la creazione dei report sono installati nei server Windows, le opzioni di creazione dei report vengono visualizzate all'interno di Websense Manager e dell'utilità Log Server Configuration.

Se si installano i componenti per la creazione dei report, il Log Server viene collegato a un Policy Server specifico. Occorre selezionare quel Policy Server durante l'accesso a Websense Manager per poter accedere alle funzioni di creazione dei report. Se si accede a un Policy Server diverso, non sarà possibile accedere ai Report di presentazione e ai Report investigativi della scheda Principale o alla sezione Creazione report della scheda Impostazioni.

Nelle organizzazioni che usano soltanto l'account di accesso a Websense Administrator, tutti coloro che usano Websense Manager hanno accesso, dall'interno di Websense Manager, a tutte le opzioni di creazione dei report, compreso i report di presentazione e i report investigativi, nonché alle impostazioni degli strumenti di creazione dei report.

Nelle organizzazioni che usano un'amministrazione con delega, l'accesso agli strumenti di creazione dei report all'interno di Websense Manager è regolato da Websense Manager e dai membri con il ruolo di Super Administrator. Durante la creazione di un ruolo, il Super Administrator determina se quel ruolo debba avere accesso a specifiche opzioni di creazione dei report.

Vedere *Modifica dei ruoli*, pagina 261 per ulteriori informazioni sulla configurazione dell'accesso agli strumenti di creazioni dei report .

L'utilità Log Server Configuration è accessibile dal menu Start di Windows. Soltanto coloro che possono accedere al computer dell'installazione possono aprire questa utilità e modificare le impostazioni del Log Server. Vedere *Utilità Configurazione di Log Server*, pagina 316.

Se la propria organizzazione ha installato Websense Manager in un server Linux, o ha scelto il programma di creazione dei report Websense Explorer per Linux, anziché i componenti di creazione dei report eseguibili su Windows, le opzioni relative a tale funzione non vengono visualizzate in Websense Manager. I grafici relativi ai filtri di accesso a Internet non vengono visualizzati nelle pagine Oggi e Storia. Vedere la *Explorer for Linux Administrator's Guide* per informazioni sull'installazione di quel programma e sul suo uso per la creazione dei report.

Configurazione di base

Argomenti correlati:

- Configurazione di Filtering Service per la registrazione, pagina 314
- Assegnazione delle categorie alle classi di rischio, pagina 312
- Configurazione delle preferenze per la creazione dei report, pagina 314
- Utilità Configurazione di Log Server, pagina 316
- Amministrazione del database di registrazione, pagina 330

È possibile usare una serie di opzioni di configurazione per personalizzare la creazione dei report in funzione del proprio ambiente.

Websense Master Database raggruppa le categorie in **classi di rischio**. Le classi di rischio suggeriscono diversi tipi, o diversi livelli, di vulnerabilità associata ai siti appartenenti a tali categorie. Usare la pagina Generale > Classi di rischio, accessibile dalla scheda Impostazioni, per personalizzare le classi di rischio per la propria organizzazione. Vedere *Assegnazione delle categorie alle classi di rischio*, pagina 312.

Usare la pagina Preferenze > di creazione report, accessibile dalla scheda Impostazioni, per configurare il server e-mail usato per distribuire i report nonché per attivare la funzione Attività utente. Vedere *Configurazione delle preferenze per la creazione dei report*, pagina 314.

La registrazione è il processo di archiviazione in un database di registrazione delle informazioni relative alle attività di filtraggio in modo che sia possibile creare dei report.

Usare la pagina Generale > Registrazione, accessibile dalla scheda Impostazioni, per consentire la registrazione, selezionare le categorie da registrare e determinare le informazioni sull'utente che si vogliono registrare. Per ulteriori informazioni, vedere *Configurazione di Filtering Service per la registrazione*, pagina 314.

Usare l'utilità Log Server Configuration per gestire la modalità di elaborazione dei record di registrazione e per gestire i collegamenti al database di registrazione. Per ulteriori informazioni, vedere *Utilità Configurazione di Log Server*, pagina 316.

Usare la pagina Creazione report > Database di registrazione, accessibile dalla scheda Impostazioni, per gestire il database di registrazione, incluso i comandi relativi ai tempi di navigazione in Internet, le opzioni di partizione del database e i registri di errore. Per ulteriori informazioni, vedere *Amministrazione del database di registrazione*, pagina 330.

Assegnazione delle categorie alle classi di rischio

Argomenti correlati:

- *Classi di rischio*, pagina 41
- Pagine di blocco, pagina 87
- Utilizzo dei report per valutare i criteri di filtraggio, pagina 97

Websense Master Database raggruppa le categorie in **classi di rischio**. Le classi di rischio suggeriscono diversi tipi, o diversi livelli, di vulnerabilità associata ai siti appartenenti a tali categorie.

Le classi di rischio vengono utilizzate primariamente nella generazione dei report. Le pagine Oggi e Storia includono grafici che monitorano l'attività svolta in Internet in base alla classe di rischio ed è quindi possibile generare report di presentazione o report investigativi organizzati in base alla classe di rischio.

Gli utenti con qualifica totale di Super Administrator possono modificare le categorie assegnate a ciascuna classe di rischio dalla pagina **Impostazioni > Classi di rischio**. Ad esempio, alcune organizzazioni potrebbero includere i siti con video pubblicati dagli utenti che rientrano nelle classi di rischio di responsabilità legale, di riduzione della larghezza di banda delle rete e di riduzione della produttività. Tuttavia, se la propria organizzazione conduce ricerche di mercato su una certa fascia demografica, è da considerare l'inserimento di questi siti nella classe di rischio Utilizzo aziendale.

Nota

La pagina di blocco per la sicurezza viene visualizzata per i siti bloccati nelle categorie predefinite per la classe Rischio di sicurezza. Eventuali modifiche apportate alle categorie della classe Rischio di sicurezza incidono sulla creazione dei report, ma non incidono sulle pagine di blocco. Vedere *Pagine di blocco*, pagina 87.

Le informazioni sulle classi di rischio contenute nei report di Websense riflettono le assegnazioni definite in questa pagina.

- 1. Selezionare una voce dall'elenco Classi di rischio.
- 2. Esaminare l'elenco **Categorie** per vedere le categorie incluse correntemente in questa classe di rischio.

Un segno di spunta indica che la categoria è assegnata attualmente alla classe di rischio selezionata. L'icona W indica le categorie incluse per predefinizione in questa classe di rischio.

3. Selezionare o cancellare le voci dall'albero delle categorie per includere o escludere una categoria dalla classe di rischio selezionata. Le categorie possono appartenere a più di una classe di rischio.

Altre opzioni includono:

Opzione	Descrizione
Seleziona tutto	Consente di selezionare tutte le categorie dell'albero.
Cancella tutto	Consente di deselezionare tutte le categorie dell'albero.
Ripristina impostazioni predefinite	Consente di ripristinare le opzioni di categoria per la classe di rischio selezionata ai valori predefiniti del software Websense. Un'icona W blu indica una categoria predefinita.

- 4. Ripetere questa procedura per ciascuna classe di rischio.
- 5. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Configurazione delle preferenze per la creazione dei report

Argomenti correlati:

- *Attività utente*, pagina 346
- Pianificazione dei report di presentazione, pagina 112
- Pianificazione dei report investigativi, pagina 141

Quando si pianificano dei report di presentazione o dei report investigativi, da creare in seguito o in base a un ciclo a ripetizione, i report vengono distribuiti via e-mail a specifici destinatari. Usare la pagina **Preferenze** > **Creazione report** accessibile dalla scheda Impostazioni, per fornire informazioni chiave per questi messaggi e-mail.

Questa pagina viene anche usata per l'uso della funzione Attività utente in cui gli individui possono generare report investigativi sull'attività da loro condotta in Internet.

- 1. Inserire l'**Indirizzo e-mail** che deve apparire nel campo "Da" quando i report pianificati vengono distribuiti via email.
- 2. Inserire l'**IP o il nome del server SMPT** per il server e-mail usato per distribuire via e-mail i report pianificati.
- 3. Contrassegnare la casella di controllo **Consenti attività utente** affinché gli utenti finali possano accedere al Websense Manager e generare report investigativi sulla loro attività in Internet. Vedere *Attività utente*, pagina 346.
- 4. Fare clic su **OK** per inserire le modifiche nella cache.

Configurazione di Filtering Service per la registrazione

Argomenti correlati:

- Introduzione del database di registrazione, pagina 328
- Utilità Configurazione di Log Server, pagina 316

Usare la pagina **Generale > Registrazione** della scheda Impostazioni per fornire l'indirizzo IP e il numero di porta da usare per l'invio dei record di registro al Log Server. Questa pagina consente di selezionare le informazioni sull'utente e le categorie degli URL che Websense Filtering Service deve inviare al Log Server e rendere disponibili per la creazione dei report e degli avvisi sull'uso della categorie (vedere *Configurazione degli avvisi di utilizzo di una categoria*, pagina 296).

In un ambiente con molteplici Policy Server, configurare la pagina Generale > Registrazione separatamente per ciascuno di essi. Tutti i Filtering Service associati al Policy Server attivo inviano i loro record di registro al Log Server identificato in questa pagina. Se si usano molteplici Policy Server, tenere presente quanto segue:

- Se l'indirizzo IP e la porta del Log Server sono vuoti per un Policy Server, il Filtering Server associato a quel Policy Server non potrà registrare il traffico ai fini della generazione di report o avvisi.
- Ciascun Filtering Service registra il traffico in base alle impostazioni definite per il Policy Server a cui è collegato. Se si modificano le selezioni relative alle informazioni sull'utente e alla registrazione delle categorie per diversi Policy Server, i report generati per gli utenti associati a diversi Policy Server potrebbero apparire discordanti.

Se il proprio ambiente include sia molteplici Policy Server che molteplici Log Server, accertarsi di accedere ad ogni Policy Server separatamente e di verificare che il Policy Server stia comunicando con il Log Server corretto.

- 1. Per registrare informazioni di identificazione dei computer con accesso a Internet, selezionare **Registra indirizzi IP**.
- 2. Per registrare le informazioni di identificazione degli utenti che accedono a Internet, selezionare **Registra nomi utente.**

Nota

Se non si registrano gli indirizzi IP o i nomi utente, i report creati potrebbero non includere i dati sugli utenti. Ci si riferisce a volte a questa condizione come **registrazione anonima**.

3. Inserire l'indirizzo IP o il nome del computer in cui è installato Log Server nel campo **Indirizzo IP o nome Log Server**.

Importante

- Se Log Server è stato installato in un computer diverso da quello in cui è installato Policy Server, questa voce potrebbe adottare l'impostazione predefinita localhost. In questo caso, inserire l'indirizzo IP del computer con Log Server per consentire la visualizzazione sia dei grafici, nelle pagine Oggi e Storia, sia delle altre funzioni di creazione dei report.
- 4. Inserire il numero della Porta usata per inviare i record di registro a Log Server.
- 5. Fare clic su **Verifica stato** per determinare se Websense Manager sia in grado di comunicare con il Log Server specificato.

Un messaggio indica se la prova di collegamento è stata superata. Aggiornare l'indirizzo IP o il nome del computer e la porta, se necessario, fino a quando la prova non viene superata.

6. Fare clic sul pulsante **Registrazione categorie selettiva** per aprire l'area che indica le categorie di URL da registrare.

Le selezioni eseguite qui vengono applicate a tutti i filtri di categoria, in tutti i criteri attivi.



Nota

Se si disattiva la registrazione per le categorie in cui sono stati attivati gli avvisi sull'uso (vedere *Configurazione degli avvisi di utilizzo di una categoria*, pagina 296), nessun avviso potrà essere inviato.

I report non possono includere informazioni sulle categorie che non sono state registrate.

- a. Espandere o comprimere le categorie principali, come necessario, per visualizzare le categorie d'interesse.
- b. Selezionare ogni categoria da registrare contrassegnando la relativa casella di controllo.

Si dovrà selezionare o deselezionare ogni categoria separatamente. La selezione di una categoria principale non selezionerà automaticamente tutte le sotto-categorie. Usare **Seleziona tutto** e **Cancella tutto** per agevolare le selezioni.

7. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Utilità Configurazione di Log Server

Argomenti correlati:

- Gestione dell'accesso ai Reporting Tools., pagina 310
- Configurazione di base, pagina 311
- Chiusura e riavvio di Log Server, pagina 327

Durante l'installazione si possono configurare determinati aspetti delle operazioni di Log Server, incluso come Log Server deve interagire con i componenti del filtraggio di Websense.

L'utilità Configurazione di Log Server consente di modificare queste impostazioni, quando necessario, e di configurare altri dettagli relativi alle operazioni di Log Server. Questa utilità viene installata nello stesso computer in cui è installato Log Server.

 Dal menu Start di Windows, selezionare Programmi > Websense > Utilità > Configurazione di Log Server.

Viene visualizzata l'utilità Configurazione di Log Server.

2. Selezionare una scheda con le opzioni disponibili e apportare le modifiche necessarie a tali opzioni. Per istruzioni dettagliate, vedere .

- Configurazione delle connessioni di LogServer, pagina 317
- Configurazione delle opzioni del database Log Server, pagina 318
- Configurazione dei file cache di registro, pagina 321
- Configurazione delle opzioni di consolidamento, pagina 322
- Configurazione di WebCatcher, pagina 324
- 3. Fare clic su **Applica** per salvare le modifiche.
- 4. Usare la scheda **Connessione** per chiudere e riavviare Log Server in modo che le modifiche vengano applicate.

IMPORTANTE

Dopo aver apportato le modifiche necessarie alla scheda Configurazione di Log Server, fare clic su **Applica**. Occorre quindi chiudere e riavviare Log Server affinché le modifiche apportate vengano applicate. Per evitare di riavviare Log Server diverse volte, apportare tutte le modifiche necessarie alla Configurazione di Log Server prima di riavviarlo.

Configurazione delle connessioni di LogServer

Argomenti correlati:

- Utilità Configurazione di Log Server, pagina 316
- Configurazione delle opzioni del database Log Server, pagina 318
- Configurazione dei file cache di registro, pagina 321
- Configurazione delle opzioni di consolidamento, pagina 322
- Configurazione di WebCatcher, pagina 324
- Chiusura e riavvio di Log Server, pagina 327

La scheda **Connessione** dell'utilità Configurazione di Log Server contiene opzioni per la creazione e il mantenimento della connessione di Log Server con i componenti di filtraggio di Websense.

1. Accettare il numero predefinito della **Porta di input Log Server** (55805) oppure inserire il numero di un'altra porta disponibile.

Questa è la porta attraverso la quale Log Server comunica con Filtering Service. Il numero di porta inserito deve corrispondere al numero di porta inserito nella pagina Generale > Registrazione (scheda Impostazioni) di Websense Manager.

 Inserire un numero di ore nel campo Intervallo di aggiornamento Utente/ Gruppo per specificare la frequenza con la quale Log Server deve contattare il servizio di directory per gli aggiornamenti.

Log Server contatta il servizio di directory per ottenere informazioni aggiornate – come ad esempio il nome completo dell'utente e le assegnazioni di gruppo – relativamente agli utenti con un record nel database di registrazione.

Le attività di un utente il cui gruppo è cambiato, continuano a far parte del gruppo precedente fino all'aggiornamento successivo. Le organizzazioni che aggiornano di frequente il loro servizio di directory o hanno un vasto numero di utenti dovranno prendere in considerazione la definizione di un aggiornamento delle informazioni sugli utenti/gruppi più frequente delle 12 ore predefinite.

- 3. Fare clic su Applica per salvare le modifiche.
- 4. Usare il pulsante dell'area Stato del servizio per avviare Log Server tramite il comando **Avvia** o per interromperlo tramite il comando **Interrompi**. L'etichetta del pulsante cambia in funzione dell'azione che si verificherà quando si fa clic su di esso.



Le modifiche apportate all'utilità Configurazione di Log Server non entrano in effetto fino a quando non si chiude e non si riavvia il Log Server.

Configurazione delle opzioni del database Log Server

Argomenti correlati:

- Utilità Configurazione di Log Server, pagina 316
- Configurazione delle connessioni di LogServer, pagina 317
- Configurazione della connessione con il database, pagina 320
- Configurazione dei file cache di registro, pagina 321
- Configurazione delle opzioni di consolidamento, pagina 322
- Configurazione di WebCatcher, pagina 324
- Chiusura e riavvio di Log Server, pagina 327

Aprire la scheda **Database** dell'utilità Configurazione di Log Server per configurare il funzionamento di Log Server nei confronti del database di registrazione.

- 1. Scegliere un Metodo di inserimento registro dalle opzioni seguenti.
 - Open Database Connectivity (ODBC): Inserisce individualmente i record nel database, usando un driver di database per la gestione dei dati tra Log Server e il database di registrazione.
 - Bulk Copy Program (BCP) (opzione consigliata): Inserisce nel database di registrazione i record raggruppati che chiama "batch". Si consiglia di usare questa opzione in quanto è più efficace di un inserimento in ODBC.

Nota

L'opzione BCP è disponibile solo se si installa SQL Server Client Tools nel computer in cui è installato Log Server. 2. Fare clic su **Connessione** per selezionare il database di registrazione per l'archiviazione delle nuove informazioni di accesso a Internet da Websense. Vedere *Configurazione della connessione con il database*, pagina 320.

ODBC Data Source Name (DSN) e **Nome di accesso ODBC** visualizzano le impostazioni definite per la connessione con il database.

3. Se, al punto 1, si sceglie BCP come metodo di inserimento dei dati nel registro, definire le opzioni che seguono. Se si sceglie ODBC come metodo di inserimento dei dati nel registro, saltare il punto che segue.

Opzione	Descrizione
Percorso del file BCP	Il percorso della directory per l'archiviazione dei file BCP. Questo deve essere un percorso per il quale Log Server ha diritti di lettura e scrittura.
	Questa opzione è disponibile soltanto se Log Server è installato nel computer in cui è installato il database di registrazione o se i SQL Server Client Tools sono stati installati nel computer in cui è installato Log Server.
Frequenza di creazione file BCP	Il numero massimo di minuti che Log Server passa a sostituire i record di un file batch prima di chiudere quel file e di crearne uno nuovo.
	Questa impostazione funziona in combinazione con l'impostazione delle dimensioni del file batch: Log Server crea un nuovo file batch non appena si raggiunge uno dei due limiti.
Dimensione massima del batch BCP	Il numero massimo di record di registro prima che venga creato un nuovo file batch.
	Questa impostazione funziona in combinazione con l'impostazione relativa alla frequenza di creazione dei file cache: Log Server crea un nuovo file batch non appena si raggiunge uno dei due limiti.

- 4. Definire il numero **Massimo di connessioni consentite** per indicare il numero massimo di connessioni interne consentite tra Log Server e il motore del database. Le opzioni disponibili dipendono dal motore del database usato.
 - MSDE: Questo valore è predefinito su 4 e non può essere modificato.
 - SQL Server: Definire un numero da 4 a 50, in base alla propria licenza di SQL Server. Il numero minimo di connessioni dipende dal metodo di inserimento selezionato per le registrazioni.



Un numero di connessioni più alto, potrebbe aumentare non solo la frequenza di elaborazione dei record di registro, ma potrebbe anche avere un impatto su altri processi di rete che utilizzano lo stesso SQL Server. Nella maggior parte dei casi, si consiglia di definire un numero di connessioni inferiori a 20. Per l'assistenza necessaria, contattare l'amministratore del database. 5. Selezionare o deselezionare **Registrazione avanzata** per attivare o disattivare questa opzione che determina la modalità di ripresa delle registrazioni da parte di Log Server dopo un'interruzione.

Se questa opzione è deselezionata (impostazione predefinita) e Log Server è stato interrotto, inizierà la sua elaborazione dall'inizio del file di registro più vecchio nella cache. Ciò potrebbe causare la duplicazione di alcune voci nel database di registrazione, ma rende più rapida l'elaborazione da parte di Log Server.

Se questa opzione è selezionata, Log Server rileva il suo percorso nel file di registro attivo nella cache. Dopo un riavvio, Log Server riprende l'elaborazione dal punto di interruzione. L'opzione di registrazione avanzata può rallentare l'elaborazione eseguita da Log Server.

6. Fare clic su **Applica** per salvare le modifiche, quindi chiudere e riavviare il Log Server (vedere *Chiusura e riavvio di Log Server*, pagina 327).

Configurazione della connessione con il database

Argomenti correlati:

- Configurazione delle connessioni di LogServer, pagina 317
- Configurazione delle opzioni del database Log Server, pagina 318

Il pulsante **Connessione** della scheda Database dell'utilità Configurazione di Log Server consente di selezionare il database di registrazione per l'archiviazione delle informazioni in ingresso da Websense sull'accesso a Internet. Questa impostazione viene configurata automaticamente durante l'installazione, ma può venire modificata qualora sia necessario modificare il database per le registrazioni. (Il database deve essere stato installato per poter stabilire una connessione.)

- 1. Nella finestra di dialogo Data Source, selezionare la scheda Machine Data Source [Origine dati computer].
- 2. Selezionare la connessione ODBC per il database in cui vanno registrate le nuove informazioni.
- 3. Fare clic su **OK** per visualizzare la finestra di dialogo Accesso a SQL Server.
- 4. Se l'opzione **Usa connessione di tipo trusted** è disponibile, verificare che sia stata impostata correttamente per il proprio ambiente.

Utenti MSDE: Deselezionare l'opzione Connessione di tipo trusted.

Utenti di SQL Server: Per assistenza, contattare l'amministratore del database.

Nota

Se si usa una connessione di tipo trusted per le comunicazioni con il SQL Server, potrebbe essere necessario configurare diversi servizi Websense con un nome utente e una password di tipo trusted. Per ulteriori dettagli, vedere la *Installation Guide*.

- 5. Inserire l'**ID di accesso** e la **Password** definiti in fase di creazione del database. Normalmente sono lo stesso ID di accesso e la stessa password inseriti durante l'installazione di Log Server e durante la creazione del database.
- 6. Interrompere e riavviare Log Server tramite la scheda **Connessione** dopo aver apportato questa ed altre eventuali modifiche all'utilità Configurazione di Log Server.

Configurazione dei file cache di registro

Argomenti correlati:

- Utilità Configurazione di Log Server, pagina 316
- Configurazione delle connessioni di LogServer, pagina 317
- Configurazione delle opzioni del database Log Server, pagina 318
- Configurazione delle opzioni di consolidamento, pagina 322
- Configurazione di WebCatcher, pagina 324
- Chiusura e riavvio di Log Server, pagina 327

La scheda **Impostazioni** dell'utilità Configurazione di Log Server consente di gestire le opzioni di creazione del file cache di registro e di specificare se Log Server deve individuare i singoli file che compongono ogni sito Web richiesto o soltanto il sito Web.

- Inserire il percorso di archiviazione dei file cache di registro nel campo Percorso del file di registro. Il percorso predefinito è <directory installazione>\bin\Cache. (La directory di installazione predefinita è C:\Programmi\Websense\).
- 2. In **Frequenza di creazione del file cache**, indicare il numero massimo di minuti che Log Server deve passare per l'invio delle informazioni di accesso a Internet a un file cache di registro (**log***n***.tmp**) prima di chiuderlo e di creare un nuovo file.

Questa impostazione funziona in combinazione con le impostazioni sulle dimensioni: Log Server crea un nuovo file cache di registro non appena si raggiunge uno dei due limiti.

3. In **Dimensioni creazione del file cache**, specificare le dimensioni massime di un file cache di registro prima che Log Server chiuda e crei un nuovo file.

Questa impostazione funziona in combinazione con l'impostazione relativa alla frequenza di creazione dei file cache: Log Server crea un nuovo file cache di registro non appena si raggiunge uno dei due limiti.

4. Selezionare **Abilita visite** per creare un record di registro per ciascun sito Web visitato.



Se questa opzione è deselezionata, viene automaticamente creato un record di registro separato per ciascuna richiesta HTTP con visualizzati i diversi elementi della pagina, come ad esempio immagini grafiche e avvisi pubblicitari. Questa opzione prende anche il nome di registrazione accessi e crea un database di registrazione che cresce rapidamente.

Se questa opzione è selezionata, Log Server unifica i vari elementi che costituiscono la pagina Web (come ad esempio, immagini grafiche e avvisi pubblicitari) in un unico record di registro.

Se si è installato Websense Web Security Gateway, l'attività di scansione in tempo reale viene sempre registrata, nei report ad essa attinenti, come numero di accessi anche se l'opzione di registrazione delle visite è attivata. In questo caso, i numeri visualizzati nei report di filtraggio del Web, che includono il traffico bloccato da una scansione in tempo reale, saranno inferiori ai numeri presentati nei report di scansione in tempo reale.



Nota

È preferibile creare una nuova partizione del database prima di cambiare il metodo di registrazione da visite ad accessi. Per creare una nuova partizione del database, vedere la pagina Creazione report > Database di registrazione (scheda Impostazioni) in Websense Manager.

5. Fare clic su **Applica** per salvare le modifiche, quindi chiudere e riavviare Log Server (vedere *Chiusura e riavvio di Log Server*, pagina 327).

Configurazione delle opzioni di consolidamento

Argomenti correlati:

- Utilità Configurazione di Log Server, pagina 316
- Configurazione delle connessioni di LogServer, pagina 317
- Configurazione delle opzioni del database Log Server, pagina 318
- Configurazione dei file cache di registro, pagina 321
- Configurazione di WebCatcher, pagina 324
- Chiusura e riavvio di Log Server, pagina 327

Usare la scheda Consolidamento dell'utilità Configurazione di Log Server per attivare il consolidamento e definire le preferenze di consolidamento.



Nota

La gestione delle dimensioni del database di registrazione è un fattore importante da tenere presente nel caso di reti ad alto traffico. L'attivazione del consolidamento consente di monitorare le dimensioni e la crescita del database.

Il consolidamento riduce le dimensioni del database di registrazione in quanto unifica le richieste Internet che condividono gli elementi seguenti:

- Nome del dominio (ad esempio: www.websense.com)
- Categoria
- Parola chiave
- Azione (ad esempio: Categoria bloccata)
- Utente/stazione di lavoro

Minori sono le dimensioni del database, più rapida sarà la generazione dei report. Tuttavia, il consolidamento dei dati di registro riduce la precisione di alcuni report dettagliati, in quanto alcuni record associati allo stesso nome di dominio potrebbero andare persi.

Importante

L'attivazione del consolidamento potrebbe alterare la precisione di alcuni dati del report, come ad esempio i calcoli relativi ai tempi di navigazione in Internet.

1. Selezionare Consolida record di registrazione per attivare il consolidamento che unifica in un singolo record di registro, richieste simili di accesso in Internet.

Quando questa opzione è deselezionata (per predefinizione), il database di registrazione conserva tutti i dettagli sugli accessi o sulle visite di ogni richiesta di accesso ad Internet (in base alla selezione effettuata nella scheda Impostazioni, vedere *Configurazione dei file cache di registro*, pagina 321). Questo consente l'inclusione di maggiori dettagli nei report generati, ma comporta anche dimensioni più grandi del database di registrazione.

La selezione di questa opzione crea un database di registrazione più piccolo con un livello inferiore di dettagli nei report.

Importante

Per garantire dei report standardizzati, considerare la possibilità di creare una nuova partizione del database ogni volta che si attiva o si disattiva il consolidamento. Accertarsi inoltre di creare i report da partizioni che condividono la stessa impostazione di consolidamento.

Se si è installato Websense Web Security Gateway, l'attività di scansione in tempo reale viene sempre registrata, nei report ad essa attinenti, come numero di accessi distinti anche se l'opzione di consolidamento è attivata. In questo caso, i numeri visualizzati nei report di filtraggio del Web che includono un traffico bloccato da una scansione in tempo reale, saranno inferiori ai numeri presentati nei report di scansione in tempo reale.

2. In **Durata consolidamento**, specificare il tempo massimo che deve intercorrere tra il primo e l'ultimo record da consolidare.

Questo rappresenta la massima differenza di tempo tra i record più recenti e meno recenti che sono stati unificati al fine di creare un record consolidato.

Ridurre l'intervallo per incrementare i dettagli dei report creati. Incrementare l'intervallo per massimizzare il consolidamento. Tenere presente che un intervallo maggiore può anche incrementare l'uso delle risorse del sistema, come ad esempio memoria, CPU e spazio su disco.

Se si attiva l'opzione URL completo nella pagina Creazione report > Database di registrazione (scheda Impostazioni) di Websense Manager, il record di registro consolidato conterrà il percorso completo (fino a 255 caratteri) del primo sito con quello stesso percorso che Log Server incontra.

Ad esempio, supponiamo che un utente abbia visitato i siti seguenti e che tutti siano stati categorizzati nella categoria Acquisti in linea.

- www.dominio.it/acquistiscarpe
- www.dominio.it/acquistipelletteria
- www.domain.it/acquistigioielli

Con l'opzione di URL completo attivata, il consolidamento creerebbe una singola voce di registro sotto l'URL www.dominio.it/acquistiscarpe.

3. Fare clic su **Applica** per salvare le modifiche, quindi chiudere e riavviare Log Server (vedere *Chiusura e riavvio di Log Server*, pagina 327).

Configurazione di WebCatcher

Argomenti correlati:

- Utilità Configurazione di Log Server, pagina 316
- Configurazione delle connessioni di LogServer, pagina 317
- Configurazione delle opzioni del database Log Server, pagina 318
- Configurazione dei file cache di registro, pagina 321
- Configurazione delle opzioni di consolidamento, pagina 322
- Configurazione di WebCatcher, pagina 324
- *Autenticazione di WebCatcher*, pagina 327
- Chiusura e riavvio di Log Server, pagina 327
WebCatcher è una funzione opzionale che raccoglie URL non riconosciuti e URL di sicurezza e li invia a Websense, Inc, dove vengono analizzati per rischi potenziali relativi a sicurezza e responsabilità civile nonché per la loro categorizzazione. (La registrazione di un URL completo non è necessaria per l'elaborazione da parte di WebCatcher.) Websense, Inc. valuta le informazioni raccolte e aggiorna il Master Database aggiungendovi gli URL appena categorizzati ed ottenendo in tal modo un miglioramento dell'azione dei filtri.

Scegliere i tipi di URL da inviare ed impostare le dimensioni dei file e i tempi di elaborazione nella scheda di **WebCatcher** dell'utilità Configurazione di Log Server.

Nota

In un ambiente con diversi Log Server, Web Catcher viene attivato per un Log Server soltanto. Una volta attivato, questa scheda non sarà più disponibile quando si usa lo strumento Configurazione di Log Server per le altre istanze di Log Server.

Le informazioni inviate a Websense, Inc. contengono soltanto gli URL e non includono informazioni sull'utente.

L'esempio seguente riporta le informazioni che verrebbero inviate a seguito dell'attivazione di WebCatcher. L'indirizzo IP di questo esempio riflette l'indirizzo del computer che funge da host dell'URL, non l'indirizzo IP del richiedente.

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP ADDR="200.102.53.105" NUM HITS="1" />
```

I dati di WebCatcher vengono inviati a Websense, Inc., via HTTP Post. È possibile creare dei ruoli o apportare altre modifiche al server proxy o al firewall per consentire il traffico HTTP in uscita. Fare riferimento alla documentazione del server proxy e del firewall per istruzioni.

- 1. Selezionare una delle opzioni seguenti:
 - L'opzione Sì, invia soltanto gli URL specificati a Websense attiva l'elaborazione di WebCatcher. Occorre indicare l'URL che si vuole inviare. Procedere quindi al punto 2.
 - No, non inviare informazioni a Websense disattiva l'elaborazione di WebCatcher. Se si sceglie questa opzione, non è necessario inserire un'altra voce.
- 2. Selezionare **Invia URL non categorizzati** per inviare un elenco di tutti gli URL non categorizzati e identificati nel database di registrazione.

Websense Inc. analizza gli URL non categorizzati che riceve e li aggiunge alle categorie del Master Database, se necessario. Ciò migliora la precisione dell'azione dei filtri per tutte le organizzazioni.



Nota I siti di Intranet non vengono inviati da WebCatcher. Ciò include tutti i siti con indirizzi IP all'interno dei seguenti intervalli: 10.xxx.xxx, 172.16.xxx.xxx e 192.168.xxx.xxx.

3. Selezionare **Invio di URL di sicurezza** per inviare un elenco di tutti gli URL di sicurezza che sono stati identificati nel database di registrazione.

Gli URL di sicurezza vengono analizzata da Websense, Inc per determinare l'attività dei siti inclusi nelle categorie keylogging, siti Web dannosi, Phishing, altri tipi di frodi e spyware.

- 4. In Selezionare un paese/regione che identifichi la posizione dell'utente, selezionare il paese in cui si registra la maggior parte delle attività.
- 5. Selezionare l'opzione **Salvare una copia dei dati inviati a Websense** per salvare una copia dei dati da inviare a Websense, Inc..

Quando questa opzione è attivata, WebCatcher salva i dati come file XML non cifrati nella directory Websense\Reporter. Questi file riportano il timbro di data e ora.

6. In **Dimensione massima del file caricato**, indicare il limite massimo delle dimensioni del file (da 4096 KB a 8192 KB) prima di inviarlo a Websense.

Accertarsi che il sistema possa inviare un file di queste dimensioni via HTTP Post.

7. In **Ora di inizio quotidiana minima**, definire l'ora di inizio alla quale Web Catcher deve inviare il file se la soglia delle dimensioni massime non è stata raggiunta quel giorno.

Questo garantisce che le informazioni vengano inviate e cancellate dal sistema almeno una volta al giorno.

8. Fare clic sul pulsante **Autenticazione** se il computer in cui è installato Log Server deve autenticare l'accesso a Internet.

Vedere *Autenticazione di WebCatcher*, pagina 327 per informazioni sulla finestra di dialogo **Autenticazione** visualizzata.

9. Fare clic su **Applica** per salvare le modifiche, quindi chiudere e riavviare Log Server (vedere *Chiusura e riavvio di Log Server*, pagina 327).

Autenticazione di WebCatcher

Argomenti correlati:

- Utilità Configurazione di Log Server, pagina 316
- *Configurazione di WebCatcher*, pagina 324
- Chiusura e riavvio di Log Server, pagina 327

La finestra di dialogo Autenticazione viene visualizzata dopo aver fatto clic su **Autenticazione** nella scheda WebCatcher.

1. Selezionare l'opzione **Usa un server proxy** se il computer in cui è installato Log Server accede a Internet tramite un server proxy e quindi fornire le informazioni che seguono.

Campo	Descrizione
Nome server proxy	Inserire l'indirizzo IP o il nome del server proxy tramite il quale Log Server accede a Internet.
Porta server proxy	Inserire il numero di porta attraverso la quale il server proxy comunica.

- 2. Selezionare l'opzione **Utilizza autenticazione di base** se il computer in cui è installato Log Server deve autenticare l'accesso a Internet e quindi inserire il nome utente e la password per la necessaria autenticazione.
- 3. Fare clic su **OK** per salvare le modifiche e per ritornare alla scheda WebCatcher.

Chiusura e riavvio di Log Server

Argomenti correlati:

- Utilità Configurazione di Log Server, pagina 316
- Configurazione delle connessioni di LogServer, pagina 317

Log Server riceve le informazioni da Filtering Service e le salva nel database di registrazione in modo da poterle usare quando genera i report. Viene eseguito come un servizio Windows, la prima volta durante l'installazione, e quindi ad ogni riavvio del computer.

Le modifiche apportate all'utilità Configurazione di Log Server entrano in effetto soltanto dopo aver chiuso e riavviato Log Server. Per questo, usare semplicemente la scheda Connessione dell'utilità Configurazione di Log Server.

- 1. Dal menu Start di Windows, selezionare **Programmi > Websense > Utilità > Configurazione di Log Server**.
- 2. Nella scheda Connessioni, fare clic su Interrompi.
- 3. Attendere diversi secondi e fare quindi clic su **Avvia** per riavviare il servizio di Log Server.
- 4. Fare clic su OK per chiudere l'utilità Configurazione di Log Server.

Nota

Websense non può eseguire un accesso a Internet se Log Server è chiuso.

Introduzione del database di registrazione

Argomenti correlati:

- Processi del database, pagina 329
- Amministrazione del database di registrazione, pagina 330

Log Database archivia i record dell'attività svolta in Internet e le relative azioni di filtraggio di Websense. L'installazione crea il database di registrazione con un database del catalogo e una partizione del database.

Il **database del catalogo** consente un unico punto di accesso per i vari componenti di Websense che necessitano di accedere al database di registrazione: Pagine dello stato, Log Server, report di presentazione e report investigativi. Contiene informazioni di supporto per le partizioni del database, incluso l'elenco dei nomi delle categorie, le definizioni delle classi di rischio, la mappa degli utenti in relazione ai gruppi, i processi del database e così via. Il database del catalogo mantiene anche un elenco di tutte le partizioni disponibili del database.

Le **Partizioni del database** archiviano i singoli record di registro delle attività svolte in Internet. Per gli utenti MSDE, vengono create nuove partizioni in funzione delle regole di rollover in base alle dimensioni stabilite da Websense. Gli utenti di Microsoft SQL Server possono configurare il database di registrazione per iniziare una nuova partizione in base alle dimensioni delle partizioni o a un intervallo di date (vedere *Configurazione opzioni di rollover*, pagina 331 per ulteriori informazioni).

Nota

Le partizioni basate sulla data sono disponibili soltanto se il software Websense usa Microsoft SQL Server come un motore di database.

Se le partizioni sono basate sulle dimensioni, tutti i record di registro in entrata vengono inseriti nella partizione attiva più recente che soddisfa la regola definita per

le dimensioni. Se la partizione raggiunge le dimensioni massime definite, viene creata una nuova partizione per l'inserimento di nuovi record di registro.

Se le partizioni sono basate sulla data, vengono create nuove partizioni in base al ciclo stabilito. Ad esempio, se l'opzione di rollover è mensile, viene creata una nuova partizione non appena i record vengono ricevuti il mese successivo. I record di registro in entrata vengono inseriti nella partizione appropriata in base alla data.

Le partizioni del database offrono flessibilità e vantaggi in termini di performance. Ad esempio, è possibile generare report da un'unica partizione per limitare l'ambito dei dati che occorre analizzare per individuare le informazioni richieste.

Processi del database

I processi del database vengono installati insieme al database di registrazione. SQL Server Agent deve essere in esecuzione nel computer in cui è in esecuzione il motore del database (MSDE o Microsoft SQL Server).

- Il processo di estrazione, trasformazione e caricamento dei dati (ETL) rimane in costante esecuzione, riceve i dati da Log Server e quindi li inserisce nella partizione del database. Il processo ETL deve essere in esecuzione affinché i record di registro possano venire elaborati nel database di registrazione.
- Il processo di manutenzione del database esegue attività di manutenzione e garantisce una performance ottimale. Per impostazione predefinita, questo processo viene eseguito normalmente di notte.
- Il processo relativo al tempo di navigazione in Internet (Internet Browse Time IBT) analizza i dati ricevuti e calcola il tempo di navigazione per ciascun client. Il processo IBT fa un uso intenso di risorse ed agisce sulla maggior parte delle risorse di database. Per impostazione predefinita, questo processo viene eseguito normalmente di notte.

Alcuni aspetti di questi processi di database possono venire configurati nella pagina Impostazioni > Database di registrazione Per ulteriori informazioni, vedere *Impostazioni dell'amministrazione del database di registrazione*, pagina 330.

Quando si configura il tempo d'inizio del processo di manutenzione e del processo di misurazione del tempo di navigazione in Internet, occorre tenere presente le risorse del sistema e il traffico di rete. Questi processi fanno un uso intenso di risorse e potrebbero rallentare la registrazione e la creazione dei report.

Amministrazione del database di registrazione

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione opzioni di rollover, pagina 331
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334
- Configurazione della registrazione di URL completi, pagina 333
- Configurazione delle opzioni di manutenzione del database di registrazione, pagina 335
- Configurazione della creazione delle partizioni del database di registrazione, pagina 338
- Configurazione delle partizioni disponibili, pagina 339
- Visualizzazione dei registri di errore, pagina 340

L'amministrazione del database di registrazione comporta il monitoraggio e il controllo di molti aspetti delle operazioni del database, tra cui:

- Le operazioni svolte dai processi del database e i tempi di esecuzione.
- Le condizioni per la creazione di nuove partizioni del database.
- Le partizioni che sono disponibili per la creazione dei report.

Queste e altre opzioni danno alla persona che amministra il database di registrazione un controllo significativo. Vedere *Impostazioni dell'amministrazione del database di registrazione*, pagina 330.

Il Super Administrator designa le persone che possono amministrare il database di registrazione quando si creano dei ruoli. Vedere *Modifica dei ruoli*, pagina 261.

Nota

È consigliabile limitare il numero di amministratori autorizzati a modificare le impostazioni del database di registrazione

Impostazioni dell'amministrazione del database di registrazione

Argomenti correlati:

• Amministrazione del database di registrazione, pagina 330

La pagina **Creazione report > Database di registrazione** a cui si può accedere dalla scheda Impostazioni, consente di gestire vari aspetti delle operazioni del Database di registrazione. Le opzioni vengono raggruppate in sezioni logiche che vengono descritte separatamente.

Per attivare le modifiche apportate a quella sezione, fare clic sul pulsante Salva ora, disponibile in quella sezione. Facendo clic su **Salva ora** si salvano immediatamente le modifiche apportate a quella sezione. (Non è necessario fare anche clic su Salva tutto.)

L'area superiore della pagina visualizza sia il nome del database di registrazione attivo sia il collegamento **Aggiorna**. Il collegamento Aggiorna visualizza ancora le informazioni inserite nella pagina del database di registrazione. Qualsiasi modifica non applicata tramite il pulsante Salva ora andranno perse.

Per ulteriori istruzioni sull'uso di ciascuna sezione, fare clic sul relativo collegamento qui sotto.

- Opzioni rollover database: *Configurazione opzioni di rollover*, pagina 331.
- Registrazione URL completo *Configurazione della registrazione di URL completi*, pagina 333.
- Configurazione del tempo di navigazione in Internet *Configurazione delle opzioni* sui tempi di navigazione in Internet, pagina 334.
- Configurazione manutenzione *Configurazione delle opzioni di manutenzione del database di registrazione*, pagina 335.
- Creazione partizioni database: *Configurazione della creazione delle partizioni del database di registrazione*, pagina 338.
- Partizioni disponibili: Configurazione delle partizioni disponibili, pagina 339.
- Attività registro errori: Visualizzazione dei registri di errore, pagina 340.

Configurazione opzioni di rollover

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334
- Configurazione della registrazione di URL completi, pagina 333
- *Configurazione delle opzioni di manutenzione del database di registrazione*, pagina 335
- Configurazione della creazione delle partizioni del database di registrazione, pagina 338
- Configurazione delle partizioni disponibili, pagina 339
- Visualizzazione dei registri di errore, pagina 340

Usare la sezione **Opzioni rollover database** della pagina Creazione report > Database di registrazione (scheda Impostazioni) per specificare quando si vuole che il Log Database crei un nuova partizione del database (rollover).

1. Usare le opzioni **Esegui rollover ogni** per indicare se le partizioni del database devono eseguire un rollover in base alle dimensioni (MB) o alla data (settimane o mesi), a seconda del motore del database usato.

Gli utenti MSDE devono usare l'opzione di rollover in base alle dimensioni. Gli utenti di Microsoft SQL Server possono scegliere tra dimensioni o data.

- Per i rollover in base alla data, selezionare settimane o mesi come unità di misura e specificare quante settimane o quanti mesi di calendario si vogliono tenere in una partizione del database prima di crearne una nuova.
- Per i rollover basati sulle dimensioni, selezionare MB e specificare il numero di megabyte che il database deve raggiungere prima che inizi il rollover.

Gli utenti di **Microsoft SQL Server** possono definire delle dimensioni superiori fino a 204800 MB.

Gli utenti **MSDE** devono definire delle dimensioni comprese tra 100 MB e 1536 MB.



Nota

Se il rollover inizia durante un periodo di punta della giornata, la performance potrebbe rallentare durante il processo di rollover.

Per evitare questa possibilità, alcuni ambienti scelgono di definire il rollover automatico in base a un lungo periodo di tempo o ad alte dimensioni. Eseguono quindi rollover manuali normali per impedire il rollover automatico. Per ulteriori informazioni sui rollover manuali, vedere *Configurazione della creazione delle partizioni del database di registrazione*, pagina 338.

Tenere presente che non si sta consigliando di creare delle partizioni di grandi dimensioni. La performance della funzione di creazione dei report può rallentare se i dati non vengono divisi in varie partizioni di più piccole dimensioni.

Quando si crea la partizione del database, la creazione dei report viene automaticamente attivata per la partizione (vedere *Configurazione delle partizioni disponibili*, pagina 339).

2. Fare clic su **OK** per attivare le modifiche apportate alle opzioni di rollover del database.

Configurazione della registrazione di URL completi

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione opzioni di rollover, pagina 331
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334
- Configurazione delle opzioni di manutenzione del database di registrazione, pagina 335
- Configurazione della creazione delle partizioni del database di registrazione, pagina 338
- Configurazione delle partizioni disponibili, pagina 339
- Visualizzazione dei registri di errore, pagina 340

La sezione **Registrazione URL completo** della pagina Creazione report > Database di registrazione (scheda Impostazioni) consente di definire quale parte dell'URL deve venire registrata per ciascuna richiesta Internet.

Nota

La gestione delle dimensioni del database di registrazione è un fattore importante da tenere presente nel caso di reti ad alto traffico. La disattivazione dell'opzione di registrazione degli URL completi è un metodo per mantenere sotto controllo le dimensioni e la crescita del database.

1. Selezionare **Registra URL completo per ogni sito richiesto** per registrare l'intero URL incluso il dominio (www.dominio.it) e il percorso a quella pagina particolare (/prodotti/productA.html).



Importante

Attivare la registrazione degli URL completi se si intende generare report sull'attività di scansione in tempo reale (vedere *Creazione di report sull'attività di scansione in tempo reale*, pagina 158). In caso contrario, i report includeranno soltanto il dominio (ww.dominio.it) del sito categorizzato anche se le pagine individuali del sito potrebbero rientrare in categorie diverse o contenere diversi tipi di minacce.

Se questa opzione non viene selezionata, vengono registrati soltanto i nomi del dominio. Questa scelta comporta un database di dimensioni inferiori ma consente l'inclusione di meno dettagli.

La registrazione di URL completi genera un database di registrazione di più grandi dimensioni ma fornisce informazioni più dettagliate.

Se si attiva la registrazione di un URL completo con attivata l'opzione di consolidamento, il record consolidato conterrà l'URL completo dal primo record del gruppo di consolidamento. Per ulteriori informazioni, vedere *Configurazione delle opzioni di consolidamento*, pagina 322.

2. Fare clic su **Salva ora** per attivare le modifiche apportate alle opzioni di registrazione degli URL completi.

Configurazione delle opzioni sui tempi di navigazione in Internet

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione opzioni di rollover, pagina 331
- Configurazione della registrazione di URL completi, pagina 333
- Configurazione delle opzioni di manutenzione del database di registrazione, pagina 335
- Configurazione della creazione delle partizioni del database di registrazione, pagina 338
- Configurazione delle partizioni disponibili, pagina 339
- Visualizzazione dei registri di errore, pagina 340

I report sui tempi di navigazione in Internet (IBT) riportano i dati relativi al tempo che gli utenti passano in Internet. Un processo di database eseguito di notte calcola i tempi di navigazione di ciascun client in base ai nuovi record di registro ricevuti quel giorno. Impostare le opzioni relative ai tempi di navigazione nella sezione **Configurazione tempo di navigazione Internet** della pagina Impostazioni > Database di registrazione.

1. Scegliere un'Ora inizio processo per il processo di database relativo a IBT.

I tempi e le risorse del sistema necessari per questo processo variano a seconda del volume dei dati registrati ogni giorno. È meglio eseguire questo processo ad un'ora diversa dal processo di manutenzione notturna (vedere *Configurazione delle opzioni di manutenzione del database di registrazione*, pagina 335) e selezionare un periodo di tempo di rete con poco traffico per ridurre al minimo l'impatto esercitato sulla generazione dei report.

Il processo IBT fa un uso intenso di risorse ed agisce sulla maggior parte delle risorse di database. Se si attiva questo processo, definire il tempo d'inizio in modo che non interferisca con la capacità del sistema di elaborare i report pianificati ed altre importanti operazioni. Monitorare inoltre il processo in corso per determinare se è necessario disporre di un hardware più potente per soddisfare tutti i requisiti relativi all'elaborazione.

2. In **Soglia durata lettura**, definire un numero medio di minuti per la lettura di un sito Web specifico.

La soglia del tempo di lettura definisce le sessioni di navigazione al fine della creazione dei report sui tempi di navigazione in Internet. L'apertura di un browser genera il traffico HTTP. Questo rappresenta l'inizio di una sessione di navigazione . La sessione rimane aperta finché il traffico HTTP viene generato in modo continuativo nell'ambito del periodo di tempo stabilito. La sessione di navigazione viene considerata chiusa una volta che questo periodo di tempo passa senza traffico HTTP. Una nuova sessione di navigazione inizia non appena il traffico HTTP viene rigenerato.

Nota

Si consiglia di modificare la Soglia tempo di lettura il più raramente possibile e di iniziare un nuova partizione di database ogni volta che si apporta una modifica.

Per evitare dati discrepanti nei report, generare dei report IBT dalle partizioni del database che usano lo stesso valore di Soglia tempo di lettura.

Tenere presente che alcuni siti Web usano una tecnica di aggiornamento automatico per aggiornare frequentemente le informazioni. Un esempio è un sito di notizie che visualizza a rotazione le notizie più recenti. Questo tipo di aggiornamento genera un nuovo traffico HTTP. Se quindi si lascia aperto questo tipo di sito, vengono generati nuovi record di registro ogni volta che il sito viene aggiornato. Se non si verificano intervalli nel traffico http, la sessione di navigazione non viene chiusa.

3. Definire un valore di **Ultima durata lettura** per tener conto del tempo passato a leggere l'ultimo sito Web prima della fine di una sessione di navigazione.

Quando l'interruzione nei tempi di traffico HTTP supera la soglia del tempo di lettura, la sessione viene chiusa e il valore Ultima durata lettura viene aggiunto alla durata della sessione.

4. Fare clic su **Salva ora** per attivare le modifiche apportate alla configurazione dei tempi di navigazione.

Configurazione delle opzioni di manutenzione del database di

registrazione

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione opzioni di rollover, pagina 331
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334
- Configurazione della registrazione di URL completi, pagina 333
- Configurazione della creazione delle partizioni del database di registrazione, pagina 338
- Configurazione delle partizioni disponibili, pagina 339
- Visualizzazione dei registri di errore, pagina 340

Usare la sezione **Configurazione manutenzione** della pagina Creazione report > Database di registrazione (scheda Impostazioni) per mantenere il controllo di determinati aspetti dell'elaborazione eseguita dal database, come ad esempio l'ora di esecuzione del processo di manutenzione, alcune delle attività svolte, la cancellazione delle partizioni del database e i registri di errore.

1. In **Ora inizio manutenzione**, selezionare l'ora del giorno per l'esecuzione del processo di manutenzione del database.

I tempi e le risorse del sistema necessari per questo processo variano a seconda delle attività selezionate in questa area. Per ridurre al minimo l'impatto su altre attività e sistemi, si consiglia di eseguire questo processo in periodi di traffico di rete lenti, diversi dall'ora definita per l'attività IBT (vedere *Configurazione delle opzioni sui tempi di navigazione in Internet*, pagina 334).

2. Selezionare Elimina automaticamente le partizioni quando tutti i giorni della partizione sono precedenti a questo numero di giorni e specificare quindi un numero di giorni (da 2 a 365) dopo i quali le partizioni devono venire eliminate.



Attenzione

Dopo aver eliminato una partizione, i relativi dati non possono più essere recuperati. Vedere *Configurazione delle partizioni disponibili*, pagina 339 per una metodo alternativo di eliminazione delle partizioni.

3. Selezionare Abilita reindicizzazione automatica delle partizioni quando necessario su e selezionare quindi un giorno della settimana in cui si vuole che questa elaborazione venga eseguita automaticamente ogni settimana.

La reindicizzazione del database è importante per mantenere l'integrità del database e per ottimizzare la velocità di creazione dei report.



Importante

È preferibile eseguire questa elaborazione durante un periodo di poco traffico su rete. La reindicizzazione delle partizioni del database usa molte risorse ed è un processo laborioso in termini di tempo. Si consiglia di non generare report durante questo processo.

4. Selezionare **Numero di giorni prima di eliminare i batch errati** ed inserire quindi un numero di giorni (da 0 a 90) dopo i quali i batch errati vanno eliminati.

Se questa opzione non è selezionata, i batch errati vengono conservati per un periodo di tempo indefinito ai fini di un'elaborazione futura.

Se esiste uno spazio su disco sufficiente o dei permessi di accesso al database non adeguati per inserire i record di registro nel database, i record vengono contrassegnati come **batch errati**. Normalmente, questi batch vengono rielaborati e inseriti con successo nel database durante il processo di manutenzione notturna del database.

Tuttavia questa rielaborazione non può venire completata se i problemi di spazio su disco o i problemi di autorizzazione non sono stati risolti. Se l'opzione **Elabora i batch non eseguiti** non è selezionata, i batch non eseguiti non verranno rielaborati. Essi verranno automaticamente eliminati dopo il periodo di tempo specificato.

5. Selezionare **Elabora i batch non eseguiti** affinché il processo di manutenzione notturna del database rielabori i batch errati.

Se questa opzione non è selezionata, i batch errati non verranno mai più elaborati. Verranno eliminati dopo il periodo di tempo specificato.

6. Selezionare **Numero di giorni prima dell'eliminazione del registro di errori** ed inserire quindi un numero di giorni (da 0 a 90) dopo i quali i record di errore del database vanno eliminati dal database del catalogo.

Se questa opzione non è selezionata, i registri di errore vengono conservati indefinitamente.

7. Fare clic su **Salva ora** per attivare le modifiche apportate alle opzioni di configurazione della manutenzione .

Configurazione della creazione delle partizioni del database di registrazione

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione opzioni di rollover, pagina 331
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334
- Configurazione della registrazione di URL completi, pagina 333
- Configurazione delle opzioni di manutenzione del database di registrazione, pagina 335
- Configurazione delle partizioni disponibili, pagina 339
- Visualizzazione dei registri di errore, pagina 340

Usare la sezione **Creazione partizioni** del database della pagina Creazione report > Database di registrazione (scheda Impostazioni) per definire le caratteristiche di nuove partizioni del database, come ad esempio il percorso e le opzioni delle dimensioni. Quest'area consente anche di creare subito una nuova partizione piuttosto che attendere il rollover pianificato (vedere *Configurazione opzioni di rollover*, pagina 331).

- 1. Inserire il **Percorso file** per creare sia i file dei **Dati** e i file di **Registro** per le nuove partizioni del database.
- In Dimensioni iniziale definire le dimensioni iniziali del file (da 100 a 204800 MB) sia per i file Dati che per i file di Registro per le nuove partizioni del database.

Utenti di Microsoft SQL Server : L'intervallo accettabile va da 100 a 204800 Utenti MSDE: L'intervallo accettabile va da 100 a 1500

Nota

Le migliori pratiche raccomandano il calcolo delle dimensioni medie delle partizioni nell'arco di un determinato periodo di tempo. Aggiornare quindi le dimensioni iniziali in base a quel valore. Questo approccio minimizza il numero di volte in cui la partizione deve venire estesa e libera le risorse necessarie per l'elaborazione dei dati nell'ambito delle partizioni.

3. In **Crescita**, definire l'incremento in base al quale occorre aumentare le dimensioni, in megabytes (MB), dei file **Dati** e **Registro** di una partizione quando è necessario disporre di ulteriore spazio.

Utenti di Microsoft SQL Server: l'intervallo accettabile va da 1 a 999999 **Utenti MSDE**: l'intervallo accettabile va da 1 a 450 4. Fare clic su **Salva ora** per implementare le modifiche apportate a percorso, dimensioni e crescita.

Le partizioni del database create dopo aver apportato queste modifiche utilizzano le nuove impostazioni.

5. Fare clic su **Crea ora** per creare una nuova partizione la prossima volta che il processo ETL viene eseguito (vedere *Processi del database*, pagina 329), indipendentemente dalle impostazioni di rollover automatico. Questo processo richiede normalmente pochi minuti.

Affinché le partizioni usino le modifiche apportate in questa sezione, fare clic su **Salva ora** prima di fare clic su **Crea ora**.

Fare clic periodicamente sul pulsante Aggiorna del riquadro del contenuto. L'area delle Partizioni disponibili visualizzerà la nuova partizione una volta che il processo di creazione è stato completato.

Configurazione delle partizioni disponibili

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione opzioni di rollover, pagina 331
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334
- Configurazione della registrazione di URL completi, pagina 333
- Configurazione delle opzioni di manutenzione del database di registrazione, pagina 335
- Configurazione della creazione delle partizioni del database di registrazione, pagina 338
- Visualizzazione dei registri di errore, pagina 340

La sezione **Partizioni disponibili** della pagina Creazione report > Database di registrazione (scheda Impostazioni) elenca tutte le partizioni disponibili per la creazione di report. L'elenco visualizza le date coperte nonché le dimensioni e il nome di ciascuna partizione.

Usare questo elenco per determinare le partizioni del database da includere nei report e per selezionare le singole partizioni da eliminare.

1. Selezionare Abilita accanto alle partizioni che si vogliono includere nei report.

Usare le opzioni **Seleziona tutte** e **Nessuna** disponibili sopra l'elenco, se necessario.

È necessario attivare almeno una partizione ai fini della creazione dei report. Usare l'opzione **Nessuna** per disattivare tutte le partizioni simultaneamente in modo da poterne attivare soltanto alcune. Usare queste opzioni per gestire i dati da analizzare, quando si generano dei report, e per rendere più rapida la loro elaborazione. Ad esempio, se si pianifica di generare una serie di report per giugno, deselezionare tutte le partizioni ad eccezione di quelle con la data di giugno.

Importante

- Questa selezione incide sui report pianificati e sui report eseguiti in modo interattivo. Per evitare la generazione di report senza dati, accertarsi che le partizioni rilevanti siano attivate quando i report vengono eseguiti in base ad una pianificazione.
- 2. Fare clic sull'opzione **Elimina** accanto al nome di una partizione se quella partizione non è più necessaria. La partizione viene di fatto eliminata alla prossima esecuzione del processo di manutenzione notturno del database.



 \mathbf{P}

Attenzione

Usare questa opzione con cautela. Non sarà infatti possibile recuperare le partizioni eliminate.

L'eliminazione delle partizioni obsolete riduce al minimo il numero di partizioni nel database di registrazione con un conseguente miglioramento della performance del database e della creazione dei report. Utilizzare l'opzione Elimina per eliminare le singole partizioni, come necessario. Vedere *Configurazione delle opzioni di manutenzione del database di registrazione*, pagina 335 se si preferisce eliminare le vecchie partizioni in base a una pianificazione.

3. Fare clic su **Salva ora** per attivare le modifiche apportate alle opzioni di partizione del database.

Visualizzazione dei registri di errore

Argomenti correlati:

- Impostazioni dell'amministrazione del database di registrazione, pagina 330
- Configurazione opzioni di rollover, pagina 331
- Configurazione delle opzioni sui tempi di navigazione in Internet, pagina 334
- Configurazione della registrazione di URL completi, pagina 333
- Configurazione delle opzioni di manutenzione del database di registrazione, pagina 335
- Configurazione della creazione delle partizioni del database di registrazione, pagina 338
- Configurazione delle partizioni disponibili, pagina 339

Usare la sezione **Attività registro errori** della pagina Creazione report > Database di registrazione (scheda Impostazioni) per visualizzare i record degli errori verificatesi durante l'esecuzione dei processi nel database di registrazione di Websense (vedere *Processi del database*, pagina 329). Queste informazioni potrebbero essere utili per la diagnostica e risoluzione problemi.

Selezionare una delle opzioni seguenti:

- Selezionare un numero dall'elenco a discesa per visualizzare un determinato numero di voci del registro di errori.
- Scegliere Visualizza tutti per visualizzare tutte le voci del registro di errori.
- Scegliere Non visualizzare per nascondere tutte le voci del registro di errori.

Configurazione dei report investigativi

Argomenti correlati:

- Collegamento con il database e impostazioni predefinite dei report, pagina 342
- Opzioni di visualizzazione e di output, pagina 344

I report investigativi offrono un quadro approfondito delle informazioni relative all'uso di Internet da parte della propria organizzazione. Vedere *Report investigativi*, pagina 119.

Il collegamento Opzioni, disponibile nella pagina dei report investigativi, offre l'opportunità di modificare il database di registrazione utilizzato per la creazione dei report. Consente anche di modificare la visualizzazione predefinita dei report dettagliati. Vedere *Collegamento con il database e impostazioni predefinite dei report*, pagina 342.

Il file **wse.ini** consente di configurare determinate impostazioni predefinite per la visualizzazione dei report riepilogativi e dei report multi-livello. Consente anche di determinare le dimensioni predefinite della pagina da usare quando un report viene convertito in formato PDF. Vedere *Opzioni di visualizzazione e di output*, pagina 344.

Collegamento con il database e impostazioni predefinite dei report

Argomenti correlati:

- Configurazione dei report investigativi, pagina 341
- Opzioni di visualizzazione e di output, pagina 344
- Report di riepilogo, pagina 121
- Report di riepilogo multi-livello, pagina 126

Usare la pagina delle opzioni dei **Report investigativi > Opzioni** per collegarsi al database di registrazione desiderato e per determinare le impostazioni predefinite per una visualizzazione dettagliata dei report investigativi.

Le modifiche apportate a questa pagina incidono sui report. Gli altri amministratori, o anche gli utenti che accedono per verificare la propria attività, possono modificare questi valori per le proprie attività di creazione di report.

- 1. Scegliere il database di registrazione da usare per i report investigativi.
 - Selezionare Visualizza database del catalogo per collegarsi al database di registrazione a cui è collegato Log Server. Procedere al punto 2.
 - Per accedere a un database di registrazione diverso:
 - a. Deselezionare l'opzione Visualizza il database del catalogo.
 - b. Inserire le informazioni seguenti per identificare il database di registrazione desiderato. (I report investigativi possono venire generati da un database v6.3.x o v7.0.)

Campo	Descrizione
Server	Inserire il nome o l'indirizzo IP del computer in cui è installato il database di registrazione.
Database	Inserire il nome del database di registrazione.
ID utente	Inserire l'ID utente per un account con permessi di accesso al database.
	Lasciare il campo vuoto se Log Server è stato installato per usare un collegamento di tipo trusted per accedere al database di registrazione.
	Se non si è sicuri, inserire sa . Questo è l'ID utente predefinito per MSDE e l'ID amministratore definito in Microsoft SQL Server.
Password	Inserire la password per l'ID utente specificato. Lasciare questo campo vuoto per un collegamento di tipo trusted.

Campo	Descrizione
Seleziona Intervallo date Report investigativi predefiniti.	Scegliere l'intervallo di date per la visualizzazione iniziale dei report di riepilogo.
Selezionare il formato del report dettagliato predefinito	Scegliere Selezione colonne intelligente per visualizzare i report dettagliati con le colonne predefinite destinate a contenere le informazioni da riportare. Scegliere Selezione colonna personalizzata per specificare le colonne esatte che si vogliono visualizzare in tutti i report dettagliati. Usare l'elenco Colonne disponibili per definire le proprie selezioni.
	visualizzate dopo aver generato i report.
Tipo di report	 Scegliere se aprire i report dettagliati che visualizzino inizialmente: Dettaglio: ciascun report appare su una riga separata; si possono visualizzare i tempi di esecuzione. Riepilogo: Unifica in un'unica voce tutti i record che condividono un elemento comune
	L'elemento specifico varia a seconda delle informazioni contenute nel report. Normalmente, la colonna all'estrema destra prima del valore di misurazione mostra l'elemento di riepilogo. I tempi di esecuzione non possono venire visualizzati.
Colonne disponibili / Report in uso	Selezionare il nome di una colonna dall'elenco Colonne disponibili e fare clic sul relativo pulsante a freccia per portarla nell'elenco Report in uso. È possibile inserire fino a 7 colonne nell'elenco Report in uso.
	Dopo aver inserito le colonne necessarie nell'elenco Report in uso per i report dettagliati iniziali, definire l'ordine delle colonne. Selezionare una voce dall'elenco e utilizzare i pulsanti a freccia su e giù per cambiare la sua posizione.

2. Selezionare le seguenti predefinizioni da applicare ai report dettagliati.

3. Fare clic su Salva le opzioni per salvare immediatamente tutte le modifiche.

Opzioni di visualizzazione e di output

Argomenti correlati:

- Configurazione dei report investigativi, pagina 341
- Collegamento con il database e impostazioni predefinite dei report, pagina 342
- *Output su file*, pagina 145

È possibile determinare il modo in cui i tipi di report selezionati e i risultati dei report debbano venire visualizzati nei report investigativi di riepilogo ed è possibile specificare le dimensioni predefinite della pagina quando i report vengono esportati in un formato PDF.

Le opzioni di configurazione dei report investigativi vengono definite nel file **wse.ini**. Il percorso predefinito è:

C:\Programmi\Websense\webroot\Explorer\wse.ini

La tabella seguente contiene un elenco dei parametri che agiscono sulla visualizzazione e sull'output dei report investigativi, gli aspetti sotto il controllo di ciascuno di essi e il relativo valore predefinito. (NON modificare le altre impostazioni del file Wse.ini.file.)

Parametro	Descrizione
maxUsersMenu	Il database deve avere un numero inferiore di utenti rispetto a questo valore (valore predefinito: 5000) per poter visualizzare l'Utente come una scelta per il tipo di report, nell'elenco Visualizza utilizzo Internet per.
maxGroupsMenu	Il database deve avere un numero inferiore di gruppi rispetto a questo valore (valore predefinito: 3000) per poter visualizzare il Gruppo come una scelta per il tipo di report, dall'elenco Visualizza utilizzo Internet per.
	Nota - Devono esserci 2 o più gruppi affinché Gruppo possa venire visualizzato in Visualizza utilizzo di Internet per.
	Devono esserci 2 o più domini affinché Dominio possa venire visualizzato in Visualizza utilizzo di Internet per. Non esiste un valore massimo per i domini.

Parametro	Descrizione
maxUsersDrilldown	Questo è applicabile al parametro warnTooManyHits che consente di determinare quando l'opzione Utente deve venire visualizzata in rosso. Le lettere scritte in rosso indicano che la selezione di Utente produrrà un report molto esteso che potrebbe essere molto lento da generare.
	Se il numero di utenti è superiore a questo valore (valore predefinito: 5000) e il numero di accessi è superiore al valore di warnTooManyHits, l'opzione Utente viene visualizzata in rosso in vari elenchi a discesa e negli elenchi dei valori.
	Se il numero di utenti è superiore a questo valore, ma il numero di accessi è inferiore al valore di warnTooManyHits, l'opzione Utente viene visualizzata in un colore normale in quanto il report che ne risulta sarà di dimensioni più accettabili.
maxGroupsDrilldown	L'opzione Gruppo viene visualizzata in rosso durante il drill-down se il report proposto include un numero superiore di gruppi rispetto al valore predefinito (ossia 2000). Le lettere scritte in rosse indicano che la selezione di Gruppo produrrà un report molto esteso che potrebbe essere molto lento da generare.
warnTooManyHits	Questo è applicabile al parametro maxUsersDrilldown che consente di determinare quando l'opzione Utente deve venire visualizzata in rosso.
	Se il numero di utenti è superiore al valore di maxUsersDrilldown ma il numero di accessi è inferiore a questo valore (valore predefinito: 10.000), l'opzione Utente <i>non</i> viene visualizzata in rosso.
	Se il numero di utenti è superiore al valore di maxUsersDrilldown e il numero di accessi è superiore a questo valore, l'opzione Utente viene visualizzata in rosso. Le lettere scritte in rosso indicano che la selezione di Utente potrebbe produrre un report molto esteso che potrebbe essere molto lento da generare.
hitsPerPage	Questo determina il numero massimo di elementi (valore predefinito: 100) visualizzati per pagina. (Questo non incide sui report stampati.)
maxOutputBufferSize	Questo è il numero massimo di dati (in byte) che possono venire visualizzati nella pagina principale dei report investigativi. Se i dati richiesti superano questo limite (valore predefinito: 4.000.000 o 4 milioni di byte), viene visualizzato un messaggio in rosso alla fine del report che avverte che alcuni risultati non sono stati inclusi.
	Se questo è un problema, si possono scegliere dei valori maggiori per visualizzare una maggiore quantità di dati in un report. Tuttavia, se si verificano errori di memoria, considerare la possibilità di ridurre questo valore.

Parametro	Descrizione
sendMulti	Per impostazione predefinita, questa impostazione è disattiva (0). Impostare il valore su 1 (attivato) per suddividere dei report dettagliati molto estesi e pianificati in molteplici file composti da 10.000 righe ciascuno. I file che costituiscono un report, vengono compressi e inviati ai destinatari via e-mail. I file dei report possono quindi venire estratti per mezzo delle utilità di compressione dei file utilizzati normalmente.
maxSlices	Il numero massimo di sezioni distinte (valore predefinito: 6) in un grafico a torta, con una sezione di tipo Altro, che riunisce tutti i valori che non dispongono di singole sezioni.
timelineCompressionThreshold	Questa opzione viene utilizzata per il Dettaglio giornaliero/mensile attività utente, se l'opzione Raggruppa accessi simili/Visualizza tutti gli accessi, è disponibile. Il report comprime tutti gli accessi che fanno parte della stessa categoria e che si sono verificati entro il numero di secondi qui definiti (valore predefinito: 10).
PageSize	 I risultati dei report investigativi possono venire esportati in formato PDF (Portable Document Forma) per semplificarne la distribuzione o la stampa. Le dimensioni della pagina (impostazione predefinita: Lettera) possono essere le seguenti: A4 (8,27 X 11,69 pollici) Lettera (8,5 X 11 pollici)

Attività utente

Argomenti correlati:

- Configurazione delle preferenze per la creazione dei report, pagina 314
- Accesso all'attività utente, pagina 147
- *Report investigativi*, pagina 119

Attività utente è una funzione che consente agli utenti di visualizzare i report investigativi della propria attività personale in Internet. Questo consente agli utenti di visualizzare il tipo di informazioni che vengono raccolte e monitorate sugli utenti, in conformità con i regolamenti governativi di molti paesi. Inoltre, la visualizzazione delle proprie attività può incoraggiare molti utenti a modificare le proprie abitudini di navigazione in modo da conformarsi alla politica di accesso ad Internet stabilita dalla propria organizzazione.



Per attivare Attività utente:

 Andare a Impostazioni >Generale > Servizi di directory e configurare il servizio di directory usato per autenticare gli utenti che accedono a Websense usando le loro credenziali di rete. Questo potrebbe essere stato fatto in precedenza per attivare i filtri applicabili in base ai nomi degli utenti e dei gruppi. Vedere Servizi di directory, pagina 65.

Se l'installazione include molteplici Policy Server, occorre collegarsi ad ognuno di essi e configurare la pagina Servizi di directory con le informazioni per il servizio di directory appropriato.

2. Andare a **Impostazioni** > **Creazione report** > **Preferenze** e selezionare la casella di controllo **Consenti attività utente**. Vedere *Configurazione delle preferenze per la creazione dei report*, pagina 314.

Dopo aver attivato questa opzione, accertarsi di fornire agli utenti le informazioni di cui hanno bisogno per l'esecuzione dei report:

 L'URL che consente di accedere all'interfaccia dell'attività utente. Ricordare agli utenti che possono salvare l'URL come un preferito e possono impostarlo come segnalibro per un uso successivo.

Leggere più avanti per informazioni dettagliate sull'URL.

• L'istanza di Policy Server da selezionare durante l'accesso.

Questo non è necessario nel caso di reti con un solo Policy Server. Se la rete include molteplici Policy Server, occorre dare agli utenti l'indirizzo IP dell'istanza di Policy Server configurata per comunicare con il servizio di directory che autentica il loro accesso in rete. Questa è l'istanza di Policy Server specificata quando si era installato Log Server.

• Il nome utente e la password da usare per l'accesso.

Gli utenti di Attività utente devono inserire il loro nome utente e password durante l'accesso.

L'URL necessario per l'accesso all'interfaccia di Attività utente è il seguente:

```
https://<ServerIP>:9443/mng/login/pages/
selfReportingLogin.jsf
```

Sostituire <ServerIP> con l'indirizzo IP del computer in cui è installato Websense Manager.

Gli amministratori e gli utenti possono anche accedere alla pagina con collegamento alla funzione Attività utente, aprendo la pagina di accesso a Websense Manager e facendo clic sul collegamento Attività utente.

Se la rete include **molteplici Policy Servers**, occorre informare gli utenti sull'istanza di Policy Server da scegliere durante l'accesso a Attività utente.

14

Configurazione della rete

Argomenti correlati:

- Configurazione dell'hardware, pagina 350
- Configurazione di Network Agent, pagina 351
- Verifica della configurazione di Network Agent, pagina 358

Se il software Websense è in modalità stand-alone (non integrato con un prodotto proxy o firewall), Websense Network Agent attiva quanto segue:

- Filtri applicati al contenuto di Internet
- Gestione del protocollo di rete e applicazioni Internet
- Gestione della banda di rete
- Registrazione dei byte trasferiti

In un'implementazione integrata del software Websense, un prodotto sviluppato da terzi potrebbe gestire l'attività di inoltro delle richieste dell'utente al software Websense per il filtraggio nonché l'inoltro delle pagine di blocco ai client. In questo ambiente, Network Agent può essere usato per filtrare richieste non-HTTP, fornire dettagli più precisi sulla registrazione, o entrambi.

Network Agent verifica continuamente l'uso complessivo di rete, incluso i byte trasferiti su rete. L'agente invia, ad intervalli predefiniti, riepiloghi sull'uso del software Websense. Ciascun riepilogo include il tempo di inizio e di fine, i byte complessivi usati e i byte usati per protocollo.

Per impostazione predefinita, Network Agent invia inoltre a Policy Server i dati sull'uso della larghezza di banda e i dati di registro sui filtri per Filtering Service.

Network Agent viene normalmente configurato in modo che possa monitorare tutto il traffico su rete. L'agente distingue tra:

- Richieste inviate dai computer interni ai computer interni (ad esempio, accessi a un server intranet)
- Richieste inviate dai computer interni ai computer esterni come ad esempio nel caso dei server Web (ad esempio, richieste di accesso a Internet da parte degli utenti)

Quest'ultimo è l'obiettivo primario del monitoraggio dei dipendenti nell'uso di Internet.

Configurazione dell'hardware

Ciascuna istanza di Network Agent monitora il traffico **dai** computer monitorati ed identificati come appartenenti alla propria rete. Per impostazione predefinita, monitora il traffico soltanto **verso** i computer interni specificati (ad esempio, i server Web interni).

È possibile definire i computer interni (segmenti di rete) che devono venire monitorati da ciascuna istanza di Network Agent o anche da ciascuna scheda di interfaccia di rete (Network Interface Card - NIC) installata in un computer con Network Agent.



Monitoraggio delle richieste inviate ai computer interni



Monitoraggio delle richieste inviate ai computer esterni

Ciascuna istanza di Network Agent deve:

- essere adeguatamente posizionata nella rete in modo da rilevare il traffico verso e dai computer monitorati.
- disporre di almeno 1 scheda NIC dedicata al monitoraggio del traffico.

Network Agent può essere installato su un computer con molteplici NIC e può usare molteplici NIC sia per il monitoraggio delle richieste che per l'invio delle pagine di blocco. Se si aggiunge una nuova scheda NIC al computer con Network Agent, occorre riavviare il servizio Network Agent e quindi configurare la nuova scheda NIC (vedere *Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC)*, pagina 355)



Per ulteriori informazioni sul percorso di Network Agent e sui requisiti della scheda interfaccia di rete NIC, vedere la *Guida di distribuzione*.

Per informazioni sulla configurazione di Network Agent al fine di monitorare le richieste di rete interne, usare le schede di interfaccia di rete NIC specifiche ed eseguire una registrazione potenziata, vedere *Configurazione di Network Agent*, pagina 351.

Configurazione di Network Agent

Argomenti correlati:

- *Configurazione dell'hardware*, pagina 350
- Configurazione delle impostazioni globali, pagina 352
- Configurazione delle impostazioni locali, pagina 353
- Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC), pagina 355
- Aggiunta o modifica degli indirizzi IP, pagina 357

Dopo aver installato Network Agent, usare Websense Manager per configurare la modalità di monitoraggio della rete. Le impostazioni di Network Agent sono suddivise in due aree principali:

- Impostazioni globali che incidono su tutte le istanze di Network Agent. Usare le seguenti impostazioni per:
 - Identificare i computer in rete.

- Compilare un elenco di computer che Network Agent deve monitorare per le richieste in entrata (ad esempio, i server Web interni).
- Specificare il calcolo della larghezza di banda e la modalità di registrazione dei protocolli.
- L'opzione **Impostazioni locali** che applica soltanto l'istanza selezionata di Network Agent. Usare le seguenti impostazioni per:
 - Identificare l'istanza di Filtering Service associata a ciascun Network Agent.
 - Prendere nota dei proxy o delle cache usati dai computer che questo Network Agent monitora.
 - Configurare come ciascuna scheda di rete (NIC) installata nel computer con Network Agent debba venire usata (per monitorare le richieste, inviare le pagine di blocco o entrambi).

Le impostazioni della scheda di rete determinano il segmento di rete che ciascuna istanza di Network Agent deve monitorare.

Configurazione delle impostazioni globali

Argomenti correlati:

- *Configurazione dell'hardware*, pagina 350
- Configurazione delle impostazioni locali, pagina 353
- Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC), pagina 355
- Aggiunta o modifica degli indirizzi IP, pagina 357

Usare la pagina **Impostazioni > Network Agent > Globale** per definire il monitoraggio di base e le modalità di registrazione per tutte le istanze di Network Agent.

L'elenco **Definizione di rete interna** elenca i computer che fanno parte della rete. Per impostazione predefinita, Network Agent non monitora il traffico (comunicazioni interne di rete) che avviene tra questi computer.

Un gruppo iniziale di voci viene configurato come predefinizione. È possibile aggiungere altre voci o modificare o eliminare voci esistenti.

L'elenco **Traffico interno di cui eseguire il monitoraggio** include i computer compresi in Definizione di rete interna il cui traffico **va monitorato** da Network Agent. Questo potrebbe includere i server Web interni, ad esempio, che aiutano a monitorare i collegamenti interni.

Qualsiasi richiesta inviata da qualunque punto della rete a un computer specifico interno viene monitorata. Per impostazione predefinita, questo elenco è vuoto.

 Fare clic sul pulsante Aggiungi per aggiungere un indirizzo IP o un intervallo di indirizzi IP all'apposito elenco. Per ulteriori informazioni, vedere Aggiunta o modifica degli indirizzi IP, pagina 357.

- Per modificare una voce dell'elenco, fare clic sull'indirizzo IP o su un intervallo di indirizzi IP. Per ulteriori informazioni, vedere Aggiunta o modifica degli indirizzi IP, pagina 357.
- Per eliminare un una voce dell'elenco, selezionare la casella di controllo accanto all'indirizzo IP o all'intervallo di indirizzi IP da eliminare e fare clic su Elimina.

Le opzioni **Impostazioni aggiuntive** consentono di determinare la frequenza di calcolo dell'utilizzo della larghezza di banda da parte di Network Agent e se, e con quale frequenza, va registrato il traffico del protocollo.

Campo	Azione
Intervallo di calcolo larghezza di banda	Inserire un numero compreso tra 1 e 300 per specificare la frequenza, in secondi, del calcolo della larghezza di banda da parte di Network Agent. Una voce di 300, ad esempio, indica che Network Agent calcolerà la larghezza di banda ogni cinque minuti. Il valore predefinito è 10 secondi.
Registra periodicamente il traffico del protocollo	Selezionare questa opzione per attivare il campo dell'intervallo di Registrazione.
Intervallo di registrazione	Inserire un numero compreso tra 1 e 300 per specificare la frequenza, in minuti, di registrazione dei protocolli da parte di Network Agent. Una voce di 60, ad esempio, indica che Network Agent effettuerà le registrazioni nel file di registro ogni ora. Il valore predefinito è 1 minuto.

Una volta terminate le modifiche, fare clic su **OK** per inserirle nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Configurazione delle impostazioni locali

Argomenti correlati:

- *Configurazione dell'hardware*, pagina 350
- Configurazione delle impostazioni globali, pagina 352
- Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC), pagina 355

Usare la pagina **Impostazioni > Network Agent > Impostazioni locali** per configurare il comportamento dei filtri, le informazioni di proxy e altre impostazioni per l'istanza selezionata di Network Agent. L'indirizzo IP dell'istanza Network Agent selezionata viene visualizzata nella barra del titolo del riquadro del contenuto e viene evidenziata nel riquadro di navigazione di sinistra. Usare **Definizione di Filtering Service** per specificare l'istanza di Filtering Service associata all'istanza di Network Agent e come rispondere alle richieste Internet se Filtering Service non è disponibile.

Campo	Azione
Indirizzo IP di Filtering Service:	Selezionare l'istanza di Filtering Service associata a questo Network Agent.
Se Filtering Service non è disponibile	Selezionare Autorizza per autorizzare tutte le richieste o selezionare Blocca per bloccare tutte le richieste fino a quando Filtering Service non ritorna ad essere disponibile. L'impostazione predefinita è Autorizza.

Per assicurare che tutte le richieste degli utenti vengano monitorate e vengano registrate correttamente, usare l'elenco **Proxy e cache** per specificare l'indirizzo IP di qualsiasi server proxy o cache che comunichi con Network Agent.

- Fare clic su Aggiungi per aggiungere un indirizzo IP o un intervallo di indirizzi IP all'apposito elenco. Per ulteriori informazioni, vedere Aggiunta o modifica degli indirizzi IP, pagina 357.
- Per modificare una voce dell'elenco, fare clic sull'indirizzo IP o su un intervallo di indirizzi IP.
- Per eliminare una voce dell'elenco, selezionare la casella di controllo accanto all'indirizzo IP o all'intervallo di indirizzi IP e fare clic su **Elimina**.

Usare l'elenco **Schede interfaccia di rete** per configurare ciascuna scheda NIC. Fare clic su una NIC nella colonna **Nome** e vedere quindi *Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC)*, pagina 355 per ulteriori informazioni.

Se le richieste HTTP di rete vengono trasmesse tramite una porta non standard, fare clic su **Impostazioni avanzate di Network Agent** per indicare le porte corrette che Network Agent deve monitorare. Per impostazione predefinita, le **Porte utilizzate per il traffico HTTP** sono **8080**, **80**.

Le altre impostazioni di questa sezione non dovrebbero venire modificate a meno che non si venga istruiti di farlo dal supporto tecnico di Websense.

Campo	Descrizione
Modalità	 Nessuna (predefinizione) Generale Errore Dettagli Larghezza di banda
Output	File (predefinizione)Finestra
Porta	55870 (predefinizione)

Una volta terminate le modifiche delle impostazioni di Network Agent, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC)

Argomenti correlati:

- Configurazione dell'hardware, pagina 350
- Configurazione di Network Agent, pagina 351
- Configurazione delle impostazioni di monitoraggio per una scheda di interfaccia di rete (NIC), pagina 356
- Aggiunta o modifica degli indirizzi IP, pagina 357

Usare la pagina **Network Agent > Impostazioni locali > Configurazione NIC** per specificare come Network Agent debba usare la scheda di interfaccia di rete (NIC) per monitorare e gestire l'uso della rete.

L'area **Informazioni su NIC** offre il contesto per le modifiche da apportare, indicando l'**Indirizzo IP**, una breve **Descrizione** della scheda NIC e il **Nome** della scheda. Usare queste informazioni per eseguire una configurazione corretta della scheda dell'interfaccia di rete (NIC).

Monitoraggio

In una configurazione con molteplici schede NIC, è possibile identificare una NIC per monitorare il traffico di rete e un'altra NIC per applicare le pagine di blocco. Occorre usare almeno una NIC per il monitoraggio ma occorre usarne più di una per monitorare il traffico.

Usare la sezione **Monitoraggio** per indicare se attivare o meno l'opzione **Utilizzare questa NIC per il monitoraggio del traffico?**

- Se questa NIC non viene usata per il monitoraggio, deselezionare la casella di controllo e quindi procedere alla sezione successiva.
- Se questa NIC viene usata per il monitoraggio, selezionare la casella di controllo e fare quindi clic su Configura. Si viene portati alla pagina Elenco di controllo. Per informazioni, vedere Configurazione delle impostazioni di monitoraggio per una scheda di interfaccia di rete (NIC), pagina 356.

Altre opzioni NIC

Oltre a configurare le opzioni di monitoraggio, è anche possibile determinare altri comportamenti della scheda NIC.

- In Blocco, verificare che le NIC corrette siano incluse nell'elenco del campo NIC di blocco. Se si stanno configurando molteplici NIC, le impostazioni di ciascuna NIC devono avere lo stesso valore in questo campo. In altre parole, si deve utilizzare soltanto una scheda NIC per il blocco.
- 2. Se si sta eseguendo il software Websense in modalità **Versione autonoma**, l'opzione **Filtra e registra richieste HTTP** è selezionata e non può essere modificata.
- 3. Se si è integrato il software Websense con un dispositivo o un'applicazione di terzi, usare le opzioni **Integrazioni** per indicare come Network Agent debba filtrare e registrare le richieste HTTP. Le opzioni non applicabili al proprio ambiente informatico, vengono disattivate.
 - Selezionare Registra richieste HTTP per migliorare l'accuratezza dei report Websense.
 - Selezionare Filtra tutte le richieste non inviate attraverso porte HTTP per utilizzare Network Agent per filtrare soltanto le richieste HTTP non inviate attraverso il prodotto di integrazione.
- 4. In Gestione protocollo, indicare se Network Agent debba usare questa scheda NIC per filtrare i protocolli non HTTP.
 - Selezionare Filtra richieste di protocolli diversi da HTTP per attivare la funzione di gestione dei protocolli. Questo consente al software Websense di filtrare le applicazioni Internet e il metodo di trasferimento dei dati, come quelli usati per la messaggistica istantanea, lo streaming media, lo scambio dei file, la posta Internet e così via. Per ulteriori informazioni, vedere *Filtri di categoria e di protocollo*, pagina 38 e *Gestione dei protocolli*, pagina 189.
 - Selezionare Misura utilizzo larghezza di banda per protocollo per attivare la funzione di ottimizzazione della larghezza di banda. Network Agent usa questa NIC per monitorare l'uso della larghezza di banda della rete da parte di ogni protocollo o applicazione. Per ulteriori informazioni, vedere Uso di Bandwidth Optimizer per la gestione della larghezza di banda, pagina 195.

Configurazione delle impostazioni di monitoraggio per una scheda di interfaccia di rete (NIC)

Usare la pagina **Impostazioni locali > Configurazione NIC > Elenco di controllo** per specificare i computer che Network Agent deve monitorare tramite la scheda di interfaccia di rete selezionata (NIC).

- 1. In Elenco di controllo, specificare le richieste che Network Agent deve monitorare:
 - Tutto: Network Agent esegue il monitoraggio delle richieste inviate da tutti i computer che vede tramite la scheda NIC selezionata. Normalmente questo include tutti i computer dello stesso segmento di rete, tra cui il computer con Network Agent in uso o con la scheda NIC.
 - Nessuno: Network Agent non monitora alcuna richiesta.
 - **Specifico**: Network Agent monitora soltanto i segmenti di rete inclusi nell'Elenco di controllo.

2. Se si è selezionato Specifico, fare clic su **Aggiungi** e specificare gli indirizzi IP dei computer che Network Agent deve monitorare. Per ulteriori informazioni, vedere *Aggiunta o modifica degli indirizzi IP*, pagina 357.



Nota

Non è consentito inserire un intervallo di indirizzi IP sovrapposti. Se gli indirizzi si sovrappongono, le misurazioni della larghezza di banda della rete non saranno precise e il filtro basato sulla larghezza di rete non potrà venire applicato correttamente.

Per eliminare un indirizzo IP o un intervallo di rete dall'elenco, verificare la voce dell'elenco appropriato e fare quindi clic su **Elimina**.

3. In Eccezioni elenco di controllo, identificare i computer interni che Network Agent deve escludere dal monitoraggio.

Ad esempio, Network Agent può ignorare le richieste inoltrate da CPM Server. In questo modo, le richieste di CPM Server non interferiranno con i dati di registro di Websense o con qualsiasi output del monitor relativo allo stato.

- a. Per identificare un computer, fare clic su **Aggiungi** ed inserire quindi il suo indirizzo IP.
- b. Ripetere la procedura per identificare eventuali altri computer.
- 4. Fare clic su **OK** per inserire nella cache le modifiche apportate e per ritornare alla pagina Configurazione NIC. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Aggiunta o modifica degli indirizzi IP

Argomenti correlati:

- Configurazione delle impostazioni globali, pagina 352
- Configurazione delle impostazioni locali, pagina 353
- Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC), pagina 355

Usare la pagina **Aggiungi indirizzi IP** o **Modifica indirizzi IP** per apportare modifiche agli elenchi seguenti di Network Agent: definizione di rete interna, Traffico interno di cui eseguire il monitoraggio, Proxy e Cache, Elenco di controllo oppure Eccezioni elenco di controllo.

- Se si aggiunge o si modifica un intervallo di indirizzi IP, accertarsi che le voci dell'elenco non si sovrappongano (sia nel caso di un indirizzo IP singolo o di un intervallo di indirizzi IP).
- Se si aggiunge o si modifica un indirizzo IP singolo, accertarsi che rientri nell'intervallo già visualizzato nell'elenco.

Per aggiungere un nuovo indirizzo IP o un intervallo di indirizzi IP:

- 1. Selezionare il pulsante di opzione Indirizzo IP o Intervallo di indirizzi IP.
- 2. Inserire un indirizzo IP o un intervallo di indirizzi IP valido.
- 3. Fare clic su **OK** per ritornare alla pagina precedente Impostazioni di Network Agent. Il nuovo indirizzo IP o il nuovo intervallo di indirizzi IP viene visualizzato nell'apposita tabella.

Per ritornare alla pagina precedente senza inserire le modifiche nella cache, fare clic su **Annulla**.

4. Ripetere questa procedura per ciascun indirizzo IP aggiunto, come necessario.

Se si modifica un indirizzo IP o un intervallo di intervallo di indirizzi IP, la pagina Modifica indirizzi IP visualizza la voce selezionata con il relativo pulsante d'opzione già selezionato. Apportare le modifiche necessarie, fare clic su **OK** per ritornare alla pagina precedente.

Una volta terminato di aggiungere o di modificare gli indirizzi IP, fare clic su **OK** nella pagina Impostazioni Network Agent. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Verifica della configurazione di Network Agent

Dopo aver configurato Network Agent in Websense Manager, usare Network Traffic Detector per verificare che il software Websense possa vedere i computer collegati in rete.

- 1. Fare clic su **Start > Programmi > Websense > Utilità > Strumento di** rilevazione del traffico di rete per avviare lo strumento di rilevazione.
- 2. Selezionare una scheda di rete dall'elenco a discesa Scheda di rete.
- 3. Verificare gli indirizzi che appaiono nell'elenco **Intervalli di rete monitorati** per confermare che tutte le subnet appropriate siano incluse nell'elenco.
- 4. Usare i pulsanti **Aggiungi subnet** e **Rimuovi subnet** per modificare le parti della rete che si vogliono analizzare.
- 5. Fare clic su Inizia monitoraggio.

Lo Strumento di rilevazione del traffico di rete rileva i computer collegati in rete monitorando le informazioni che tali computer inviano attraverso la rete. Nell'elenco **Numero di computer rilevati** viene riportato il numero totale di computer rilevati in quel particolare momento.

6. Per visualizzare informazioni specifiche sui computer rilevati da questo strumento, selezionare una subnet dall'elenco Intervalli di rete monitorati e fare quindi clic su **Visualizza computer rilevati**.

Se un determinato computer non è incluso nell'elenco, verificare che stia effettivamente generando del traffico di rete. In questo caso, andare al computer, lanciare un browser e navigare a un sito Web. Tornare quindi allo Strumento di rilevazione del traffico di rete e verificare che il computer appaia nella finestra di dialogo **Computer rilevati**. 7. Una volta terminato di verificare la visibilità del traffico di rete, fare clic su **Interrompi monitoraggio**.

Se alcuni computer non sono visibili:

- Controllare la configurazione di rete e i requisiti relativi alla configurazione della scheda NIC (vedere *Configurazione dell'hardware*, pagina 350).
- Verificare le informazioni più dettagliate sulla configurazione di rete incluse nella *Installation Guide* del software Websense.
- Verificare di aver configurato correttamente la scheda NIC di monitoraggio (*Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC)*, pagina 355).
15 Diagnostica e risoluzione problemi

Prima di contattare l'assistenza tecnica, consultare questa sezione per informazioni relative alla soluzione dei problemi più comuni.

Il sito Websense Web contiene una Knowledge Base molto estesa, disponibile all'indirizzo <u>www.websense.com/global/en/SupportAndKB/</u>. Cercare l'argomento necessario usando parole chiave o un numero di riferimento, oppure aprire gli articoli più letti.

Le istruzioni di diagnostica e risoluzione problemi sono raggruppate nelle sezioni seguenti:

- Problemi di installazione e di sottoscrizione
- Problemi con il Master Database, pagina 363
- Problemi di filtro, pagina 369
- Problemi con Network Agent, pagina 373
- Problemi di identificazione utenti, pagina 376
- Problemi dei messaggi di blocco, pagina 386
- Problemi di registro, di messaggi di stato e di avvisi di errore, pagina 389
- Problemi di Policy Server e Policy Database, pagina 391
- Problemi di amministrazione con delega, pagina 393
- Problemi di creazione report, pagina 394
- Strumenti di diagnostica e risoluzione problemi, pagina 406

Problemi di installazione e di sottoscrizione

- Lo stato Websense mostra un problema di sottoscrizione, pagina 361
- Dopo l'aggiornamento, mancano degli utenti in Websense Manager, pagina 362

Lo stato Websense mostra un problema di sottoscrizione

È necessario disporre di una una chiave di sottoscrizione per scaricare Websense Master Database ed applicare i filtri per l'accesso a Internet. Se la propria sottoscrizione scade o non è valida e se il Master Database non è stato scaricato da più di due settimane, la schermata Integrità di Websense visualizza un messaggio di avvertenza.

- Verificare di aver inserito la chiave di sottoscrizione esattamente come è stata ricevuta. La chiave distingue tra maiuscole e minuscole.
- Accertare che la sottoscrizione non sia scaduta. Vedere Chiave di sottoscrizione, pagina 364.
- Verificare che il Master Database sia stato scaricato da non oltre 2 settimane. Verificare lo stato del download in Websense Manager: fare clic su Scarica database nella pagina Stato > Oggi.

Vedere *Il download del Master Database non può venire completato*, pagina 364 per informazioni di diagnostica e risoluzione problemi sul download del database.

Se si è inserita correttamente la chiave ma si continua a ricevere un errore di stato o se la sottoscrizione è scaduta, contattare Websense Inc o il rivenditore autorizzato.

Se la sottoscrizione è scaduta, le impostazioni di Websense Manager determinano se a tutti gli utenti deve venire concesso un accesso Internet non filtrato o se tutte le richieste Internet devono venire bloccate. Per ulteriori informazioni, vedere *Sottoscrizioni*, pagina 28.

Dopo l'aggiornamento, mancano degli utenti in Websense Manager

Se, dopo un aggiornamento del software Websense, si è definita la Directory attiva come servizio di directory, i nomi degli utenti non verranno visualizzati in Websense Manager. Questo si verifica quando i nomi degli utenti includono caratteri che non fanno parte del set di caratteri UTF-8.

Per supportare LDAP 3.0, l'installatore di Websense modifica il set di caratteri da MBCS a UTF-8 durante l'aggiornamento. Ne risulta che i nomi degli utenti che includono caratteri non-UTF-8 non vengono riconosciuti.

Per risolvere questo problema, modificare manualmente il set di caratteri impostandoli su MBCS:

- 1. In Websense Manager, andare a Impostazioni > Servizi di directory.
- 2. Verificare che Active Directory (Native Mode) sia selezionata in Directory, accanto all'area superiore della pagina.
- 3. Fare clic su Impostazioni directory avanzate.
- 4. In Set di caratteri, fare clic su **MBCS**. Potrebbe essere necessario scorrere verso il basso per visualizzare queste opzioni.
- 5. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Problemi con il Master Database

- Il database dei filtri iniziale è in uso, pagina 363
- Il Master Database risale a più di 1 settimana fa, pagina 363
- Il download del Master Database non può venire completato, pagina 364
- Il download del Master Database non avviene ai tempi previsti, pagina 368
- Come contattare il Supporto tecnico per problemi di download del database, pagina 368

Il database dei filtri iniziale è in uso

Websense Master Database ospita le definizioni delle categorie e dei protocolli che costituiscono la base per i filtri da applicare ai contenuti di Internet .

Una versione parziale del Master Database viene installata insieme al software Websense in ogni computer in cui è installato Filtering Service. Questo database parziale viene utilizzato per attivare la funzione di base dell'applicazione dei filtri dal momento in cui si immette una chiave di sottoscrizione.

È necessario eseguire il download del database completo per garantire un filtraggio completo. Per ulteriori informazioni, vedere *Websense Master Database*, pagina 32.

La procedura di scaricamento dell'intero database potrebbe richiedere diversi minuti o più di un'ora, a seconda della velocità del collegamento con Internet, della larghezza di banda, della memoria disponibile e dello spazio disponibile sul disco fisso.

Il Master Database risale a più di 1 settimana fa

Websense Master Database ospita le definizioni delle categorie e dei protocolli che costituiscono la base per i filtri da applicare ai contenuti di Internet. Il software Websense scarica le modifiche apportate al Master Database in base alla frequenza stabilita in Websense Manager. Per predefinizione, la frequenza del download è una volta al giorno.

Per avviare manualmente il download del database:

- 1. In Websense Manager, andare a **Stato> Oggi** e fare clic su **Download del** database.
- 2. Fare clic su **Aggiorna** accanto all'istanza corrispondente di Filtering Service per avviare il download del database o fare clic su **Aggiorna tutto** per avviare il download in tutti i computer con Filtering Service installato.



Nota

Dopo aver aggiornato il Master Database, l'uso della CPU può raggiungere il 90% o oltre per un breve periodo di tempo mentre il database viene caricato nella memoria locale. Si consiglia di eseguire il download in un orario non di punta. 3. Per continuare a lavorare durante il download del database, fare clic su **Chiudi**. Fare clic sul pulsante **Download del database** in gualsiasi momento per

Fare clic sul pulsante **Download del database** in qualsiasi momento per visualizzare lo stato di avanzamento del download.

Se si aggiunge una nuova versione del Master Database o se si eliminano categorie o protocolli, gli amministratori che eseguono attività di gestione dei criteri associati a una categoria o a un protocollo (come ad esempio la modifica di un set di categorie) durante il download, potrebbero ricevere un messaggio di errore. Sebbene questi aggiornamenti siano rari, è consigliabile cercare di evitare di apportare modifiche associate a una categoria o a un protocollo durante il download di un database.

Il download del Master Database non può venire completato

Se non è possibile scaricare il Websense Master Database:

- Assicurarsi che la chiave di sottoscrizione sia stata immessa correttamente in Websense Manager e che non sia scaduta (*Chiave di sottoscrizione*, pagina 364).
- Verificare che il computer con Filtering Service installato sia in grado di accedere a Internet (*Accesso a Internet*, pagina 365).
- Verificare le impostazioni di firewall o del server proxy per accertare che Filtering Service possa collegarsi al server di Websense per il download (*Verifica delle impostazioni del firewall o del server proxy*, pagina 365).
- Verificare che esista spazio sufficiente sul disco fisso (Spazio su disco insufficiente, pagina 366) e nella memoria Memoria insufficiente, pagina 367, del computer che sta effettuando il download.
- Identificare eventuali applicazioni o dispositivi di rete, come ad esempio un software anti-virus, che potrebbe impedire il collegamento per il download (*Applicazione delle restrizioni*, pagina 368).

Chiave di sottoscrizione

Per verificare che la chiave di sottoscrizione sia stata immessa correttamente e non sia scaduta:

- 1. In Websense Manager, andare a **Impostazioni > Account**.
- 2. Confrontare la chiave di sottoscrizione ricevuta da Websense, Inc o dal proprio rivenditore con la chiave di sottoscrizione indicata nel campo **Chiave di sottoscrizione**. La chiave deve usare le stesse minuscole/maiuscole indicate nel documento della chiave.
- 3. Verificare la data adiacente a **Scadenza chiave**. Se si è superata la data di scadenza, contattare il proprio rivenditore o Websense, Inc. per il rinnovo della sottoscrizione.
- 4. Se si sono apportate modifiche alla chiave nella finestra di dialogo Impostazioni, fare clic su **OK** per attivare la chiave e il download del database.

Per avviare manualmente il download del database, o per verificare lo stato di download del database più recente, fare clic su **Download del database** nella barra degli strumenti nell'area superiore della pagina Stato > Oggi.

Accesso a Internet

Per scaricare il Master Database, il computer in cui è installato Filtering Service invia un comando **HTTP post** ai server di download ai seguenti indirizzi URL:

download.websense.com ddsdom.websense.com ddsint.websense.com portal.websense.com my.websense.com

Per verificare che Filtering Service disponga dell'accesso a Internet necessario per comunicare con il server di download:

- 1. Aprire un browser nel computer con Filtering Service installato.
- 2. Digitare l'URL seguente:

http://download.websense.com/

Se il computer è in grado di aprire un collegamento HTTP al sito, viene visualizzata una pagina di ridirezionamento e il browser visualizza la home page di Websense.

Se questo non dovesse accadere, verificare che il computer:

- possa comunicare tramite la porta 80 o tramite la porta designata in rete per il traffico HTTP
- sia configurato correttamente per eseguire ricerche DNS
- sia configurato per l'uso di qualsiasi server proxy (vedere Verifica delle impostazioni del firewall o del server proxy, pagina 365)

Accertarsi inoltre che il proprio gateway non includa delle regole che bloccano il traffico HTPP dal computer in cui è installato Filtering Service.

- 3. Usare uno dei metodi seguenti per confermare che il computer possa comunicare con il sito dei download:
 - Dal prompt di comando, inserire il comando seguente:

ping download.websense.com

Verificare che il ping riceva una risposta dal server del download.

 Usare telnet per collegarsi a download.websense.com 80. Se viene visualizzato un cursore e non viene visualizzato un messaggio di errore, è possibile collegarsi al server di download.

Verifica delle impostazioni del firewall o del server proxy

Se il Master Database è stato scaricato attraverso un firewall o un server proxy che richiede un'autenticazione, verificare che un browser del computer in cui è installato Filtering Service possa caricare correttamente le pagine Web. Se le pagine si aprono normalmente ma il Master Database non viene scaricato, verificare le impostazioni del server proxy del browser Web.

Microsoft Internet Explorer:

- 1. Selezionare Strumenti > Opzioni Internet.
- 2. Aprire la scheda Connessioni .
- 3. Fare clic su **Impostazioni LAN**. Le informazioni sulla configurazione del server proxy vengono visualizzate in **Proxy server**.

Prendere nota delle impostazioni del proxy.

Mozilla Firefox:

- 1. Selezionare Strumenti > Opzioni> avanzate.
- 2. Selezionare la scheda Rete.
- Fare clic su Impostazioni. La finestra di dialogo Impostazioni connessione visualizza se il browser è stato configurato per il collegamento con un server proxy.

Prendere nota delle impostazioni del proxy.

Accertarsi che il software Websense sia stato configurato per usare lo stesso server proxy per l'esecuzione del download.

- 1. In Websense Manager, andare a Impostazioni > Download del database.
- 2. Verificare che Utilizza server proxy o firewall sia stato selezionato e che il server corretto e la porta siano inclusi nell'elenco.
- 3. Verificare che le impostazioni di **Autenticazione** siano corrette. Verificare il nome utente e la password controllando che ortografia e maiuscole/minuscole siano corrette.

Se il software Websense deve fornire informazioni di autenticazione, il firewall o il server proxy devono essere configurati in modo da accettare un semplice testo o un'autenticazione di base. Nel <u>Knowledge Base</u> di Websense sono disponibili informazioni sull'attivazione dell'autenticazione di base.

Se un firewall limita l'accesso a Internet durante l'intervallo di tempo in cui il software Websense scarica normalmente il database o limita le dimensioni di un file trasferibile via HTTP, il software Websense non potrà scaricare il database. Per determinare se il firewall stia impedendo il download, controllare se esiste una regola nel firewall che potrebbe bloccare il download e cambiare, se necessario, i tempi definiti per lo scaricamento di Websense Manager (*Configurazione dei download del database*, pagina 34).

Spazio su disco insufficiente

Websense Master Database è archiviato nella directory Websense **bin** di Websense (/ opt/Websense/bin or C:\Programmi\Websense\bin, per impostazione predefinita). L'unità disco che contiene questa directory deve disporre di uno spazio sufficiente per scaricare il database compresso e di uno spazio sufficiente per contenere il database decompresso.

Il computer deve avere almeno il doppio dello spazio necessario per il Master Database. Mano a mano che le voci del Master Database aumentano, lo spazio necessario per il download aumenta di conseguenza. Come regola generale, Websense, Inc consiglia di disporre di almeno 3 GB di spazio su disco nell'unità designata per il download.

In Windows, usare Windows Explorer per verificare lo spazio su disco disponibile:

- 1. Aprire Risorse del computer in Windows Explorer (non in Internet Explorer).
- 2. Selezionare l'unità su cui è installato il software Websense. Per predefinizione, il software Websense è situato nell'unità C.
- 3. Fare clic con il pulsante destro del mouse su **Proprietà** dal menu a discesa.
- 4. Nella scheda Generale, verificare che siano disponibili almeno 3 GB di spazio libero su disco. Se lo spazio su disco non è sufficiente, eliminare i file non necessari per liberare lo spazio necessario.

Nei sistemi Linux, usare il comando **df** per verificare la quantità di spazio disponibile nel sistema dei file in cui il software Websense è stato installato:

- 1. Aprire una sessione del terminale.
- 2. Alla visualizzazione del prompt, inserire:

df -h /opt

Il software Websense c normalmente installato nella directory /opt/Websense/bin . Se è installato altrove, usare il percorso della sua installazione.

3. Verificare che siano disponibili almeno 3 GB di spazio libero su disco. Se lo spazio su disco non è sufficiente, eliminare i file non necessari fino a ottenere lo spazio necessario.

Se si conferma che lo spazio su disco è sufficiente, ma esistono ancora problemi di download, provare a interrompere tutti i servizi Websense (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290), eliminare **Websense.xfr** e i file **Websense** (nessuna estensione), avviare i servizi e quindi scaricare manualmente un nuovo database.

Memoria insufficiente

La memoria necessaria per l'esecuzione del software Websense e per il download del Master Database varia a seconda delle dimensioni della rete. Ad esempio, in una rete di piccole dimensioni, è consigliabile disporre di 2 GB di memoria per tutte le piattaforme.

Per raccomandazioni sulle impostazioni del sistema, fare riferimento alla *Guida di distribuzione*.

Per verificare la memoria in un sistema Windows:

- 1. Aprire il Task Manager.
- 2. Selezionare la scheda Prestazioni .
- 3. Verificare la Memoria fisica disponibile.
- 4. Se la memoria disponibile è inferiore ai 2 GB, aumentare la RAM del computer.

Si può anche selezionare **Pannello di controllo > Strumenti amministrativi > Prestazioni** per catturare le informazioni necessarie.

Per verificare la memoria in un sistema Linux:

- 1. Aprire una sessione del terminale.
- 2. Alla visualizzazione del prompt, inserire:
- 3. Calcolare la memoria totale disponibile aggiungendo Mem: av e Swap: av.
- 4. Se la memoria disponibile è inferiore ai 2 GB installati, aumentare la RAM del computer.

Applicazione delle restrizioni

Alcune applicazioni o dispositivi limitativi, come ad esempio gli scanner di virus, le applicazioni di limitazione delle dimensioni o i sistemi di rilevazione delle intrusioni possono interferire con lo scaricamento del database. Sarebbe preferibile configurare il software Websense in modo che vada direttamente all'ultimo gateway senza collegarsi a queste applicazioni o a questi dispositivi. In alternativa:

1. Disattivare le limitazioni associate al computer con installato Filtering Service e al percorso per il download del Master Database.

Vedere la documentazione del dispositivo o del software in questione per istruzioni su come modificare la relativa configurazione.

2. Provare a scaricare il Master Database.

Se questa modifica non produce alcun effetto, riconfigurare l'applicazione o il dispositivo in modo da includere il computer con Filtering Service installato.

Il download del Master Database non avviene ai tempi previsti

La data e l'ora del sistema potrebbero non essere stati impostati correttamente nel computer con installato Filtering Service. Il software Websense utilizza l'orologio del sistema per determinare i tempi di download del Master Database.

Se il download non avviene per nulla, vedere *Il download del Master Database non può venire completato*, pagina 364.

Come contattare il Supporto tecnico per problemi di download del database

Se, dopo aver completato le operazioni di diagnostica/risoluzione problemi qui riportate, si stanno ancora verificando problemi di scaricamento del Master Database, inviare le seguenti informazioni al Supporto tecnico di Websense:

- 1. Il messaggio di errore esatto visualizzato nella finestra di dialogo Download del database
- 2. Gli indirizzi IP esterni del computer che cerca di scaricare il database

- 3. La chiave di sottoscrizione rilasciata da Websense
- 4. La data e l'ora dell'ultimo tentativo
- 5. Numero di eventuali byte trasferiti
- Aprire un prompt di comando ed eseguire un nslookup in download.websense.com. Se il collegamento con il server di download riesce, inviare al Supporto tecnico gli indirizzi IP restituiti.
- Aprire un prompt di comando ed eseguire un tracert in download.websense.com. Se il collegamento con il server di download riesce, inviare al Supporto tecnico la traccia al routing.
- 8. La traccia o la cattura di un pacchetto eseguite in un server di download di Websense durante un tentativo di download.
- 9. La traccia o la cattura di un pacchetto, eseguite nel gateway di rete durante il medesimo tentativo di download.
- 10. I file seguenti dalla directory bin di Websense. websense.ini, eimserver.ini e config.xml.

Andare a <u>www.websense.com/SupportPortal/default.aspx</u> per informazioni di contatto con il Supporto tecnico.

Problemi di filtro

- Filtering Service non è in esecuzione, pagina 369
- User Service non è disponibile, pagina 370
- Siti erroneamente categorizzati come Tecnologia informatica, pagina 371
- Le parole chiave non vengono bloccate, pagina 371
- Gli URL personalizzati o con un filtro per restrizioni di accesso, non vengono filtrati come previsto., pagina 372
- Un utente non può accedere a un protocollo o un'applicazione come previsto, pagina 372
- Una richiesta FTP non viene bloccata come previsto, pagina 372
- Il software Websense non applica i criteri previsti per utenti o gruppi, pagina 373
- Gli utenti remoti non vengono filtrati dal criterio corretto, pagina 373

Filtering Service non è in esecuzione

Se il Filtering Service non è in esecuzione, le richieste di accesso a Internet non possono venire filtrate e registrate.

L'esecuzione di Filtering Service potrebbe venire interrotta se:

• Lo spazio sul disco del computer con installato Filtering Service non è sufficiente.

- Il download del Master Database non è riuscito a causa dell'insufficienza di spazio su disco (vedere *Il download del Master Database non può venire* completato, pagina 364).
- Il file websense.ini risulta mancante o danneggiato.
- Occorre interrompere il servizio (dopo aver creato, ad esempio, delle pagine di blocco personalizzate) e non riavviarlo.

Se si sono riavviati molteplici servizi Websense, e se non sono stati avviati nell'ordine corretto, Filtering Service potrebbe sembrare interrotto. Quando si riavviano molteplici servizi, ricordarsi di avviare il Policy Database, Policy Broker e Policy Server prima di avviare altri servizi Websense.

Per diagnosticare e risolvere questi problemi:

- Verificare che siano disponibili almeno 3 GB di spazio su disco nel computer con installato Filtering Service. Potrebbe essere necessario eliminare dei file non utilizzati o aumentare la capacità di spazio.
- Navigare alla directory bin di Websense (C:\Programmi\Websense\bin o /opt/ Websense/bin) ed accertarsi di poter aprire websense.ini in un programma di gestione del testo. Se questo file è stato danneggiato, sostituirlo con un file di backup.
- Aprire il visualizzatore degli eventi di Windows oppure il file websense.log per verificare la presenza di messaggi di errore relativi a Filtering Service (vedere Strumenti di diagnostica e risoluzione problemi, pagina 406).
- Scollegarsi da Websense Manager, riavviare Policy Server di Websense e riavviare quindi Filtering Service di Websense (vedere *Chiusura e riavvio dei* servizi di Websense, pagina 290).

Attendere 1 minuto prima di ricollegarsi a Websense Manager.

User Service non è disponibile

Se User Service non è in esecuzione o se Policy Server non può comunicare con User Service, il software Websense non può applicare correttamente i criteri di filtro basati sull'utente.

Se si riavvia Policy Server dopo aver riavviato altri Websense Services, User Services potrebbero sembrare interrotti. Per correggere questo problema:

- 1. Riavviare Policy Server di Websense (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Avviare o riavviare User Service di Websense.
- 3. Chiudere Websense Manager.

Attendere 1 minuto prima di ricollegarsi a Websense Manager.

Se l'azione precedente non ha risolto il problema:

 Aprire il visualizzatore degli eventi di Windows oppure il file websense.log per verificare la presenza di messaggi di errore relativi a User Services (vedere Strumenti di diagnostica e risoluzione problemi, pagina 406). Navigare alla directory bin di Websense (C:\Programmi\Websense\bin o /opt/ Websense/bin) ed accertarsi che sia possibile aprire websense.ini in un programma di gestione del testo. Se questo file è stato danneggiato, sostituirlo con un file di backup.

Siti erroneamente categorizzati come Tecnologia informatica

Le versioni 4.0 e successive di Internet Explorer sono in grado di accettare ricerche dalla barra degli indirizzi. Quando questa opzione è attiva, se un utente inserisce il nome di un dominio nella barra degli indirizzi (**websense** anziché **http:**// **www.websense.com**, ad esempio), Internet Explorer considera l'immissione una richiesta di ricerca e non la richiesta di un sito. Visualizza il sito che molto probabilmente l'utente sta cercando, insieme a un elenco di siti corrispondenti in massima parte a quello visualizzato.

Ne consegue che il software Websense autorizza, blocca o limita la richiesta in base allo stato della categoria Tecnologia informatica/Motori di ricerca e Portali dei criteri attivi, non in base alla categoria del sito richiesto. Per fare in modo che il software Websense applichi un filtro in base alla categoria del sito richiesto, occorre disattivare la ricerca dalla barra degli indirizzi:

- 1. Andare a Strumenti > Opzioni Internet.
- 2. Selezionare la scheda Avanzate .
- 3. In Ricerca dalla barra degli indirizzi, selezionare l'opzione che indica di **non** cercare dalla barra degli indirizzi.
- 4. Fare clic su OK.

Nota Queste azioni sono utilizzabili con Internet Explorer versioni 5, 6 e 7.

Le parole chiave non vengono bloccate

Esistono 2 condizioni che possono causare questo problema: l'opzione **Disabilita blocco per parole chiave** è stata selezionata, oppure il sito il cui URL contiene la parola chiave, usa il metodo **POST** per inoltrare i dati al server Web.

Per accertarsi che il blocco in base alle parole chiave sia attivato:

- 1. In Websense Manager, andare a Impostazioni > Filtri.
- In Filtri generici, selezionare l'elenco Opzioni di ricerca per parole chiave. Se Disabilita blocco per parole chiave è visualizzato, selezionare un'altra opzione dall'elenco. Per ulteriori informazioni sulle opzioni disponibili, vedere *Configurazione delle impostazioni di filtraggio di Websense*, pagina 57.
- 3. Fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Se un sito usa il metodo **POST** per inoltrare i dati al server Web, il software Websense non riconosce le impostazioni di filtro in base alle parole chiave per quell'URL. A

meno che il prodotto di integrazione non riconosca i dati inviati con il metodo POST, gli utenti possono sempre accedere agli URL contenenti le parole chiave bloccate.

Per verificare se un sito usa un comando POST, visualizzare l'origine del sito direttamente dal browser. Se il codice sorgente contiene una stringa del tipo **<method=post>**, questo metodo viene utilizzato per caricare quel sito.

Gli URL personalizzati o con un filtro per restrizioni di accesso, non vengono filtrati come previsto.

Se un URL di tipo HTTPS che fa parte di un elenco di filtri per accesso limitato o di URL personalizzati (ricategorizzati o non filtrati), non vengono filtrati come previsto, un prodotto di integrazione potrebbe aver trasformato l'URL in un formato che Filtering Service non riconosce.

I prodotti di integrazione non-proxy traducono gli URL da un formato di dominio a un formato IP. Ad esempio, l'URL **https://<dominio>** viene letto come **https:// <Indirizzo IP>:443**. In questo caso, Filtering Service non trova una corrispondenza dell'URL ricevuto dal prodotto di integrazione con un URL personalizzato o con un filtro per restrizioni di accesso e non filtra quindi il sito in modo corretto.

Per ovviare a questo problema, aggiungere sia gli indirizzi IP sia gli URL dei siti che si vogliono filtrare usando gli URL personalizzati o i filtri per restrizione di accesso.

Un utente non può accedere a un protocollo o un'applicazione come previsto

Se la rete include Microsoft ISA Server, alcune configurazioni dei metodi di autenticazione possono causare connessioni non riuscite con le applicazione di messaggistica.

Se è attivo un metodo diverso dall'Autenticazione anonima, il server proxy tenta di identificare i pacchetti dei dati ricevuti quando gli utenti richiedono la connessione con un'applicazione. Il server proxy non riesce ad identificare il pacchetto dei dati e la connessione non viene completata. Questo potrebbe influire sull'attività di applicazione dei filtri ai protocolli di Websense.

L'impossibilità di accedere a un protocollo o a un'applicazione a Internet potrebbe anche verificarsi se la porta usata dall'applicazione è bloccata. Questo si verifica se:

- La porta è bloccata da un firewall.
- Un protocollo personalizzato bloccato include la porta (come una singola porta o come parte di un intervallo di porte) nei suoi identificatori.

Una richiesta FTP non viene bloccata come previsto

Nel caso di un'integrazione con i firewall Check Point[®], il software Websense richiede l'attivazione della **visualizzazione delle cartelle** nel browser del client al fine di riconoscere e di filtrare le richieste FTP.

Se la visualizzazione delle cartelle non è attivata, le richieste FTP inviate al proxy Fire Wall -1 vengono inviate al software Websense con il prefisso "http://". Come risultato, il software Websense filtra queste richieste come richieste HTTP anziché come richieste FTP.

Il software Websense non applica i criteri previsti per utenti o gruppi

Se il software Websense applica dei criteri al computer o alla rete, o applica il criterio **Predefinito**, anche dopo che i criteri per gli utenti e per i gruppi sono stati assegnati, vedere *Problemi di identificazione utenti*, pagina 376. Nella <u>Knowledge Base</u> sono disponibili ulteriori informazioni.

Gli utenti remoti non vengono filtrati dal criterio corretto

Se un utente remoto accede alla rete usando credenziali di dominio memorizzate nella cache (informazioni di accesso alla rete), il software Websense applica, se necessario, il criterio assegnato a quell'utente, o al gruppo o al dominio di quell'utente. Se non sono stati assegnati dei criteri all'utente, al gruppo o al dominio, o se l'utente si collega al computer con un account di utente locale, il software Websense applica il criterio predefinito.

A volte un utente non viene filtrato da un criterio per utenti o per gruppi o da un criterio predefinito. Questo si verifica se l'utente accede al computer remoto tramite un account utente locale e se l'ultima porzione dell'indirizzo Media Access Control (MAC) del computer remoto si sovrappone a un indirizzo IP su rete al quale è stato assegnato un criterio. In questo caso, il criterio assegnato a quel particolare indirizzo IP viene applicato all'utente remoto.

Problemi con Network Agent

- Network Agent non è stato installato, pagina 373
- Network Agent non è in esecuzione, pagina 374
- Network Agent non sta monitorando le schede NIC., pagina 374
- Network Agent non può comunicare con Filtering Service., pagina 375

Network Agent non è stato installato

Occorre aver installato Network Agent per poter attivare i filtri di protocollo. In alcuni casi di integrazione, Network Agent viene anche utilizzato per ottenere registrazioni più accurate.

Se è in esecuzione un prodotto di integrazione e non si richiede il filtraggio o la registrazione di un protocollo da parte di Network Agent, si può nascondere il

messaggio "Network Agent non installato". Per istruzioni, vedere *Revisione dello stato del sistema in uso*, pagina 299.

Per installazioni autonome, è necessario aver installato Network Agent per il monitoraggio e filtro del traffico di rete. Per istruzioni di installazione, vedere la *Installation Guide* e vedere *Configurazione di Network Agent*, pagina 351.

Network Agent non è in esecuzione

Occorre aver installato Network Agent per poter attivare i filtri di protocollo. In alcuni casi di integrazione, Network Agent viene anche utilizzato per ottenere registrazioni più accurate.

Per installazioni autonome, Network Agent deve essere in esecuzione per poter monitorare e filtrare il traffico di rete.

Per diagnosticare e risolvere questo problema:

- 1. Aprire la finestra di dialogo Windows Services (vedere *Finestra di dialogo Servizi di Windows*, pagina 406) per verificare se il servizio **Websense Network Agent** è stato avviato.
- 2. Riavviare i servizi **Policy Broker** e **Policy Server** di Websense (vedere *Chiusura* e riavvio dei servizi di Websense, pagina 290).
- 3. Avviare o riavviare il servizio Websense Network Agent .
- 4. Chiudere Websense Manager.
- 5. Attendere 1 minuto e quindi ricollegarsi a Websense Manager.

Se questo non risolve il problema:

- Aprire il visualizzatore degli eventi di Windows per verificare la presenza di messaggi di errore di Network Agent (vedere *Visualizzatore eventi di Windows*, pagina 406).
- Aprire **Websense.log** per verificare la presenza di messaggi di errore relativi a Network Agent (vedere *File di registro di Websense*, pagina 407).

Network Agent non sta monitorando le schede NIC.

È necessario associare Network Agent con almeno una scheda di interfaccia di rete (NIC) per poter monitorare il traffico di rete.

Se si aggiungono o si rimuovono schede dal computer con Network Agent, occorre aggiornare la configurazione di Network Agent.

- 1. In Websense Manager, andare a Impostazioni.
- 2. Nel riquadro di navigazione di sinistra, in Network Agent, selezionare l'indirizzo IP del computer Network Agent.
- 3. Verificare che tutte le schede NIC del computer selezionato siano incluse nell'elenco.

4. Verificare che almeno una scheda NIC sia stata definita per il monitoraggio del traffico.

Per ulteriori informazioni, vedere Configurazione di Network Agent, pagina 351.

Network Agent non può comunicare con Filtering Service.

Network Agent deve essere in grado di comunicare con Filtering Service per applicare i criteri relativi all'utilizzo di Internet.

• Si è cambiato l'indirizzo IP del computer con installato Filtering Service o si è reinstallato Filtering Service?

In questo caso, vedere *Aggiornamento dell'indirizzo IP o delle informazioni* sull'identificatore interno (UID) di Filtering Service., pagina 375.

• Si dispone di più di 2 schede di interfaccia di rete (NIC) nel computer con installato Network Agent?

In questo caso, vedere *Configurazione della rete*, pagina 349 per verificare le impostazioni del software Websense.

• Si è riconfigurato lo switch collegato a Network Agent?

In questo caso, fare riferimento alla *Installation guide* per verificare l'impostazione hardware e vedere *Configurazione di Network Agent*, pagina 351 per verificare le impostazioni di Websense.

Se nessuna di queste impostazioni è applicabile, vedere *Configurazione delle impostazioni locali*, pagina 353 per informazioni su come associare Network Agent a Filtering Service.

Aggiornamento dell'indirizzo IP o delle informazioni sull'identificatore interno (UID) di Filtering Service.

Se Filtering Service è stato disinstallato e reinstallato, Network Agent non aggiorna automaticamente l'identificatore interno (UID) per Filtering Service. Websense Manager cerca di eseguire una query di Filtering Service usando il vecchio identificatore interno che non esiste più.

Analogamente, se si cambia l'indirizzo IP del computer con installato Filtering Service, questa modifica non viene automaticamente registrata.

Per ristabilire il collegamento con Filtering Service:

1. Aprire Websense Manager.

Un messaggio di stato indica che un'istanza di Network Agent è incapace di collegarsi a Filtering Service.

- 2. Fare clic su Impostazioni nell'area superiore del riquadro di navigazione.
- 3. Nel riquadro di navigazione di sinistra, in Network Agent, selezionare l'indirizzo IP del computer con Network Agent.

- 4. Nell'area superiore della pagina, in Definizione di Filtering Service, espandere l'elenco **Indirizzo IP del server** e selezionare quindi l'indirizzo IP del computer con installato Filtering Service.
- 5. Fare clic su **OK** nell'area inferiore della pagina per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Problemi di identificazione utenti

Argomenti correlati:

- *Problemi di filtro*, pagina 369
- Agli utenti remoti non viene richiesta l'autenticazione manuale, pagina 386
- Gli utenti remoti non vengono filtrati correttamente, pagina 386

Se il software usa criteri per i computer o per la rete, o il criterio **Predefinito**, per filtrare richieste di accesso a Internet, anche dopo aver assegnato dei criteri basati sugli utenti o sui gruppi, oppure se si sta applicando un criterio non corretto, basato su un utente o su un gruppo, seguire la procedura seguente per identificare il problema:

- Se si sta usando Microsoft ISA Server e si cambia il metodo di autenticazione, accertarsi di riavviare Web Proxy Server.
- Se si stanno usando gruppi nidificati in Windows Active Directory, i criteri assegnati a un gruppo principale vengono applicati agli utenti che appartengono a un sottogruppo e non direttamente al gruppo principale. Per informazioni sulle gerarchie di utenti e di gruppi, vedere la documentazione del servizio di directory.
- La cache di User Service potrebbe essere obsoleta. User Service tiene memorizzati nella cache i mapping di nome utente e indirizzi IP per 3 ore. È possibile forzare l'aggiornamento della cache di User Service memorizzando nella cache le modifiche apportate a Websense Manager e facendo quindi clic su Salva tutto.
- Se un utente viene filtrato in modo erroneo in un computer con Windows XP SP2, il problema potrebbe essere dovuto a Windows Internet Connection Firewall (ICF) il quale viene incorporato e attivato per predefinizione in Windows XP-SP2. Per ulteriori informazioni su Windows ICF, vedere Microsoft Knowledge Base Article n.320855

Per fare in modo che DC Agent o Logon Agent utilizzino informazioni di accesso da un computer dotato di Windows XP SP2:

- Da Windows, fare clic sul menu Start del computer client e selezionare quindi Impostazioni > Pannello di controllo > Centro sicurezza > Windows Firewall.
- 2. Selezionare la scheda Eccezioni .

- 3. Aprire File e Condivisione stampante.
- 4. Fare clic su **OK** per chiudere la finestra di dialogo ICF e quindi chiudere le altre finestre aperte.

Se si sta usando un agente di identificazione trasparente di Windows, consultare la relativa sezione di diagnostica/risoluzione problemi:

- *Diagnostica/risoluzione problemi di DC Agent*, pagina 377.
- Diagnostica/risoluzione problemi di Logon Agent, pagina 379.
- *Diagnostica/risoluzione problemi di eDirectory Agent*, pagina 381.
- Diagnostica/risoluzione problemi di RADIUS Agent, pagina 384.

Diagnostica/risoluzione problemi di DC Agent

Per diagnosticare/risolvere problemi di identificazione utenti con DC Agent:

- 1. Controllare tutte le connessioni di rete.
- 2. Aprire il visualizzatore eventi di Windows per verificare la presenza di messaggi di errore (vedere *Visualizzatore eventi di Windows*, pagina 406).
- 3. Aprire **Websense.log** per accedere a informazioni di errore dettagliate (vedere *File di registro di Websense*, pagina 407).

Le cause comuni di problemi di identificazione utente in DC Agent includono:

- I servizi di rete o i servizi di Windows stanno comunicando con il controller di domini in modo che DC Agent possa vedere il servizio come un nuovo utente per il quale non è stato definito alcun criterio. Vedere *Gli utenti vengono erroneamente filtrati dal criterio Predefinito*, pagina 377.
- DC Agent o User Service potrebbero essere stati installati come un servizio usando l'account Ospite, equivalente a un utente anonimo nel caso del controller di dominio. Se il controller di dominio è stato impostato in modo da non visualizzare l'elenco di utenti e di gruppi per un utente anonimo, a DC Agent non è consentito scaricare l'elenco. Vedere *Modifica manuale delle autorizzazioni di DC Agent e User Services*, pagina 378.
- La cache di User Service è obsoleta. User Service tiene memorizzati nella cache i mapping di nomi utente e indirizzi IP per 3 ore. La cache viene aggiornata ogni volta che si apportano modifiche e si fa clic su **Salva tutto** in Websense Manager.

Gli utenti vengono erroneamente filtrati dal criterio Predefinito

Se una rete o Microsoft Windows 200x contattano il controller di dominio, il nome dell'account da loro usato potrebbe comportare che il software Websense pensi che un utente non identificato stia accedendo a Internet dal computer filtrato. Poiché nessun criterio basato sull'utente o sul gruppo è stato assegnato a questo utente, vengono applicati il criterio di computer o di rete o il criterio Predefinito.

 Potrebbe essere necessario che i servizi di rete dispongano dei privilegi di dominio per poter accedere ai dati su rete e che utilizzino il nome utente del dominio in cui vengono eseguiti, per poter contattare il controller di dominio. Per ovviare a questo problema, vedere *Configurazione di un agente affinché ignori determinati nomi utente*, pagina 239.

 I servizi di Windows 200x contattano il controller di dominio periodicamente con un nome utente costituito dal nome del computer seguito dal simbolo del dollaro (NomeUtente-computer\$). DC Agent interpreta il servizio come un nuovo utente al quale non è stato assegnato alcun criterio.

Per ovviare a questo problema, configurare DC Agent in modo che ignori qualsiasi accesso in linea che usi **computer\$**.

- 1. Nel computer con DC Agent, navigare alla directory **bin** di Websense (per predefinizione, **C:\Programmi \Websense\bin**).
- 2. Aprire il file transid.ini in un programma di gestione del testo.
- 3. Aggiungere la seguente voce al file:

IgnoreDollarSign=true

- 4. Salvare e chiudere il file.
- 5. Riavviare DC Agent (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

Modifica manuale delle autorizzazioni di DC Agent e User Services

Nel computer in cui è in esecuzione il controller di dominio:

1. Creare un account utente come ad esempio **Websense**. Si può usare un account esistente, ma un account Websense è preferibile per impostare la password senza una scadenza. Non sono necessari privilegi speciali.

Impostare la password senza una scadenza. Questo account costituisce un contesto di sicurezza per l'accesso agli oggetti della directory.

Prendere nota del nome utente e della password stabiliti per questo account in quanto devono venire inseriti con le operazioni descritte al punto 6 e 7.

- Aprire la finestra di dialogo Servizi di Windows su ciascun computer DC Agent di Websense (andare a Start > Programmi > Strumenti amministrativi > Servizi).
- 3. Selezionare la voce Websense DC Agent e fare clic su Interrompi.
- 4. Fare doppio clic sulla voce Websense DC Agent.
- 5. Nella scheda Accedi, selezionare l'opzione Questo account.
- 6. Inserire il nome utente dell'account Websense DC Agent creato al punto 1. Ad esempio: NomeDominio\websense.
- 7. Inserire e confermare la password di Windows per questo account.
- 8. Fare clic su **OK** per chiudere la finestra di dialogo.
- 9. Selezionare la voce Websense DC Agent nella finestra di dialogo Servizi e fare quindi clic su Start.
- 10. Ripetere questa procedura per ciascuna istanza di Websense User Service.

Diagnostica/risoluzione problemi di Logon Agent

Se alcuni utenti della rete vengono filtrati dal criterio **Predefinito**, Logon Agent non sarà in grado di identificarli:

- Verificare che Windows Group Policy Objects (GPO) siano stati applicati correttamente ai computer di questi utenti (vedere Oggetti Criteri di gruppo (Group Policy Objects), pagina 379).
- Se User Service è stato installato in un computer Linux e si sta usando Windows Active Directory (modalità nativa), aprire la configurazione del servizio di directory (vedere User Service in esecuzione su Linux, pagina 380).
- Verificare che il computer client possa comunicare con il controller di dominio dal quale è in esecuzione lo script di accesso (vedere *Visibilità del controller di dominio*, pagina 380).
- Verificare che NetBIOS sia attivato nel computer client (vedere *NetBIOS*, pagina 380).
- Verificare che il profilo utente nel computer client non sia danneggiato (vedere *Problemi di profilo utente*, pagina 381).

Oggetti Criteri di gruppo (Group Policy Objects)

Dopo aver verificato che il proprio ambiente informatico soddisfa i prerequisiti descritti nella *Installation Guide* per il software Websense, accertarsi che gli Oggetti Criteri di gruppo siano stati applicati correttamente:

- 1. Nel computer con Active Directory, aprire il Pannello di controllo di Windows e andare a **Strumenti amministrativi > Utenti e gruppi di Active Directory**.
- 2. Fare clic con il pulsante destro del mouse sulla voce del dominio e selezionare **Proprietà**.
- 3. Fare clic sulla scheda **Criteri di gruppo** e selezionare i criteri di dominio dall'elenco degli oggetti di policy di gruppo del dominio.
- 4. Fare clic su **Modifica** ed espandere quindi il nodo Configurazione utenti del diagramma ad albero della directory Configurazione utenti.
- 5. Espandere il nodo Impostazioni di Windows e selezionare Script.
- 6. Nel riquadro di destra, fare doppio clic su **Accesso** e verificare quindi che **logon.bat** venga elencato nella finestra di dialogo Proprietà di accesso.

Questo script è richiesto da Applicazione di accesso del client.

- Se **logon.bat** non fa parte dello script, fare riferimento al capitolo *Initial Setup* [Configurazione iniziale] della Installation Guide del software Websense.
- Se logon.bat è incluso nello script, ma Logon Agent non funziona, adottare le procedure supplementari di diagnostica/risoluzione problemi di questa sezione per accertare che non esista un problema di connettività di rete, oppure fare riferimento alla <u>Knowledge Base</u> di Websense.

User Service in esecuzione su Linux

Se si utilizza Logon Agent per l'identificazione trasparente degli utenti e User Service è stato installato su un computer con Linux, occorre configurare temporaneamente il software Websense affinché comunichi con Active Directory in Mixed Mode.

- 1. In Websense Manager, andare a Impostazioni > Servizi di directory.
- 2. Prendere nota delle impostazioni di directory definite.
- 3. In Directory, selezionare NT Directory / Active Directory (Mixed Mode) di Windows.
- 4. Fare clic su **OK** per salvare le modifiche nella cache e fare quindi clic su **Salva** tutto.
- In Directory, selezionare Active Directory (Native Mode). Se la configurazione originale non viene visualizzata, usare le annotazioni prese al punto 2 per ricreare le impostazioni della directory. Vedere Active Directory di Windows (modalità nativa), pagina 65 per istruzioni dettagliate.
- 6. Una volta terminate le modifiche della configurazione, fare clic su **OK** e quindi su **Salva tutto**.

Visibilità del controller di dominio

Per verificare che il computer client possa comunicare con il controller del dominio :

- 1. Provare a mappare un'unità del computer client all'unità condivisa di base del controller di dominio. Qui è dove lo script di accesso viene normalmente eseguito e dove risiede **LogonApp.exe**.
- 2. Nel computer client, aprire un prompt di comando di Windows ed eseguire il comando seguente:

net view /domain:<nome dominio>

Se una o entrambe queste prove non riescono, vedere la documentazione del sistema operativo di Windows per possibili soluzioni. Esiste un problema di connettività di rete non associata al software Websense.

NetBIOS

NetBIOS per TCP/IP deve essere attivato e il servizio TCP/IP NetBIOS Helper deve essere in esecuzione affinché lo script di accesso di Websense possa venire eseguito nel computer dell'utente.

Per accertare che NetBIOS per TCP/IP sia attivato nel computer client:

- 1. Fare clic con il pulsante destro del mouse su **Risorse di rete** e selezionare quindi **Proprietà**.
- 2. Fare clic con il pulsante destro del mouse su **Connessione alla rete locale** e selezionare quindi **Proprietà**.
- 3. Selezionare Protocollo Internet (TCP/IP) e selezionare quindi Proprietà.
- 4. Fare clic su Avanzate.

- 5. Selezionare la scheda **WINS** e verificare che sia stata impostata l'opzione corretta NetBIOS.
- 6. Se si fa una modifica, fare clic su **OK** e quindi su **OK** due volte per chiudere le diverse finestre di dialogo Proprietà e per salvare le modifiche.

Se non necessitano modifiche, fare clic su **Annulla** per chiudere ciascuna finestra di dialogo senza apportare alcuna modifica.

Usare la finestra di dialogo Servizi Windows per verificare se il servizio **TCP/IP NetBIOS Helper** è in esecuzione nel computer client (vedere *Finestra di dialogo Servizi di Windows*, pagina 406). Il servizio TCP/IP NetBIOS Helper è eseguibile in Windows 2000, Windows XP, Windows Server 2003 e Windows NT.

Problemi di profilo utente

Se il profilo utente nel computer client è danneggiato, lo script di accesso a Websense e le impostazioni di GOP - Group Policy Objects, non possono essere eseguite. Questo problema può essere risolto ricreando il profilo utente.

Se si ricrea un profilo utente, la cartella Documenti, Preferiti e altri dati e impostazioni personalizzati non verranno automaticamente trasferiti al nuovo profilo. Non eliminare il profilo esistente e danneggiato fino a quando il nuovo profilo non ha risolto il problema e non ha copiato i dati esistenti dell'utente nel nuovo profilo.

Per ricreare il profilo utente:

- 1. Accedere al computer client come amministratore locale:
- 2. Assegnare un nuovo nome alla directory che contiene il profilo utente:

C:\Documenti e impostazioni\<nome utente>

- 3. Riavviare il computer.
- 4. Accedere al computer come utente filtrato. Viene creato automaticamente un profilo utente.
- 5. Verificare che l'utente venga filtrato come previsto.
- 6. Copiare i dati personalizzati (come ad esempio il contenuto della cartella Documenti) dal vecchio profilo a quello nuovo. Non usare il Trasferimento guidato file e impostazioni, in quanto si potrebbe trasferire il danno subito al nuovo profilo.

Diagnostica/risoluzione problemi di eDirectory Agent

Argomenti correlati:

- Attivazione della diagnostica di eDirectory Agent, pagina 382
- *eDirectory Agent calcola erroneamente le connessioni con il server eDirectory*, pagina 383
- Esecuzione di eDirectory Agent in modalità console, pagina 384

L'utente potrebbe non venire filtrato adeguatamente se il nome utente non viene passato a eDirectory Agent. Se un utente non accede al server con Novell Directory, eDirectory Agent non può rilevare l'accesso. Questo accade in quanto:

- Un utente accede a un dominio non incluso nel contesto principale predefinito per le sessioni di accesso a eDirectory. Questo contesto principale viene specificato durante l'installazione e dovrebbe corrispondere al contesto principale specificato per Novell eDirectory nella pagina Impostazioni > Servizi di directory.
- Un utente tenta di aggirare il prompt di accesso per evitare i filtri di Websense.
- Un utente non possiede un account nel server di eDirectory.

Se un utente non accede al server di eDirectory, i criteri specifici per l'utente non possono venire applicati a quell'utente. Il criterio **Predefinito** entra invece in effetto. Se esistono stazioni di lavoro condivise nella rete a cui gli utenti si collegano anonimamente, impostare un criterio di filtro per questi computer particolari.

Per determinare se eDirectory Agent deve ricevere un nome utente e identificare quell'utente:

- 1. Attivare l'accesso a eDirectory Agent, come descritto in *Attivazione della diagnostica di eDirectory Agent*, pagina 382.
- 2. Aprire il file di registro specificato in un programma di gestione del testo.
- 3. Cercare una voce corrispondente all'utente a cui si sta applicando un filtro incorrettamente.
- 4. Una voce come quella riportata qui di seguito indica che eDirectory Agent ha identificato un utente:

```
WsUserData::WsUserData()
Utente: cn=Admin,o=novell (10.202.4.78)
WsUserData::~WsUserData()
```

Nell'esempio qui sopra, l'utente **Amministratore** ha acceduto al server di eDirectory ed è stato identificato correttamente.

5. Se un utente viene identificato ma non viene filtrato come previsto, verificare la propria configurazione criteri per confermare che il criterio corretto sia stato applicato all'utente e che il nome utente definito in Websense Manager corrisponda al nome utente definito in Novell Directory.

Se l'utente non viene identificato, verificare che:

- l'utente abbia un account in Novell Directory.
- l'utente acceda a un dominio incluso nel contesto principale predefinito per gli accessi degli utenti a eDirectory.
- l'utente non stia aggirando un prompt di accesso.

Attivazione della diagnostica di eDirectory Agent

eDirectory Agent dispone di funzioni diagnostiche incorporate che non vengono attivate per predefinizione. È possibile attivare le operazioni di accesso e di debug durante l'installazione o in qualsiasi altro momento.

- 1. Interrompere eDirectory Agent (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Dal computer con installato eDirectory Agent andare alla directory di installazione di eDirectory Agent.
- 3. Aprire il file **wsedir.ini** in un programma di gestione del testo.
- 4. Individuare la sezione [eDirAgent].
- 5. Per attivare l'accesso e il debug, modificare il valore di **DebugMode** impostandolo su **On**:

DebugMode=On

6. Per specificare il livello di dettagli della registrazione, modificare la riga seguente:

```
DebugLevel=<N>
```

N può essere un valore compreso tra 0 e 3, dove 3 indica il livello di dettagli più alto.

7. Modificare la riga **LogFile** per specificare il nome del file di output di registro (log output file):

LogFile=filename.txt

Per predefinizione, l'output di registro viene inviato alla console di eDirectory Agent. Se l'esecuzione dell'agente è in modalità console (vedere *Esecuzione di eDirectory Agent in modalità console*, pagina 384), è possibile mantenere il valore predefinito.

- 8. Salvare e chiudere il file wsedir.ini.
- 9. Avviare il servizio eDirectory Agent (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

eDirectory Agent calcola erroneamente le connessioni con il server eDirectory

Se eDirectory Agent sta monitorando più di 1000 utenti in rete, ma visualizza soltanto 1000 connessioni al server Novell eDirectory, ciò potrebbe essere dovuto a una limitazione di Windows API che invia informazioni dal server di eDirectory a Websense eDirectory Agent. Questo accade molto raramente.

Per ovviare a questa limitazione, aggiungere un parametro al file **wsedir.ini** che calcola correttamente le connessioni al server (Windows soltanto):

- 1. Interrompere il servizio eDirectory Agent di Websense (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Andare alla directory **bin** di Websense (per predefinizione, **C:\Programmi\Websense\bin**).
- 3. Aprire il file **wsedir.ini** in un programma di gestione del testo.
- 4. Inserire una riga vuota e quindi inserire:

```
MaxConnNumber = <NNNN>
```

<*NNNN>* rappresenta qui il numero massimo di connessioni consentite per il server Novell eDirectory. Ad esempio, se la rete dispone di 1950 utenti, si può immettere 2000 come numero massimo.

- 5. Salvare il file.
- 6. Riavviare eDirectory Agent.

Esecuzione di eDirectory Agent in modalità console

- 1. Eseguire una delle operazioni seguenti:
 - Al prompt di comando di Windows (Start > Esegui > cmd), inserire il comando:

eDirectoryAgent.exe -c

- Al prompt di comando Shell di Linux, inserire il comando seguente:
 eDirectoryAgent -c
- 2. Quando si è pronti a interrompere l'agente, fare clic su **Invio**. L'interruzione dell'esecuzione dell'agente potrebbe richiedere qualche secondo.

Diagnostica/risoluzione problemi di RADIUS Agent

RADIUS Agent dispone di funzioni di diagnostica incorporate che non sono attive per predefinizione. Per attivare la registrazione e il debug di RADIUS Agent:

- 1. Interrompere il servizio RADIUS Agent (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Nel computer con installato RADIUS Agent, andare alla directory di installazione dell'agente (per predefinizione, **Websense\bin**\).
- 3. Aprire il file **wsradius.ini** in un programma di gestione del testo.
- 4. Individuare la sezione RADIUSAgent.
- 5. Per attivare l'accesso e il debug, modificare il valore di **DebugMode** impostandolo su **On**:

DebugMode=On

6. Per specificare il livello di dettagli della registrazione, modificare la riga seguente:

```
DebugLevel=<N>
```

N può essere un valore compreso tra 0 e 3, dove 3 indica il livello di dettagli più alto.

7. Modificare la riga LogFile per specificare il nome del file di output:

```
LogFile=filename.txt
```

Per predefinizione, l'output di registro viene inviato alla console di RADIUS Agent. Se l'esecuzione dell'agente è in modalità console (vedere *Esecuzione di RADIUS Agent in modalità console*, pagina 385), è possibile mantenere il valore predefinito.

8. Salvare e chiudere il file wsradius.ini.

9. Avviare il servizio RADIUS Agent (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).

Se gli utenti remoti non vengono identificati e filtrati come previsto, la causa più frequente è da attribuire a problemi di comunicazione tra RADIUS Agent e il server RADIUS. Verificare i registri di RADIUS Agent per determinare la causa.

Esecuzione di RADIUS Agent in modalità console

Per avviare RADIUS Agent in modalità console (come un'applicazione), inserire quanto segue:

• Al prompt di comando di Windows:

RadiusAgent.exe -c

• Al prompt di comando Shell di Windows:

./RadiusAgent -c

Per interrompere l'agente in qualsiasi momento, premere ancora **Invio**. L'interruzione dell'esecuzione dell'agente potrebbe richiedere un paio di secondi.

RADIUS Agent accetta i seguenti parametri per le righe di comando:



Per Linux, Websense, Inc. consiglia di usare lo script fornito per l'avvio o l'interruzione di Websense RADIUS Agent (**WsRADIUSAgent start**|**stop**), anziché i parametri -r e -s.

Parametro	Descrizione
-i	Installa il servizio/daemon RADIUS Agent
-r	Esegue il servizio/daemon RADIUS Agent
-S	Interrompe il servizio/daemon RADIUS Agent
-c	Esegue RADIUS Agent come un processo applicativo anziché come un servizio o un daemon. In modalità console, RADIUS Agent può venire configurato per inviare output di registro alla console o a un file di testo.
-V	Visualizza il numero di versione di RADIUS Agent.
-? -h -help < <i>no option</i> >	Visualizza informazioni sull'uso nella riga di comando. Elenca e descrive tutti i possibili parametri delle righe di comando.

Agli utenti remoti non viene richiesta l'autenticazione manuale

Se gli utenti remoti sono stati configurati per un'autenticazione manuale quando accedono a Internet, potrebbe accadere che non venga richiesta l'autenticazione ai singoli utenti. Questo può accadere in situazioni in cui alcuni indirizzi IP di rete sono stati configurati per aggirare l'autenticazione manuale.

Se un utente remoto accede alla rete, il software Websense legge l'ultima porzione dell'indirizzo Media Access Control (MAC) del computer. Se questo corrisponde all'indirizzo IP di rete configurato per ovviare a tale autenticazione, all'utente remoto non verrà richiesta l'autenticazione manuale quando accede a Internet.

Una possibile soluzione è quella di riconfigurare l'indirizzo IP di rete in modo da usare un'autenticazione manuale. Una soluzione alternativa è quella di disattivare il requisito di autenticazione manuale per l'utente remoto in questione.

Gli utenti remoti non vengono filtrati correttamente

Se gli utenti remoti non vengono filtrati, o non vengono filtrati tramite particolari criteri ad essi assegnati, controllare la presenza, nei registri di RADIUS Agent, del messaggio "Error receiving from server: 10060" (Windows) oppure "Error receiving from server: 0" (Linux).

Questo si verifica di solito se il server RADIUS non riconosce RADIUS Agent come client (origine delle richieste RADIUS). Verificare che il server RADIUS sia stato configurato correttamente (vedere *Configurazione dell'ambiente RADIUS*, pagina 225)

È possibile usare lo strumento diagnostico incorporato di RADIUS Agent per diagnosticare/risolvere problemi di filtraggio (vedere *Diagnostica/risoluzione problemi di RADIUS Agent*, pagina 384).

Se si è implementata la funzione Filtro remoto (vedere *Filtro per i client remoti*, pagina 161), gli utenti remoti non possono venire filtrati se il client Remote Filtering non può comunicare con Remote Filtering Server all'interno della rete.

Per istruzioni su come configurare Remote Filtering, vedere l'inserto tecnico di *Remote Filtering.*

Problemi dei messaggi di blocco

- Non è stata visualizzata una pagina di blocco per un determinato tipo di file bloccato, pagina 387
- Gli utenti ricevono un errore di browser anziché una pagina di blocco., pagina 387
- Viene visualizzata una pagina bianca vuota anziché una pagina di blocco, pagina 388

- I messaggi di blocco del protocollo non vengono visualizzati come previsto, pagina 388
- Viene visualizzato un messaggio di blocco del protocollo anziché una pagina di blocco, pagina 389

Non è stata visualizzata una pagina di blocco per un determinato tipo di file bloccato

Se si utilizza il blocco in base al tipo di file, il messaggio di blocco potrebbe non essere visibile per l'utente. Ad esempio, se un file scaricabile è contenuto in un frame (IFRAME) di un sito a cui è consentito accedere, il messaggio di blocco inviato a quel frame non è visibile in quanto le dimensioni del frame sono pari a 0.

Questo è soltanto un problema di visualizzazione; gli utenti non possono comunque accedere o scaricare il file bloccato.

Gli utenti ricevono un errore di browser anziché una pagina di blocco.

Se gli utenti ricevono un messaggio di errore anziché una pagina di blocco, le 2 cause più comuni sono:

- Il browser dell'utente è configurato per l'uso di un proxy esterno. La maggior parte dei browser dispone di un'impostazione che consente l'uso di un proxy esterno. Verificare che il browser non sia stato configurato per l'uso di un proxy esterno.
- Si è verificato un problema di identificazione o di comunicazione con il computer in cui è installato Filtering Service.

Se le impostazioni del browser dell'utente sono corrette, accertarsi che l'indirizzo IP del computer con Filtering Service appaia correttamente nell'elenco del file **eimserver.ini**.

- 1. Chiudere **Websense Filtering Service** (vedere *Chiusura e riavvio dei servizi di Websense*, pagina 290).
- 2. Navigare alla directory **bin** di Websense (per predefinizione, \Programmi\Websense\bin o /opt/websense/bin).
- 3. Aprire il file eimserver.ini in un programma di gestione del testo.
- 4. In [WebsenseServer], aggiungere una riga vuota ed inserire quanto segue:

BlockMsgServerName = <>

Ad esempio, se l'indirizzo IP di Filtering Service è 10.201.72.15, inserire:

BlockMsgServerName = 10.201.72.15

- 5. Salvare e chiudere il file.
- 6. Riavviare Filtering Service.

Se il computer con Filtering Service dispone di più di una scheda NIC, e la pagina di blocco non viene visualizzata correttamente dopo aver modificato il file **eimserver.ini**, provare gli indirizzi IP delle altre schede NIC del parametro **BlockMsgServerName**.

Se la pagina di blocco non viene visualizzata, accertarsi che gli utenti abbiano accesso di lettura ai file nelle directory della pagina di blocco di Websense:

- Websense\BlockPages\en\Default
- Websense\BlockPages\en\Custom

Se i problemi della pagina di blocco non vengono risolti, consultare la Websense Knowledge Base per ulteriori istruzioni di diagnostica/risoluzione problemi.

Viene visualizzata una pagina bianca vuota anziché una pagina di blocco

Se gli avvisi pubblicitari vengono bloccati, o un browser non rileva correttamente la codifica associata a una pagina di blocco, gli utenti potrebbero ricevere una pagina bianca vuota anziché una pagina di blocco. I motivi di questa condizione sono i seguenti:

- Se la categoria Pubblicità è bloccata, il software Websense interpreta a volte la richiesta di un file di immagine grafica come una richiesta di pubblicità e quindi visualizza un'immagine vuota anziché un messaggio di blocco (il metodo normalmente usato per il blocco di avvisi pubblicitari). Se l'URL richiesto termina con .gif o simile estensione, l'utente dovrà reinserire l'URL, senza includere l'estensione *.gif.
- Alcuni browser di più vecchia data non riconoscono la codifica delle pagine di blocco. Per consentire la rilevazione dei caratteri, configurare il browser in modo che visualizzi il set di caratteri appropriati (UTF-8 per il francese, tedesco, italiano, spagnolo, portoghese brasiliano, cinese semplificato, cinese tradizionale o coreano; e Shift_JIS per il giapponese). Consultare la documentazione del browser per istruzioni oppure aggiornare il browser ad una versione più recente.

I messaggi di blocco del protocollo non vengono visualizzati come previsto

I messaggi di blocco del protocollo potrebbero non venire visualizzati o potrebbero venire visualizzati soltanto dopo un ritardo per una delle ragioni seguenti:

- User Service deve essere installato in un computer Windows affinché i messaggi di blocco del protocollo vengano correttamente visualizzati. Per ulteriori informazioni, vedere la *Installation Guide*.
- I messaggi di blocco del protocollo potrebbero non raggiungere i computer client se Network Agent è stato installato in un computer con molteplici schede di interfaccia di rete (NIC) e se una scheda NIC sta monitorando un segmento di rete diverso da Filtering Service. Accertarsi che il computer con Filtering Service

disponga del protocollo NetBIOS e blocco del messaggio del server, per l'accesso ai computer client e che la porta 15871 non sia bloccata.

- Un messaggio di blocco del protocollo potrebbe avere un lieve ritardo o venire visualizzato in un computer interno dal quale era stata originata la richiesta di dati di protocollo (anziché in un computer client), se Network Agent è stato configurato per monitorare le richieste inviate a computer interni.
- Se il client filtrato o il computer con i filtri di Websense è dotato di Windows 200x, il Messenger Service di Windows deve essere in esecuzione affinché il messaggio di blocco del protocollo possa venire visualizzato. Usare la finestra di dialogo Servizi di Windows in un computer client o server, per verificare se il Messanger Service è in esecuzione (vedere *Finestra di dialogo Servizi di Windows*, pagina 406). Anche se il messaggio di blocco non viene visualizzato, le richieste di protocollo sono sempre bloccate.

Viene visualizzato un messaggio di blocco del protocollo anziché una pagina di blocco

Se il prodotto di integrazione non invia informazioni HTTPS al software Websense o se il software Websense è in esecuzione in modalità autonoma, Network Agent potrebbe interpretare la richiesta di accesso a un sito HTTPS, bloccata tramite le impostazioni per le categorie, come una richiesta di protocollo. In questo caso, viene visualizzato un messaggio di blocco del protocollo. Anche la richiesta HTTPS viene registrata come una richiesta di protocollo.

Problemi di registro, di messaggi di stato e di avvisi di errore

- Dove posso trovare i messaggi di errore dei componenti Websense?, pagina 389
- Avvisi di errore di integrità Websense, pagina 390
- Vengono generati due record di registro per una singola richiesta, pagina 391

Dove posso trovare i messaggi di errore dei componenti Websense?

Se vengono visualizzati messaggi di errore o avvertenze associati ai componenti di base di Websense, verranno anche visualizzati brevi avvisi di errore nell'elenco **Riepilogo avvisi di integrità** nell'area superiore della pagina **Stato > Oggi** di Websense Manager (vedere *Avvisi di errore di integrità Websense*, pagina 390).

- Fare clic sull'avviso di errore per visualizzare ulteriori informazioni nella pagina Stato > Avvisi.
- Per informazioni di diagnostica/soluzione problemi, fare clic su Soluzioni, accanto a un messaggio visualizzato nella pagina Stato > Avvisi.

Gli errori, avvertenze e messaggi generati dai componenti del software Websense, così come i messaggi sullo stato di avanzamento dei download del database, vengono registrati nel file **websense.log** della directory Websense **bin** (per predefinizione, C:\Programmi\Websense\bin oppure /opt/Websense/bin). Vedere *File di registro di Websense*, pagina 407.

Nel caso di componenti software di Websense installati nei computer con Windows, è anche possibile controllare il Visualizzatore eventi di Windows. Vedere *Visualizzatore eventi di Windows*, pagina 406.

Avvisi di errore di integrità Websense

L'elenco Riepilogo avvisi di integrità riporta problemi potenziali incontrati dai componenti monitorati del software Websense. Questi includono:

- Filtering Service non in esecuzione
- User Service non è disponibile
- Log Server non in esecuzione
- Log Server non configurato per Policy Server
- Database di registrazione non disponibile
- Network Agent non in esecuzione
- Non esiste un Network Agent configurato per un Policy Serve
- Nessuna NIC di monitoraggio configurata per Network Agent
- Nessun Filtering Service configurato per un Network Agent
- l database di filtraggio iniziale è in uso
- 1 Master Database è in corso di scaricamento per la prima volta
- 1 Master Database è in corso di aggiornamento
- Il Master Database risale a più di 1 settimana fa
- I download del Master Database non è stato completato.
- WebCatcher non abilitato
- Si è verificato un problema di sottoscrizione
- La chiave di sottoscrizione sta per scadere.
- Nessuna chiave di sottoscrizione inserita

La pagina degli Avvisi di errore contengono informazioni sulle condizioni di errore o di avvertenza. Fare clic su **Soluzioni** per informazioni su come risolvere il problema.

In alcuni casi, se si stanno ricevendo messaggi di errore o di stato su un determinato componente che non si sta usando o che è stato disattivato, è possibile scegliere di nascondere gli avvisi di errore. Per ulteriori informazioni, vedere *Revisione dello stato del sistema in uso*, pagina 299.

Vengono generati due record di registro per una singola richiesta

Se Windows QoS Packet Scheduler è installato nello stesso computer di Network Agent, vengono registrate due richieste per ciascuna richiesta di HTTP o di protocollo inoltrata dal computer con Network Agent. (Questo duplicato non si verifica nel caso di richieste inoltrate da un computer client all'interno della rete.)

Per risolvere il problema, disattivare Windows QoS Packet Scheduler nel computer con Network Agent.

Questo problema non si verifica se si usa Network Agent per tutte le registrazioni. Per ulteriori informazioni, vedere *Configurazione delle impostazioni della scheda dell'interfaccia di rete (NIC)*, pagina 355.

Problemi di Policy Server e Policy Database

- Password dimenticata, pagina 391
- Non posso collegarmi a Policy Server, pagina 392
- Impossibile avviare il servizio Websense Policy Database, pagina 392

Password dimenticata

Se si ha il ruolo di Super Administrator o di amministratore con delega e si utilizza un account utente di Websense per accedere al Policy Server via Websense Manager, qualsiasi utente con qualifica totale di Super Administrator può ridefinire la password.

- La password di Websense Administrator viene definita su Impostazioni > Account.
- Le password per gli altri account di amministratori vengono definite nella pagina Amministrazione con delega > Gestisci account utente di Websense.

Se non si sta utilizzando l'amministrazione con delega e ci si è dimenticati la password di WebsenseAdmninistrator, collegarsi con MyWebsense per ridefinire la password.

- La chiave di sottoscrizione associata all'account deve corrispondere alla chiave di sottoscrizione di Websense Web Security o di Websense Web Filter.
- Se si possiedono molteplici chiavi di sottoscrizione, occorre selezionare la chiave appropriata di Websense Web Security o di Websense Web Filter affinché la procedura di ripristino della password possa venire completata.
- Occorre avere accesso al computer con installato Websense Manager per completare la procedura di ripristino.

Non posso collegarmi a Policy Server

Verificare che l'indirizzo IP di Policy Server IP sia corretto. Se l'indirizzo IP del computer con installato Policy Server è stato modificato da quando Policy Server era stato aggiunto a Websense Manager, occorrerà collegarsi a un Policy Server diverso, eliminare il vecchio indirizzo IP da Websense Manager e quindi aggiungere il nuovo indirizzo IP di Policy Server. Vedere *Aggiunta e modifica delle istanze di Policy Server*, pagina 283.

Se Websense Manager viene improvvisamente interrotto, o se è stato interrotto tramite i comandi kill (linux) o End Task (Termina attività), attendere qualche minuto e riprovare ad accedere. Il software Websense rileva e chiude la sessione terminata entro 3 minuti.

Impossibile avviare il servizio Websense Policy Database

Impossibile eseguire il servizio Websense Policy Database come un account speciale: **WebsenseDBUser**. Se questo account incontra problemi di accesso, il Policy Database non può essere avviato.

Per risolvere questo problema, modificare la password di WebsenseDBUser.

- 1. Accedere al computer con installato il Policy Database come un amministratore locale.
- 2. Andare a Start > Programmi > Strumenti di amministrazione > Gestione computer.
- 3. Nel riquadro di navigazione, in Strumenti del sistema, espandere Utenti e gruppi locali e selezionare Utenti. Le informazioni sull'utente vengono visualizzate nel riquadro del contenuto.
- 4. Fare clic con il pulsante destro del mouse su **WebsenseDBUser** e selezionare **Imposta password**.
- 5. Inserire e confermare la nuova password per questo account utente e fare clic su **OK**.
- 6. Chiudere la finestra di dialogo Gestione computer.
- 7. Andare a Start > Programmi > Strumenti di amministrazione > Servizi.
- 8. Fare clic con il pulsante destro del mouse su **Websense Policy Database** e selezionare **Proprietà**.
- 9. Nella scheda Accedi della finestra di dialogo Proprietà, inserire le informazioni sulla nuova password WebsenseDBUser e fare clic su **OK**.
- 10. Fare ancora clic con il pulsante destro del mouse su Websense Policy Database e selezionare **Start**.

Una volta avviato il servizio, chiudere la finestra di dialogo Servizi.

Problemi di amministrazione con delega

- I client gestiti non possono venire eliminati da un ruolo, pagina 393
- Un errore di accesso segnala che un altro utente è collegato al mio computer, pagina 393
- Alcuni utenti non possono accedere a un sito dell'elenco URL non filtrati, pagina 393
- I siti ricategorizzati vengono filtrati in base alla categoria errata, pagina 394
- Impossibile creare un protocollo personalizzato, pagina 394

I client gestiti non possono venire eliminati da un ruolo

I client non possono venire eliminati direttamente dall'elenco dei client gestiti della pagina Amministrazione con delega > Modifica ruolo se:

- l'amministratore ha applicato un criterio al client
- l'amministratore ha applicato un criterio a uno o più membri di una rete, di un gruppo, di un dominio o di un'unità organizzativa

Potrebbero anche insorgere problemi se, durante il collegamento con Websense Manager, il Super Administrator sceglie un Policy Server diverso da quello che comunica con il servizio di directory contenente i client da eliminare. In questo caso, il Policy Server e il servizio di directory non riconoscono i client.

Per assistenza riguardo all'eliminazione dei client gestiti, vedere *Eliminazione client gestiti*, pagina 269.

Un errore di accesso segnala che un altro utente è collegato al mio computer

Se si tenta di accedere a Websense Manager, si potrebbe ricevere a volta il messaggio di errore "Accesso non riuscito". Il <nome del ruolo> è in uso da parte di <nome utente>, da <data, ora>, nel computer 127.0.0.1." L'indirizzo IP 127.0.0.1 si chiama anche indirizzo "loopback" e indica normalmente il computer locale.

Questo messaggio significa che qualcun altro è collegato al computer con installato Websense Manager, nello stesso ruolo che si sta richiedendo. Selezionare un ruolo diverso (se si amministrano vari ruoli), collegarsi soltanto a scopo di creazione di report oppure aspettare fino a quando l'altro amministratore si scollega.

Alcuni utenti non possono accedere a un sito dell'elenco URL non filtrati

Gli URL non filtrati incidono soltanto sui client gestiti dal ruolo in cui è consentito aggiungere degli URL. Ad esempio, se un Super Administrator aggiunge degli URL

non filtrati, i client gestiti dai ruoli di amministrazione con delega non verranno autorizzati ad accedere a questi siti.

Per rendere il sito disponibile ai client assegnati ad altri ruoli, il Super Administrator può passare ad ognuno degli altri ruoli e aggiungere i siti rilevanti all'elenco degli URL non filtrati di quel ruolo.

I siti ricategorizzati vengono filtrati in base alla categoria errata

Gli URL ricategorizzati incidono soltanto sui client gestiti dal ruolo a cui vengono aggiunti gli URL. Ad esempio, se un Super Administrator ricategorizza degli URL, i client gestiti dai ruoli di amministrazione con delega continuano a venire filtrati in base alla categoria del Master Database assegnata a quei siti.

Per applicare la ricategorizzazione ai client in altri ruoli, il Super Administrator può passare ad ognuno degli altri ruoli e ricategorizzare i siti rilevanti per quel ruolo.

Impossibile creare un protocollo personalizzato

Soltanto i Super Administrator sono in grado di creare i protocolli personalizzati. Tuttavia, gli amministratori con delega possono definire azioni di filtraggio per i protocolli personalizzati.

Se i Super Administrator creano protocolli personalizzati, devono definire l'azione predefinita appropriata per la maggior parte dei client. Devono quindi informare gli amministratori con delega del nuovo protocollo in modo che possano aggiornare i filtri per il loro ruolo, come necessario.

Problemi di creazione report

- Log Server non è in esecuzione, pagina 395
- Nessun Log Server è stato installato per un'istanza di Policy Server, pagina 396
- Il database di registrazione non è stato creato, pagina 397
- Il database di registrazione non è disponibile, pagina 397
- Dimensioni del database di registrazione, pagina 398
- Log Server non registra i dati nel database di registrazione, pagina 399
- ◆ Aggiornamento del collegamento con il Log Server, pagina 399
- Configurazione delle autorizzazioni per l'utente relativamente a Microsoft SQL Server 2005, pagina 400
- Log Server non può stabilire la connessione con il servizio di directory, pagina 401
- I dati dei report sui tempi di navigazione in Internet sono alterati, pagina 401
- La larghezza di banda è superiore al previsto, pagina 401
- Alcune richieste di protocollo non vengono registrate, pagina 402

- Tutti i report sono vuoti, pagina 402
- Nelle pagine Oggi e Cronologia non viene visualizzato alcun grafico, pagina 404
- Impossibile accedere ad alcune funzioni di creazione report, pagina 404
- L'esportazione in Microsoft Excel causa la perdita di alcuni dati del report, pagina 404
- Salvataggio di un'esportazione in HTML dei report di presentazione, pagina 404
- Problemi di ricerca all'interno dei report investigativi, pagina 405
- Problemi generali dei report investigativi, pagina 405

Log Server non è in esecuzione

Se Log Server non è in esecuzione, o se i componenti Websense non sono in grado di comunicare con Log Server, le informazioni sull'uso di Internet non vengono memorizzate e potrebbe non essere possibile generare report sull'utilizzo di Internet.

Log Server potrebbe non essere disponibile se:

- Lo spazio sul disco del computer con installato Log Server non è sufficiente.
- Si è modificata la password per Microsoft SQL Server o MSDE senza aggiornare la configurazione di ODBC o di Log Server.
- Sono passati più di 14 giorni dall'ultimo scaricamento del Master Database.
- Il file logserver.ini risulta mancante o è danneggiato.
- Si è interrotto Log Server per evitare la registrazione delle informazioni sull'uso di Internet.

Per diagnosticare e risolvere questo problema:

- Verificare lo spazio disponibile su disco ed eliminare file superflui, come necessario.
- Se si ritiene che la modifica della password sia all'origine del problema, vedere *Aggiornamento del collegamento con il Log Server*, pagina 399.
- Navigare alla directory bin di Websense (C:\Programmi \Websense\bin o /opt/ Websense/bin, come predefinizione) ed accertarsi che sia possibile aprire logserver.ini in un programma di gestione del testo. Se questo file è stato danneggiato, sostituirlo con un file di backup.
- Aprire la finestra di dialogo Windows Services per verificare che Log Server sia stato avviato e riavviare quindi il servizio, se necessario (vedere *Chiusura e* riavvio dei servizi di Websense, pagina 290).
- Aprire il Visualizzatore eventi di Windows e il file websense.log per verificare la presenza di messaggi di errore relativi al Log Server (vedere *Strumenti di diagnostica e risoluzione problemi*, pagina 406).

Nessun Log Server è stato installato per un'istanza di Policy Server

Il Log Server di Websense raccoglie informazioni sull'uso di Internet e le archivia nel database di registrazione per un uso nei report investigativi, nei report di presentazione nonché nei grafici e riepiloghi delle pagine Oggi e Cronologia di Websense Manager.

Il Log Server deve venire installato affinché sia possibile creare i report.

È possibile vedere questo messaggio se:

- Log Server è installato in un computer diverso da quello in cui è installato Policy Server e l'indirizzo IP di Log Server è stato erroneamente definito su Localhost in Websense Manager.
- Log Server è stato installato in un computer su piattaforma Linux.
- Non si stanno usando gli strumenti di creazione dei report Websense.

Per verificare che il corretto indirizzo IP di Log Server sia definito su Websense Manager:

- 1. Selezionare la scheda **Impostazioni** del riquadro di navigazione di sinistra e andare quindi a **Generale > Accesso**.
- 2. Inserire l'indirizzo IP del computer in cui è installato Log Server nel campo **Indirizzo IP o nome Log Server**.
- 3. Fare clic su **OK** per salvare le modifiche nella cache e fare quindi clic su **Salva** tutto.

Se Log Server è installato in un computer dotato del sistema Linux, oppure se non si stanno utilizzando gli strumenti di creazione report di Websense, è possibile nascondere il messaggio di avvertenza visualizzato in Websense Manager.

- Nella scheda Principale del riquadro di navigazione di sinistra, andare a Stato > Avvisi.
- 2. In Avvisi attivi, fare clic su Avanzati.
- 3. Selezionare **Nascondi questo avviso** per il messaggio "Nessun log server installato".
- 4. Fare clic su Salva ora. La modifica viene implementata immediatamente.
Il database di registrazione non è stato creato

A volte il programma di installazione non è in grado di creare il database di registrazione. L'elenco che segue descrive le cause più comuni di questa condizione e le possibili soluzioni.

Problema:	Un file o dei file esistenti usano dei nomi che il software Websense usa per il database di registrazione (wslogdb70 e wslogdb70_1) ma i file non sono correttamente collegati al motore del database e quindi non possono venire usati dal programma di installazione di Websense.
Soluzione:	Eliminare o assegnare un nuovo nome ai file esistenti e quindi eseguire ancora il programma di installazione.
Problema:	L'account utilizzato per accedere all'installazione non possiede le autorizzazioni necessarie relative all'unità in cui è installato il database.
Soluzione:	Aggiornare l'account di accesso in modo che possieda permessi di lettura e scrittura per il percorso di istallazione oppure accedere a un account diverso che possiede già questi permessi. Eseguire nuovamente il programma di installazione.
Problema:	Non si dispone di uno spazio su disco sufficiente per creare e mantenere il database di registrazione nel percorso specificato.
Soluzione:	Liberare una quantità di spazio sufficiente sul disco selezionato per installare e mantenere il database di registrazione. Eseguire nuovamente il programma di installazione. In alternativa, scegliere un altro percorso.
Problema:	L'account utilizzato per accedere all'installazione non possiede le autorizzazioni SQL Server necessarie per creare un database.
Soluzione:	Aggiornare l'account di accesso o accedere con un account che possiede già le autorizzazioni necessarie. Eseguire nuovamente il programma di installazione.
	Le autorizzazioni necessarie sono in funzione dalla versione di Microsoft SQL Server:
	 SQL Server 2000 o MSDE: sono necessarie autorizzazioni di tipo dbo (titolare del database)
	 SQL Server 2005: sono necessari permessi di tipo dbo e SQLServerAgentReader

Il database di registrazione non è disponibile

Il database di registrazione di Websense raccoglie informazioni sull'uso di Internet da includere nei report di presentazione, nei report investigativi e nei grafici e riepiloghi delle pagine Oggi e Cronologia di Websense Manager.

Se il software Websense non è in grado di collegarsi con il database di registrazione, verificare per prima cosa che il motore del database (Microsoft SQL Server oppure

Microsoft SQL Server Desktop Engine [MSDE]) sia in esecuzione nel computer in cui è installato il database di registrazione.

- 1. Aprire la finestra di dialogo Windows Services (vedere *Finestra di dialogo Servizi di Windows*, pagina 406) per verificare se i servizi seguenti sono in esecuzione.
 - Microsoft SQL Server:
 - MSSQLSERVER
 - SQLSERVERAGENT
 - Microsoft SQL Desktop Engine (MSDE):
 - MSSQL\$WEBSENSE (se si è ottenuto MSDE da Websense, Inc.)
 - SQLAgent\$WEBSENSE
- 2. Se un servizio è stato chiuso, fare clic sul nome del servizio e fare clic su Start.

Se il servizio non viene riavviato, aprire il Visualizzatore eventi di Windows (vedere *Visualizzatore eventi di Windows*, pagina 406) per verificare la presenza di errori e avvertenze relative a Microsoft SQL Server o MSDE.

Se il motore del database è in esecuzione:

- Verificare che SQL Server Agent sia in esecuzione nel computer con installato il motore del database.
- Aprire la finestra di dialogo Windows Services per verificare se il servizio
 Websense Log Server sia in esecuzione.
- Se Log Server e il database di registrazione sono installati in diversi computer, accertarsi che entrambi i computer siano in esecuzione e che la connessione di rete tre i computer non sia in qualche modo difettosa o non sia stata interrotta.
- Accertarsi che esista una spazio sufficiente sul disco del computer con installato il database di registrazione e che sia stata allocata una quantità di spazio sufficiente per il database di registrazione (vedere *Log Server non registra i dati nel database di registrazione*, pagina 399).
- Accertarsi che la password di accesso a Microsoft SQL Server o MSDE non sia stata modificata. Se la password è stata modificata, occorre aggiornare le informazioni usate dal Log Server per il collegamento al database. Vedere Aggiornamento del collegamento con il Log Server, pagina 399.

Dimensioni del database di registrazione

Le dimensioni del database di registrazione sono un elemento determinante da tenere sempre presente. Se si sono generati report Websense e si osserva che la visualizzazione dei report richiede molto più tempo o se si ricevono messaggi di timeout dal browser Web, prendere in considerazione la possibilità di disattivare alcune partizioni del database.

- 1. In Websense Manager, andare a Impostazioni > Creazione report>Database di registrazione).
- 2. Individuare la sezione Partizioni disponibili della pagina.
- 3. Deselezionare la casella di controllo **Abilita** in relazione a qualsiasi partizione non necessaria per le operazioni di creazione dei report corrente.

4. Fare clic su Salva ora per applicare le modifiche.

Log Server non registra i dati nel database di registrazione

Se Log Server non scrive dati nel database di registrazione significa, molto spesso, che il database ha esaurito lo spazio allocato su disco. Questo può accadere se l'unità disco è piena o, nel caso di Microsoft SQL Server, se si sono definite dimensioni massime per il database.

Se l'unità disco che contiene il database di registrazione è piena, occorre aggiungere spazio al disco del computer per ripristinare la funzione di registrazione.

Se l'amministratore del SQL Server Database ha definito delle dimensioni massime di crescita per un singolo database residente in Microsoft SQL Server, procedere come segue:

- Contattare l'amministratore del SQL Server Database per aumentare il limite massimo di spazio.
- Determinare le dimensioni massime stabilite e andare a Impostazioni > Creazione report >Database di registrazione per configurare il rollover del database di registrazione quando raggiunge approssimativamente il 90% dello spazio disponibile. Vedere *Configurazione opzioni di rollover*, pagina 331.

Se il reparto di Tecnologia informatica ha stabilito un limite massimo di spazio su disco per le operazioni di SQL Server, contattare il personale del reparto per ottenere l'assistenza necessaria.

Aggiornamento del collegamento con il Log Server

Se si modifica la password per l'account che il software Websense utilizza per il collegamento con il database di registrazione, si deve aggiornare Log Server in modo che possa utilizzare la nuova password.

- Nel computer con installato Log Server, andare a Start > Programmi > Websense >Utilità > Configurazione di Log Server. Viene visualizzata l'utilità Configurazione di Log Server.
- Fare clic sulla scheda Database e verificare che il database corretto (per impostazione predefinita, wslogdb70) sia visualizzato nel campo ODBC Data Source Name (DSN).
- 3. Fare clic su **Connessione**. Viene aperta la finestra di dialogo Seleziona origine dati.
- 4. Fare clic sulla scheda Machine Data Source [Origine dati computer] e quindi fare doppio clic su **wslogdb70** (o sul nome del database di registrazione). Viene aperta la finestra di dialogo Accesso a Microsoft SQL Server.
- 5. Accertarsi che il campo LoginID contenga il nome di account corretto (normalmente **sa**) ed inserire quindi la nuova password.
- 6. Fare clic su **OK** e quindi, nella finestra di dialogo Configurazione di Log Server, fare clic su **Applica**.

- 7. Fare clic sulla scheda Connessione e quindi chiudere e riavviare Log Server.
- 8. Quando Log Server è di nuovo in esecuzione, fare clic su **OK** per chiudere l'utilità.

Configurazione delle autorizzazioni per l'utente relativamente a Microsoft SQL Server 2005

Microsoft SQL Server 2005 definisce i ruoli di SQL Server Agent che regolano l'accessibilità alla struttura del processo. I processi di SQL Server Agent per SQL Server 2005 sono memorizzati nel database SQL Server msdb.

Per installare Websense Log Server, l'account utente che possiede il database Websense deve appartenere ad uno dei seguenti ruoli del MSDB Database:

- SQLAgentUserRole
- SQLAgentReader Role
- SQLAgentOperator Role



- Nel computer con installato Log Server, andare a Start > Programmi > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio.
- 2. Selezionare il diagramma ad albero Explorer oggetto.
- 3. Selezionare Sicurezza > Accessi.
- 4. Selezionare l'account di accesso da utilizzare durante l'installazione.
- 5. Fare clic con il pulsante destro del mouse sull'account di accesso e selezionare **Proprietà** per questo utente.
- 6. Selezionare Mapping utente e procedere come segue:
 - a. Selezionare msdb nel mapping del database.
 - b. Assegnare l'appartenenza a uno di questi ruoli:
 - Ruolo SQLAgentUserRole
 - Ruolo SQLAgentReader
 - Ruolo SQLAgentOperator
 - c. Fare clic su OK per salvare.
- 7. Selezionare **Ruoli del server** e selezionare quindi **dbcreator**. È stato così creato il ruolo dbcreator.
- 8. Fare clic su **OK** per salvare.

Log Server non può stabilire la connessione con il servizio di directory

Se si verifica uno degli errori elencati di seguito, Log Server non sarà in grado di accedere al servizio di directory necessario per aggiornare i mapping di utente-gruppo per i report. Questi errori sono inclusi nel Visualizzatore eventi di Windows (vedere *Visualizzatore eventi di Windows*, pagina 406).

- EVENT ID:4096 Impossibile inizializzare Directory Service. Websense Server potrebbe essere inattivo o non raggiungibile.
- EVENT ID:4096 Impossibile collegarsi al servizio di directory. I gruppi per questo utente non verranno risolti in questa fase del processo. Verificare che questo processo possa accedere al servizio di directory.

La causa più frequente è che il Websense Log Server e Websense User Service sono ai due lati diversi del firewall che limita l'accesso.

Per risolvere questo problema, configurare il firewall per consentire l'accesso attraverso le porte usate per la comunicazione tra questi componenti.

I dati dei report sui tempi di navigazione in Internet sono alterati

Tenere presente che il consolidamento potrebbe alterare i dati inclusi nei report sui tempi di navigazione in Internet. Questi report mostrano il tempo che gli utenti passano in Internet e possono includere dettagli sul tempo passato in ogni sito. I tempi di navigazione in Internet vengono calcolati usando un logaritmo speciale e l'attivazione del consolidamento potrebbe alterare la precisione dei calcoli effettuati per i report.

La larghezza di banda è superiore al previsto

Molte, ma non tutte le integrazioni di Websense forniscono informazioni sulla larghezza di banda. Se l'integrazione non fornisce informazioni sulla larghezza di banda, è possibile configurare Network Agent in modo che possa eseguire la registrazione includendo i dati della larghezza di banda.

Se un utente richiede lo scaricamento consentito di un file, il prodotto di integrazione o Network Agent inviano le dimensioni complete del file che il software Websense registra come byte ricevuti.

Se l'utente in seguito annulla l'effettivo download, o se il file non viene scaricato completamente, il valore dei byte ricevuti nel database di registrazione rappresenta le dimensioni complete del file. In questo caso, i byte registrati come ricevuti saranno superiori al numero effettivo di byte ricevuti.

Questo incide anche sui valori di larghezza di banda riportati, in quanto rappresenta una combinazione di byte ricevuti e di byte inviati.

Alcune richieste di protocollo non vengono registrate

Alcuni protocolli, come ad esempio quelli usati da ICQ e AOL, richiedono agli utenti di accedere a un server usando un determinato indirizzo IP e quindi inviano un indirizzo IP e un numero di porta di identificazione diversi al client ai fini della messaggistica. In questo caso, tutti i messaggi inviati e ricevuti non potranno venire monitorati e registrati da Websense Network Agent in quanto il server dei messaggi non viene riconosciuto al momento dello scambio dei messaggi.

Ne risulta che il numero di richieste registrate potrebbe non corrispondere al numero di richieste effettivamente inviate. Questo incide sull'accuratezza dei report prodotti dagli strumenti di creazione report di Websense.

Tutti i report sono vuoti

Se i report non contengono dati, verificare che:

- le partizioni attive del database includano le informazioni necessarie per i dati da includere nei report. Vedere *Partizioni del database*, pagina 402.
- il processo di SQL Server Agent sia attivo in Microsoft SQL Server o MSDE Vedere Processo di SQL Server Agent, pagina 402.
- Log Server sia stato configurato correttamente in modo da ricevere le informazioni di registrazione da Filtering Service. Vedere *Configurazione di Log Server*, pagina 403.

Partizioni del database

I record di registro di Websense sono archiviati nelle partizioni all'interno del database. È possibile creare nuove partizioni in base alle dimensioni o alla data, a seconda del motore e della configurazione del database.

È possibile attivare o disattivare le singole partizioni in Websense Manager. Se si cerca di generare un report in base alle informazioni archiviate nelle partizioni disattivate, non verrà reperita alcuna informazione e il report sarà vuoto.

Per accertare che le partizioni appropriate del database siano attive:

- 1. Andare a Impostazioni > Creazione report > Database di registrazione.
- 2. Scorrere verso il basso fino alla sessione Partizioni disponibili.
- 3. Selezionare la casella di controllo **Abilita** per ciascuna partizione che contiene i dati da includere nei report.
- 4. Fare clic su Salva ora per applicare le modifiche.

Processo di SQL Server Agent

È possibile che il processo del SQL Server Agent database sia stato disattivato. Il processo deve essere in esecuzione affinché i record di registro possano venire elaborati nel database dal processo ETL.

Se MSDE è in esecuzione:

- 1. Andare a Start > Strumenti di amministrazione > Servizi.
- Verificare che i servizi di SQL Server e SQL Server Agent siano stati avviati. Se si è ottenuto MSDE da Websense, Inc., questi servizi prendono il nome di MSSQL\$WEBSENSE e SQLAgent\$WEBSENSE.

Se Microsoft SQL Server è in esecuzione completa, chiedere all'amministratore del database di verificare che il processo di SQL Server Agent sia in esecuzione.

Configurazione di Log Server

Le impostazioni di configurazione devono essere corrette sia in Websense Manager e in Log Server per essere certi che Log Service riceva le informazioni di registrazione da Filtering Service. In caso contrario, i dati di registrazione non verranno mai elaborati nel database di registrazione.

Prima di tutto, verificare che Websense Manager sia collegato con Log Server.

- 1. Collegarsi con Websense Manager tramite i permessi di utente con qualifica totale di Super Administrator.
- 2. Andare a **Impostazioni > Generale > Registrazione**.
- 3. Inserire il nome o l'indirizzo IP del computer in cui è installato Log Server.
- 4. Inserire il numero della **porta** dalla quale il Log Server sta ascoltando (l'impostazione predefinita è 55805).
- 5. Fare clic su **Verifica stato** per determinare se Websense Manager sia in grado di comunicare con il Log Server specificato.

Un messaggio indica se la prova di collegamento è stata superata. Aggiornare l'indirizzo IP o il nome del computer e la porta, se necessario, fino a quando la prova non viene superata.

6. Al termine della procedura, fare clic su **OK** per inserire le modifiche nella cache. Le modifiche non vengono implementate fino a quando non si fa clic su **Salva tutto**.

Verificare ora le impostazioni definite per l'utilità Configurazione di Log Server.

- Nel computer con installato Log Server, andare a Start > Programmi > Websense >Utilità > Configurazione di Log Server.
- 2. Nella scheda **Connessioni**, verificare che il numero della porta corrisponda al valore immesso in Websense Manager.
- 3. Fare clic su **OK** per salvare eventuali modifiche.
- 4. Usare il pulsante della scheda **Connessioni** per interrompere e quindi riavviare Log Server.
- 5. Fare clic su Esci per chiudere l'utilità Configurazione di Log Server.

Nelle pagine Oggi e Cronologia non viene visualizzato alcun grafico

Nelle organizzazioni che usano un'amministrazione con delega,verificare le autorizzazioni assegnate al ruolo di amministratore con delega. Se l'opzione **Visualizza report nelle pagine Oggi e Cronologia** non è selezionata, questo grafico non viene visualizzato per gli amministratori con delega in quel ruolo.

Negli ambienti che usano molteplici Policy Server, Log Server viene installato per comunicare con un solo Policy Server. Occorre accedere a quel Policy Server per visualizzare i grafici delle pagine Oggi e Cronologia oppure per accedere ad altre funzioni di creazione report.

Impossibile accedere ad alcune funzioni di creazione report

Se il browser Web ha un'impostazione di blocco dei pop-up, potrebbe bloccare anche determinate funzioni di creazione report. Per usare queste funzioni, occorre ridurre il livello di blocco o disattivare completamente il blocco dei pop-up.

L'esportazione in Microsoft Excel causa la perdita di alcuni dati del report

Il numero massimo di righe che possono venire aperte in un foglio elettronico di Microsoft Excel è 65.536. Se si esporta in Microsoft Excel un report che contiene oltre 65.536 record, i record a partire dal 65.537esimo non verranno inseriti nel foglio di Excel.

Per assicurare l'accesso a tutte le informazioni del report esportato, eseguire una delle operazioni seguenti:

- Nel caso di report di presentazione, modificare il filtro del report al fine di
 ottenere un report di dimensioni inferiori, impostando ad esempio un
 intervallo di date più breve, selezionando meno utenti e gruppi o selezionando
 un numero inferiore di azioni.
- Nel caso di report investigativi, eseguire un drill-down dei dati al fine di ottenere un report più corto.
- Selezionare un altro formato di esportazione.

Salvataggio di un'esportazione in HTML dei report di presentazione

Se si genera un report direttamente dalla pagina Creazione report > Report di presentazione, è possibile scegliere tra 3 formati di visualizzazione: HTML, PDF e XLS. Se si sceglie il formato HTML, il report viene visualizzato nella finestra di Websense Manager.

Si consiglia di non eseguire la stampa e il salvataggio dei report di presentazione direttamente dal browser. In questo caso infatti, l'output di stampa includerà l'intera finestra del browser e l'apertura successiva di un file salvato lancerà Websense Manager.

Per stampare o salvare dei report in modo più efficace, scegliere un formato di output in PDF o XLS. È possibile aprire questi file immediatamente se il software di visualizzazione (Adobe Reader o Microsoft Excel) è installato nel computer locale. È anche possibile salvare il file su disco (l'unica opzione se il software necessario per la visualizzazione non è disponibile).

Dopo aver aperto un report in Adobe Reader o Microsoft Excel, usare le opzioni di stampa e di salvataggio necessarie per la produzione dell'output finale desiderato.

Problemi di ricerca all'interno dei report investigativi

Esistono due potenziali problemi associati ad una ricerca condotta nei report investigativi.

- Non è possibile inserire i caratteri ASCII estesi
- Potrebbe non essere possibile trovare uno schema di ricerca.

Caratteri ASCII estesi

I campi della funzione Cerca, disponibili sopra il grafico a barre della pagina principale dei report investigativi consente di cercare una determinata parola o una stringa di testo nell'elemento grafico selezionato.

Se si usa Mozilla Firefox in un server su piattaforma Linux per accedere a Websense Manager, non si possono inserire in questi campi i caratteri ASCII estesi . Questa è una limitazione conosciuta di Firefox o Linux.

Se occorre cercare un report investigativo per una stringa di testo che include dei caratteri ASCII estesi, accedere a Websense Manager da un server su piattaforma Windows, usando qualsiasi browser supportato.

Non si è trovato un criterio ricerca

I report investigativi non sono in grado di trovare un URL associato a un criterio inserito nei campi di ricerca della pagina principale dei report investigativi. In questo caso e se si è ragionevolmente sicuri che il criterio esista all'interno degli URL riportati, provare ad inserire un criterio diverso in grado di trovare l'URL di interesse.

Problemi generali dei report investigativi

- Alcune query richiedono tempi di esecuzione molto lunghi. Potrebbe venire visualizzata una schermata vuota o un messaggio che segnala che la query è entrata in time out. Questo potrebbe accadere per le ragioni seguenti:
 - Il server Web è entrato in time-out
 - MSDE o Microsoft SQL Server sono entrati in time-out.

Il proxy o la cache sono entrati in time-out

Potrebbe essere necessario aumentare manualmente il limite di time-out definito per questi componenti.

- Se gli utenti non fanno parte di un gruppo, non verranno visualizzati in un dominio. La scelta di Gruppo o Dominio apparirà inattiva.
- Anche se il Log Server sta registrando visite anziché accessi, i report investigativi interpretano queste informazioni come Accessi.

Strumenti di diagnostica e risoluzione problemi

- Finestra di dialogo Servizi di Windows, pagina 406
- Visualizzatore eventi di Windows, pagina 406
- File di registro di Websense, pagina 407

Finestra di dialogo Servizi di Windows

Nei computer dotati del sistema operativo Microsoft Windows, Filtering Service, Network Agent, Policy Server, User Service e tutti gli agenti di identificazione trasparente di Websense vengono eseguiti come servizi. È possibile usare la finestra di dialogo Servizi di Windows per verificare lo stato di questi servizi.

- 1. Nel Pannello di controllo di Windows, aprire la cartella **Strumenti di amministrazione**.
- 2. Fare clic su Servizi.
- 3. Scorrere lungo l'elenco dei servizi per trovare il servizio di cui si sta eseguendo una diagnostica/risoluzione problemi.

La voce del servizio include il nome del servizio, una breve descrizione, lo stato del servizio (avviato o interrotto), il metodo di avvio del servizio e l'account usato dal servizio per eseguire le sue attività.

4. Fare doppio clic sul nome di un servizio per aprire una finestra di dialogo delle proprietà con informazioni più dettagliate sul servizio.

Visualizzatore eventi di Windows

Il Visualizzatore Eventi di Windows registra i messaggi di errore sugli eventi Windows, incluso le attività svolte dal servizio. Questi messaggi possono aiutare ad identificare gli errori di rete o del servizio che potrebbero causare problemi di filtraggio degli accessi a Internet o problemi di identificazione dell'utente.

- 1. Nel Pannello di controllo di Windows, aprire la cartella **Strumenti di amministrazione**.
- 2. Fare doppio clic su Visualizzatore eventi.
- 3. In Visualizzatore eventi, fare clic su **Applicazione** per un elenco di messaggi di errore e di messaggi informativi.

4. Scorrere lungo l'elenco per identificare errori o avvertenze originati dai servizi di Websense.

File di registro di Websense

Il software Websense scrive messaggi di errore nel file **websense.log**, situato nella directory Websense **bin** (C:\Programmi\Websense\bin oppure in /opt/Websense/bin, come impostazione predefinita).

Le informazioni contenute in questo file sono comparabili a quelle trovate nel Visualizzatore eventi di Windows. In ambiente Windows, il Visualizzatore eventi di Windows presenta i messaggi in un formato più intuitivo. Il file **websense.log** tuttavia è disponibile nei sistemi Linux e può essere inviato a Websense Technical Support se si ha bisogno di risolvere un problema di diagnostica/risoluzione problemi.

INDICE ANALITICO

A

accedi con password in un ambiente con molteplici Policy Server, 284 accessi definiti, 322 registrazione, 310 accesso, 18 accesso a Websense Manager, 17, 250 account di rete definizione directory di accesso, 255 account utenti, 241, 242 aggiunta a Websense, 258 password, 246 Websense, 246, 257 WebsenseAdministrator, 243 account utenti Websense, 246, 257 aggiunta, 258 gestione, 260 password, 246 WebsenseAdministrator, 18 Active Directory Native Mode, 65 Active Directory di Windows (modalità nativa), 65 aggiorna database di registrazione, impostazioni, 331 aggiornamenti del database, 33 in tempo reale, 33, 299 Real-Time Security, 33, 299 scansione in tempo reale, 150 aggiornamenti del database in tempo reale, 33, 299 aggiornamento utenti mancanti, 362 aggiornamento scansione in tempo reale del database, 150 Aggiungi criteri, 78 filtro categoria, 49

filtro per restrizioni di accesso, 174 filtro protocollo, 52 gruppi LDAP personalizzati, 69 parole chiave, 185 aggiunta ai protocolli definiti da Websense, 195 client, 70 criteri, 78 Esegui sempre la scansione o Non eseguire mai la scansione, voci dell'elenco, 156 filtri categoria, 49 filtri per restrizioni di accesso, 174 filtri protocollo, 52 tipi di file, 199 amministratori, 242 accesso a Websense Manager, 255 accesso simultaneo allo stesso ruolo, 270 account utenti Websense, 257 aggiunta al ruolo, 261, 265 autorizzazione creazione rapporti, 244, 263 autorizzazione parziale gestione criteri, 244 autorizzazione totale di gestione criteri, 244 autorizzazioni, 243 autorizzazioni, impostazioni, 261, 266 blocco filtro, effetto, 271 con delega, 245 creazione di rapporti, 252 creazione rapporti, 243, 271 eliminazione dal ruolo, 261 in molteplici ruoli, 246, 265, 270 notifica responsabilità, 250 operazioni degli amministratori con delega, 251 operazioni per il Super Administrator, 247 panoramica, 243 rilevamento modifiche apportate, 289 Super Administrator, 243 visualizzazione definizione del ruolo, 252 amministratori con delega, 245 amministrazione con delega

accesso a creazione rapporti, 311 accesso a Websense Manager, 255 aggiunta di amministratori, 265 aggiunta ruoli, 259, 260 applicazione criteri, 249 autorizzazione creazione rapporti, 244 autorizzazioni di gestione criteri, 243 Blocco filtro, 271 conflitti di ruolo, 268 eliminazione dei client dai ruoli, 269 eliminazione ruoli, 259 eliminazione ruoli, effetto, 269 impostazione, 247 introduzione, 247 modifica ruoli, 261 notifica agli amministratori, 250 panoramica, 241 uso, 259 applet tempo assegnato, 47 Applica ai client, 79 Applica criterio ai client, 82 applicazioni, scansione, 154 approfondimento, rapporti investigativi, 122 Assegna, 45 assegnazione nuovo nome filtri categoria, 50 assistenza tecnica, 36 atipici, rapporto, 120, 145 attività utente, 147, 267 configurazione, 346 notificazione utenti, 347 attività utente, consenti attivazione, 314 autenticazione Log Server, 326, 327 selettiva, 210 autenticazione manuale, 207, 210 attivazione, 209 Autorizza tutti i filtri, 55 Autorizzazione, 45 autorizzazione parziale gestione criteri, 244 autorizzazioni, 242 creazione di rapporti, 246

creazione rapporti, 244 criteri, 243, 245 criteri parziali, 244 criteri totali, 244 impostazione, 263 impostazioni, 261, 266 molteplici ruoli, 246 rapporti, 255 rilascio criterio, 250 SQL Server, 397 unità di installazione, 397 autorizzazioni d'uso, 28 autorizzazioni di gestione criteri, 243, 245 parziale, 244 qualifica totale, 244 rilascio, 250 avvertenze Riepilogo avviso di integrità, 22 avvio Log Server, 317, 318, 327 servizi di Websense, 290 avvisi, 299 aggiornamenti del database in tempo reale, 299 e-mail, 294 limiti di configurazione, 293 metodi di configurazione, 293 metodo di invio, 292 pop-up, 294 prevenzione numero eccessivo, 293 Real-Time Security Updates, 299 sistema, 292 sistema, configurazione, 295 SNMP, 294 uso protocollo, aggiunta, 298 utilizzo categoria, 292 utilizzo categoria, aggiunta, 297 utilizzo categoria, configurazione, 296 utilizzo protocollo, 292 utilizzo protocollo, configurazione, 297 Websense, integrità, 299 avvisi di integrità, 299 descrizione, 390 riepilogo, 22 soluzioni, 390

avvisi di sistema, 292 configurazione, 295 avvisi di utilizzo, 292 categoria, aggiunta, 297 categoria, configurazione, 296 categorie di registrazione, 314 protocollo, aggiunta, 298 protocollo, configurazione, 297 avvisi di utilizzo categoria aggiunta, 297 avvisi di utilizzo categorie e registrazione, 314 avvisi di utilizzo di una categoria configurazione, 296 eliminazione, 296 avvisi di utilizzo protocolli aggiunta, 298 avvisi di utilizzo protocollo configurazione, 297 avvisi mediante e-mail, 294 avvisi pop-up, 294 Avvisi SNMP, 294 azioni, 44 Assegna, 45 Autorizzazione, 45 Blocca per parole chiave, 46 Blocca per tipi di file, 46 Blocco, 45 Conferma, 45 selezione rapporti di presentazione, 107

B

backup dei dati di Websense, 300 batch errati, 337 BCP, 318, 319 Blocca Parole chiave, 46 Tipi di file, 46 Blocca tutti i filtri, 55 Blocco, 45 blocco, 272 categorie, 272 in base a parole chiave, 185 parole chiave, 273

protocolli, 189, 274 tipi di file, 197, 273 blocco dei pop-up accesso a creazione rapporti, 404 Blocco filtro blocco dei protocolli, 274 blocco delle categorie, 272 blocco parole chiave, 273 blocco tipi di file, 273 configurazione, 248 creazione, 244, 272 effetto sui ruoli, 245, 254, 271 registrazione protocolli, 274 blocco, parole chiave diagnostica e risoluzione problemi, 371 BrandWatcher, 30 Bulk Copy Program (BCP), 318

C

caratteri ASCII estesi nel nome del computer con DC Agent, 219 nel nome del computer con eDirectory Agent, 231 nel nome del computer con Logon Agent, 222 nel nome del computer con RADIUS Agent, 226 ricerca nei rapporti investigativi, 405 Carico del filtro attuale, 23 Casella degli strumenti, 201 catalogo database, 328 rapporti, 100 catalogo globale, 65 catalogo rapporti, 100 nome, 108 categorie aggiunta personalizzazioni, 182 aggiunte al Master Database, 39 blocco per tutti i ruoli, 272 definite, 32, 38 elenco completo, 38 Eventi speciali, 40 Larghezza di banda, 40 modifica personalizzazione, 180 personalizzazione, 179

Produttività, 40 Protezione estesa, 41 registrazione, 314 selezione rapporti di presentazione, 106 sicurezza, 40 uso larghezza di banda, 195 categorie personalizzate, 179 aggiunta, 182 creazione, 178 modifica, 180 nuovo nome, 182 categorizzazione contenuto, 152 chiave, 28 chiave di sottoscrizione, 28 inserimento, 31 non valida o scaduta, 361 verifica, 364 chiusura contro errori, 166 Remote Filtering, 168 timeout, 166, 168 chiusura contro errori, timeout, 166 classi di rischio, 41, 312 assegnazione categorie, 313 nella creazione dei rapporti, 312 Perdita di larghezza di banda, 42 Perdita di produttività, 42, 43 Perdita larghezza di banda, 42 responsabilità legale, 42 Rischio sicurezza, 42 selezione di rapporti investigativi, 130 selezione rapporti di presentazione, 106 Utilizzo aziendale, 42 client, 61 aggiunta, 70 amministrazione, 62 applicazione criteri, 61 assegnazione criteri, 79, 82 computer, 61, 63 gruppi, 64 modifica, 72 rete, 61, 63 selezione rapporti di presentazione, 105 spostamento a un ruolo diverso, 72

utenti, 61, 64 client gestiti, 242 aggiunta ai ruoli, 249 assegnazione al ruolo, 262, 266 eliminazione dal ruolo, 262, 269 spostamento a un altro ruolo, 248 client, gestiti, 242 aggiunta ai ruoli, 249 applicazione criteri, 254 assegnazione ai ruoli, 252, 262, 266 eliminazione dal ruolo, 251, 269 in molteplici ruoli, 253, 266 ruoli sovrapposti, 268 spostamento a un altro ruolo, 248 coda processi rapporti di presentazione, 103 rapporti investigativi, 120, 144 colonne per i rapporti investigativi dettagliati, 130 come contattare l'assistenza al cliente, 29 come ottenere assistenza tecnica, 36 come trovare informazioni sul prodotto, 29 componenti, 161, 276 database di registrazione, 280 DC Agent, 281 eDirectory Agent, 282 Filtering Service, 277 Log Server, 280 Logon Agent, 281 Master Database, 278 Network Agent, 277 Policy Broker, 277 Policy Database, 277 Policy Server, 277 RADIUS Agent, 282 Remote Filtering Client, 162, 278 Remote Filtering Server, 278 Usage Monitor, 278 User Service, 281 Websense Content Gateway, 279 Websense Manager, 278 Websense Security Gateway, 279 componenti filtro, 178 computer

client, 61 comunicazione, 166 Conferma, 45 in un ambiente con molteplici Policy Server, 284 configurazione criteri ripristino predefinizioni, 56 configurazione di rete, 350 Configurazione NIC, 351 impostazioni, 355 monitoraggio, 355 configurazione, utilità accesso, 316 connessione di tipo trusted, 320 consolidamento registrazione URL completo, 334 registrazione, record, 310, 323 tempo di navigazione in Internet, 401 Content Gateway, 279 contenuto categorizzazione, 152 scansione, 149, 153 contenuto ActiveX eliminazione, 155 contenuto attivo eliminazione, 155 contenuto dinamico categorizzazione, 152 Continua, pulsante, 45 controller di dominio prove di visibilità, 380 copia filtri categoria, 49 filtri per accesso limitato, 49 filtri protocollo, 49 rapporti di presentazione, 103 Copia nel ruolo, 177 criteri, 77 filtri, 49 creazione criteri, 78 filtri categorie, 80 filtri per restrizioni di accesso, 80 filtri protocolli, 80 creazione dei rapporti

limitazioni dell'amministratore, 246 creazione di rapporti autorizzazioni, 246 creazione rapporti accesso, 310 amministratore, 271 attività utente, 267 autorizzazioni, 244, 263 autorizzazioni, impostazioni, 263 blocco dei pop-up, 404 componenti, 309 configurazione attività utente, 346 configurazione server e-mail, 314 Linux, 97, 311 opzioni in tempo reale, 158 preferenze, 314 strategia, 310 timeout, 398 credenziali di rete accesso a Websense Manager, 255 criteri aggiunta, 77, 78 applicazione, 82 applicazione a utenti e gruppi, 64 applicazione ai client, 79, 82 applicazione ai client gestiti, 249, 254 copia nei ruoli, 77, 248, 249 copia nel ruolo, 177 creazione per il ruolo, 254 definiti, 37, 75 descrizioni, 78 determinazione applicazione, 82 Esempio – Utente standard, 75 Illimitato, 75 modifica, 77, 79 modifica per il ruolo, 253 molteplici gruppi, 82 nuovo nome, 79 Predefinito, 76 priorità di filtraggio, 83 stampa su file, 77 visualizzazione, 77 criteri per molteplici gruppi, 82 criterio di ricerca

rapporti investigativi, 405 criterio illimitato, 75 Criterio predefinito, 76 applicato erroneamente, 379 Cronologia, pagina, 25 grafici, 26 personalizzazione, 26, 27

D

database aggiornamenti del database in tempo reale, 33 catalogo, 328 database di registrazione, 328 manutenzione, processo, 336 Master Database, 32 partizioni database di registrazione, 328 per una scansione in tempo reale, 150 Policy Database, 282 processi database di registrazione, 329 Real-Time Security Updates[™], 33 database di registrazione, 280, 309, 310, 312 amministrazione, 312, 330 attivo, 331 collegamento per i rapporti investigativi, 342 configurazione manutenzione, 336 connessione di tipo trusted, 320 connessioni a LogServer, 319 consolidamento, 323 creazione partizioni, 338 database del catalogo, 328 dimensioni, 398 eliminazione errori, 337 IBT, processo, 99, 329 impostazioni, 331 introduzione, 328 non creato, 397 non disponibile, 397 partizioni database, 328 processi, 329 processo di manutenzione, 329, 336 reindicizzazione, 336 requisiti di spazio su disco, 310 selezione di partizioni per i rapporti, 339 spazio su disco esaurito, 399

Visualizzazione del registro di errori, 341 database iniziale, 32 database, download problemi con le applicazioni limitative, 368 requisiti della memoria, 367 requisiti di spazio su disco, 366 scansione in tempo reale, 150 verifica accesso a Internet, 365 DC Agent, 217, 281 configurazione, 218 diagnostica e risoluzione problemi, 377 definizione criteri pianificazione tempi, 79 dettagli, visualizzazione colonne, 130 configurazione impostazioni predefinite, 343 modifica, 128 Dettaglio attività utente giorno/mese, 120 Dettaglio attività utente giorno/mese, rapporto, 132 Dettaglio giornaliero attività utente, rapporto, 133 mappa categorie, 135 Dettaglio mensile attività utente, rapporto, 134 diagnostica eDirectory Agent, 382 dimensioni massime per scansione di file, 154 Directory di accesso definizione, 255 DMZ, 163, 164 download del database, 32 aggiornamenti in tempo reale, 33 configurazione, 34 diagnostica e risoluzione problemi, 364 problemi di sottoscrizione, 364 Real-Time Security Updates[™], 33 ripresa, 288 stato, 288 via proxy, 35

E

eDirectory, 67 eDirectory Agent, 229, 282 configurazione, 231 diagnostica, 382

diagnostica e risoluzione problemi, 382 modalità console, 384 eDirectory, repliche server configurazione, 232 elenco di processi pianificati rapporti di presentazione, 103 rapporti investigativi, 144 eliminazione contenuto attivo, 155 Esegui sempre la scansione o Non eseguire mai la scansione, voci dell'elenco, 157 istanze di Policy Server in Websense Manager, 283 VB Script, contenuto, 155 eliminazione client gestiti, 393 eliminazione di un contenuto, 155 eliminazione di un contenuto attivo, 155 eliminazione voci dagli elenchi Esegui sempre la scansione or Non eseguire mai la scansione, 158 e-mail distribuzione rapporti, 314 errore di accesso., 393 esecuzione di Websense Manager, 17 Esegui sempre la scansione, elenco aggiunta di siti, 156 eliminazione voci, 157 esempi criteri, 75 filtro di categoria e di protocollo, 55 esempio criteri, 75 filtro di categoria e di protocollo, 55 Esempio – Utente standard, criterio, 75 esercitazioni Esercitazioni di riferimento rapido, 18 Esercitazioni di riferimento rapido, 18 lancio, 18 espressioni regolari, 178, 200 e URL non filtrato, 187 filtro per restrizioni di accesso, 175 ricategorizzazione degli URL, 180 estensioni dei file scansione in tempo reale, 154 estensioni di file aggiunta ai tipi di file, 200

filtro in base a, 197 estensioni file aggiunta ai tipi di file predefiniti, 199 in tipi di file predefiniti, 198 esternamente alla rete, 164 estrazione, trasformazione e caricamento (ETL), processo, 329 Eventi speciali, 40 Excel, formato rapporti incompleti, 404 registro di controllo, 289 Explorer per Linux, 97, 311

F

fail open - autorizzazione, 166 file cache registrazione, 321 file cache di registro, 321 file registro, 165, 407 Remote Filtering, 169 file, scansione, 154 Filtering Service, 277 aggiornamento UID, 375 descrizione, 287 download del database, 288 modifica indirizzo IP, 375 pagina dettagli, 287 Riepilogo, grafico, 24 filtraggio diagramma, 83 ordine, 82 priorità, 83 priorità, URL personalizzato, 186 filtri, 48 accesso limitato, 48 Autorizza sempre, 249 azioni, 44 categoria, 37, 48 copia nei ruoli, 248, 249 copia nel ruolo, 177 creazione per il ruolo, 254 determinazione dell'uso, 80 modifica, 81 modifica per il ruolo, 253

protocollo, 37, 48 rapporti di presentazione, 100, 102 restrizioni di accesso, 172 ripristino predefinizioni, 56 filtri Autorizza sempre e priorità di filtraggio, 83 filtri categoria creazione, 49 definiti, 37 duplica, 49 modelli, 49, 55 modifica, 50 nuovo nome, 50 filtri categorie, 48 aggiunta, 80 filtri per accesso limitato, 48 filtri per restrizioni di accesso, 172 aggiunta, 80 creazione, 174 espressioni regolari, 175 nuovo nome, 175 priorità di filtraggio, 172 filtri protocolli, 48 aggiunta, 80 filtri protocollo creazione, 52 definiti, 37 modelli, 52, 56 modifica, 53 nuovo nome, 53 filtro casella strumenti, 201 con parole chiave, 184 protocolli, 189 tipi di file, 197 filtro Autorizza sempre e ruoli amministrativi, 249 filtro Blocca sempre e priorità di filtraggio, 83 filtro di rapporto, rapporti di presentazione, 102, 104 conferma, 110 selezione azioni, 107 selezione categorie, 106

selezione classi di rischio, 106 selezione client, 105 selezione protocolli, 107 filtro in base a reputazione, 41 filtro per rapporti, rapporti di presentazione, 100 formato Excel rapporti di presentazione, 101, 112, 117 rapporti investigativi, 121, 143 formato HTML rapporti di presentazione, 101 formato HTML, rapporti di presentazione, 112 formato PDF rapporti di presentazione, 101, 112, 117 rapporti investigativi, 121, 143 formato XLS rapporti di presentazione, 101, 112 rapporti investigativi, 121, 146

G

gestione categorie, 178 grafici Carico del filtro attuale, 23 Cronologia, pagina, 26 pagina Oggi, 23 Riepilogo Filtering Service, 24 Risultati del giorno, 22 scelta per la pagina Oggi, 24 grafico a barre, 124 grafico a torta, 124 gruppi, 64 gruppi di protocolli per la sicurezza, 44 gruppi LDAP personalizzati, 68 aggiunta, 69 gestione, 260 modifica, 69

H

heartbeat, 163, 164 heartbeat, 163, 164 HTML, formato salvataggio rapporti di presentazione, 404 HTTP Post, 325

Ι

IBT - Internet browse time

configurazione, 334 identificatori protocollo, 191 identificatori protocolli, 191 indirizzi IP, 191 porte, 191 identificazione utente diagnostica e risoluzione problemi, 376 manuale, 207 trasparente, 205 utenti remoti, 206 identificazione utente trasparente, 205 agenti, 205 configurazione, 208 DC Agent, 217 eDirectory Agent, 229 Logon Agent, 221 identificazione utenti trasparente RADIUS Agent, 224 impostazioni Account, 31 Avvisi e notifiche, 293 database di registrazione, 331 Directory di accesso, 255 download del database, 34 Filtri, 57 Identificazione utente, 208 Network Agent, 352 Policy Server, 283 Remote Filtering, 168 servizi di directory, 65 Sicurezza in tempo reale, 151 impostazioni del firewall database, download, 365 impostazioni di filtraggio configurazione, 57 impostazioni directory avanzate, 67 impostazioni proxy database, download, 365 verifica, 366 Impostazioni, scheda., 20 Informazioni di configurazione di Websense, 282 informazioni sull'account configurazione, 31

informazioni utente, registrazione, 314 internamente alla rete, 163 interruzione Log Server, 317, 318, 327 servizi di Websense, 290 intervallo date processo pianificato dei rapporti investigativi, 143 processo pianificato per rapporti di presentazione, 116

J

Java System Directory di Sun, 67 JavaScript, contenuto eliminazione, 155

L

lancio di Websense Manager, 17 larghezza di banda gestione, 195 impostazioni restrizioni, 197 più larga del previsto, 401 registrato per le richieste bloccate, 123 usata da categorie, 195 usata dai protocolli, 195 larghezza di banda registrata, richieste bloccate, 132 Larghezza di banda, categoria, 40 larghezza di banda, filtro, 161 LDAP gruppi personalizzati, 68 set di caratteri, 68 lettere in rosso, rapporti investigativi, 123 Linux, creazione rapporti, 97, 311 Log Server, 280, 309 aggiornamento informazioni utente/gruppo, 317 autenticazione, 326, 327 avvio, 317, 318, 327 configurazione, 403 configurazione, utilità, 316 connessione al database di registrazione, 320 connessione al servizio di directory, 401 interruzione, 317, 318, 327 non installato, 396 uso del server proxy, 327

Utilità di configurazione, 311, 312 logo modifica della pagina di blocco, 91 rapporti di presentazione, 104 logo personalizzato pagine di blocco, 91 rapporti di presentazione, 104, 109 logo, rapporti di presentazione, 109 Logon Agent, 221, 281 configurazione, 222 diagnostica e risoluzione problemi, 379

Μ

manutenzione, processo database di registrazione, 336 mappa categorie rapporto dettagliato attività utente, 135 Master Database, 32, 278 aggiornamenti in tempo reale, 33 categorie, 38 donwnload, 32 download, problemi, 364 miglioramento, 325 protocolli, 39 Real-Time Security Updates[™], 33 ripresa del download, 288 stato download, 288 tempi stabiliti per il download, 34 messaggi di blocco creare personalizzazione, 90 creazione messaggi alternativi, 94 modifica dimensioni del frame, 91 per tipi di file, 198 personalizzazione, 89 protocollo, 88 messaggi di blocco alternativi, 94 messaggi di blocco personalizzati, 90 messaggio e-mail personalizzazione rapporti di presentazione, 117 personalizzazione rapporti investigativi, 143 metodo di inserimento registro, 319 Microsoft Excel rapporti incompleti, 404

Microsoft SQL Server, 309 Microsoft SQL Server Desktop Engine, 309 minacce nei file, 154 nella pagine Web, 153 scansione per, 153 modalità console eDirectory Agent, 384 modalità mista Active Directory, 65 modalità nativa Active Directory, 65 modelli, 55 filtro categoria, 49, 55 filtro protocollo, 52, 56 modelli filtro, 55 Modifica filtro categoria, 50 gruppo LDAP personalizzato, 69 modifica criteri, 79 filtri categoria, 50 filtri per restrizioni di accesso, 175 filtri protocollo, 53 impostazioni per i client, 72 modifica categoria URL, 188 Modifica categorie, pulsante, 178 modifica indirizzo IP Policy Server, 285 Modifica protocolli, pulsante, 178 modifiche cache, inserimento, 21 revisione, 21 salvataggio, 21 modifiche memorizzate nella cache, 21 molteplici criteri priorità di filtraggio, 61 molteplici Policy Server, 284 molteplici ruoli, autorizzazione, 246 monitoraggio NIC, 355 motori database supportati, 309 MSDE, 309 MyWebsense, portale, 29

N

nascondere i nomi utente rapporti investigativi, 125 navigazione Websense Manager, 20 **NetBIOS** attivazione, 380 Network Agent, 277, 349 blocco, scheda NIC, 356 comunicazione con Filtering Service, 375 configurazione dell'hardware, 350 Configurazione NIC, 355 e Remote Filtering, 162 impostazioni globali, 352 impostazioni locali, 353 monitoraggio NIC, 355 più di 2 schede NIC, 375 NIC di blocco, 356 NIC, configurazione blocco, 356 nome del file rapporto di presentazione pianificato, 101 Non eseguire mai la scansione, 152 aggiunta di siti, 156 Non eseguire mai la scansione, elenco eliminazione voci, 157 Novell, eDirectory, 67 NT Directory / Active Directory di Windows (modalità mista), 65 numero eccessivo di avvisi, limiti, 293

0

ODBC, 318 Oggi, pagina, 22 personalizzazione, 24 Riepilogo avviso di integrità, 22 Open Database Connectivity (ODBC), 318 opzioni di impostazione in tempo reale, 151 opzioni di output rapporti investigativi, 344 opzioni di visualizzazione rapporti investigativi, 344 opzioni in tempo reale, 153, 158 categorizzazione contenuto, 152 creazione rapporti, 158 eliminazione di un contenuto, 155 salvataggio modifiche, 157 scansione dei file, 154 opzioni, rapporti investigativi, 120 ordine filtraggio, 83

P

pagina Identificazione utente, 208 pagina Oggi grafici, 23 pagine di blocco, 87 Continua, pulsante, 45 file d'origine, 89 modifica del logo, 91 ripristino delle predefinizioni, 93 sovrascrittura password, 47 Utilizza tempo assegnato, pulsante, 45 variabili contenuto, 92 parole chiave, 178, 184 blocco, 46 blocco per i ruoli, 273 definizione, 185 non bloccata, 371 partizioni creazione, 338 database di registrazione, 328 eliminazione, 310, 340 opzioni rollover, 331 selezione di rapporti, 339 partizioni database creazione, 338 eliminazione, 336, 340 opzioni rollover, 331 selezione dei rapporti, 339 passaggio a un altro ruoli, 245 passaggio da un ruolo a un altro, 245 password modifica per l'utente Websense, 258, 260 utenti Websense, 246, 257 WebsenseAdministrator, 243 password WebsebseAdministrator ridefinizione a causa perdita, 29 patch correttivi, 29 PDF, formato rapporti investigativi, 146

perdita della password WebsebseAdministrator, 29 personalizzazione Cronologia, pagina, 26, 27 messaggi di blocco, 89 Oggi, pagina, 24 pagina Oggi, 24 Pianificatore, rapporti di presentazione, 112 pianificazione tempi definizione criteri, 79 Policy Broker, 277 e Policy Database, 282 Policy Database, 277, 282 Policy Server, 277, 282 aggiunta a Websense Manager, 283 e Policy Database, 282 e Websense Manager, 283 modifica indirizzo IP, 285 molteplici istanze, 284 molteplici istanze, configurazione registrazioni, 314 rimozione da Websense Manager, 283 preferenze per creazione rapporti, 314 Preferiti rapporti di presentazione, 98, 100, 102, 108, 110 rapporti investigativi, 120, 139, 140, 141 Principale, scheda, 20 priorità criterio di filtraggio, 61 filtraggio, 83 ruolo di amministrazione con delega, 268 priorità, ruolo, 259, 268 processi database di registrazione, 329 ETL, 329 IBT, 329 manutenzione database di registrazione, 329 rapporti di presentazione pianificati, 113, 117 rapporti investigativi pianificati, 141, 144 SQL Server Agent, 402 processi del database ETL, 329 manutenzione, 329 SQL Server Agent, 402

Tempo di navigazione in Internet (IBT - Internet browse time), 329 processi pianificati attivazione, 118 cronologia processo, 119 disattivazione, 118 eliminazione, 118 formato di output, 116 intervallo date, 116, 143 nome file del rapporto, 101 personalizzazione e-mail, 117, 143 pianificazione tempi, 113, 142 rapporti di presentazione, 113, 115, 117 rapporti investigativi, 120, 141 processo di manutenzione configurazione, 336 database di registrazione, 329 processo ETL, 329 Produttività, categoria, 40 profilo utente problemi dello script di accesso, 381 Protezione estesa, 41 protocolli aggiunti al Master Database, 39 blocco per tutti i ruoli, 272, 274 creazione nuovi protocolli, 190 definiti, 32, 39 definizione personalizzata, 178 definizioni, 189 elenco completo, 39 filtraggio, 53 filtro, 189 gruppi di protocolli per la sicurezza, 44 modifica definita da Websense, 195 non registrato, 402 nuovo nome, personalizza, 192 raccolta di dati sull'uso, 32 registrazione per tutti i ruoli, 274 selezione di rapporti investigativi, 131 selezione rapporti di presentazione, 107 supporto TCP e UDP, 54 uso larghezza di banda, 195 protocolli personalizzati, 189 creazione, 193

identificatori, 191 impossibile creare, 394 modifica, 191 nuovo nome, 192 protocolli supportati, 161, 162 protocollo definizioni, 189 gestione, 178 messaggi di blocco, 88

R

RADIUS Agent, 224, 282 configurazione, 226 rapporti amministratore, 252 autorizzazioni, 255 configurazione rapporti investigativi, 341 conservazione, 101 Dettaglio giornaliero attività utente, 133 Dettaglio mensile attività utente, 134 distribuzione e-mail, 314 incompleti, 404 investigativi, 97, 98 presentazione, 97 vuoti, 402 rapporti di presentazione, 97, 309 catalogo rapporti, 100 coda processi, 103, 117 conferma filtro di rapporto, 110 conservazione, 101 copia, 103 cronologia processo, 119 esecuzione, 111 Excel, formato, 112 filtro di rapporto, 102, 104 filtro per rapporti, 100 formato di output, 116 formato Excel, 101, 112, 117 formato HTML, 101 formato PDF, 101, 112, 117 formato XLS, 101, 112 HTML, formato, 112 impostazione intervallo di date per il processo, 116

logo personalizzato, 104, 109 nome catalogo rapporti, 108 nome del file, 101 pianificazione, 112, 113 pianificazione tempi, 103 Preferiti, 98, 100, 102, 108, 110 salvataggio, 112 stampa, 112 uso dello spazio su disco, 101 rapporti di riepilogo multi-livello, 126 rapporti investigativi, 122 rapporti investigativi, 97, 98, 309 accesso, 26 anonimo, 125 atipici, 145 attività utente, 120, 147, 346 casi atipici, 120 coda processi, 120, 144 configurazione, 341 criteri di ricerca, 405 definizione pianificazione per, 142 dettagli, visualizzazione, 127, 128, 130 Dettaglio giornaliero attività utente, 133 Dettaglio mensile attività utente, 134 Excel, formato, 143, 146 formato Excel, 121 formato PDF, 121, 143, 146 grafico a barre, 124 grafico a torta, 124 impostazioni predefinite, 343 lettere in rosso, 123 nascondere i nomi utente, 125 opzioni, 120 opzioni di output, 344 opzioni di visualizzazione, 344 panoramica, 98, 120 personalizzazione e-mail, 143 Preferiti, 120, 139, 140 processi pianificati, 120, 141 ricerca, 125, 405 riepilogo, 122 riepilogo multi-livello, 126 salvataggio dei Preferiti, 139

scelta di un database di registrazione, 342 stampa, 146 standard, 120, 137 XLS, formato, 146 rapporti standard, investigativi, 120, 137 rapporto uso, 97 Real-Time Security Updates, 299 Real-Time Security Updates[™], 33 registrazione accessi, 322 anonima, 315 avanzata, 320 categorie, 310, 314 configurazione, 314 molteplici Policy Server, 314 definiti, 312 informazioni utente, 314 opzioni in tempo reale, 158 opzioni in tempo reale/filtraggio, 159 record di registro, 323 selettiva, registrazione categorie, 315 strategia, 310 URL completi, 324, 333 visite, 322 registrazione anonima, 315 registrazione avanzata, 320 registrazione categorie selettiva, 315 registrazione di determinate categorie, 310 registrazione di URL completi, 310, 324, 333 registrazione protocolli per tutti i ruoli, 274 registrazione, record, 158 registro, 165 controllo, 289 metodo di inserimento, 318 registro di controllo, 289 registro di errori eliminazione dal database di registrazione, 337 visualizzatore eventi, 406 visualizzazione per il database di registrazione, 341 Websense.log, 407 reindicizzazione del database di registrazione, 336

Remote Filtering, 161 chiusura contro errori, 168 chiusura contro errori, timeout, 168 client, 278 e Network Agent, 162 file registro, 169 impostazioni, 168 server, 278 Remote Filtering Client, 162 rename filtri protocollo, 53 requisiti della memoria database, download, 367 rete client. 61 ricerca barra degli indirizzi, 371 client directory, 71 rapporti investigativi, 125, 405 ricerca utenti, 71 richieste bloccate larghezza di banda registrata, 123 richieste bloccate, larghezza di banda registrata, 132 ridefinizione password WebsebseAdministrator, 29 rilascio autorizzazione criterio, 250 rilevamento attività Internet, 292 modifiche sistema, 289 rinomina categoria, 182 criteri, 79 filtri per restrizioni di accesso, 175 protocollo personalizzato, 192 ripristino dei dati Websense, 300 risparmio ampiezza di banda Cronologia, pagina, 28 risparmio tempi Cronologia, pagina, 25, 28 risparmio uso larghezza di banda Cronologia, pagina, 25 Risultati del giorno, grafico, 22 rollover, opzioni partizioni database, 331 ruoli

aggiunta, 259, 260 aggiunta client gestiti, 249, 252, 262, 266 aggiunta di amministratori, 261, 265 amministrativi, 242 amministratori in molteplici, 265 applicazione criteri, 249, 254 Autorizza sempre, filtro, 249 blocco dei protocolli, 274 blocco delle categorie, 272 Blocco filtro, effetto, 271 client in molteplici, 268 client sovrapposti, 253 creazione criteri, 254 creazione filtri, 254 eliminazione, 259 eliminazione client, 262 eliminazione Super Administrator, 242, 269 eliminazione, effetto, 269 modifica, 261 modifica criteri, 253 modifica filtri, 253 nomi, 259 passaggio, 245 priorità, 259, 268 Super Administrator, 241, 242, 243 visualizzazione definizioni, 252 ruoli amministrativi, 242

S

Salva tutto, 21 salvataggio di rapporti di presentazione, 112 scansione applicazione, 154 scansione contenuto, 149, 151 scansione dei file file, estensione, 154 impostazione dimensioni massime, 154 scansione in tempo reale, 149 aggiornamenti del database, 150 impostazioni, 151 panoramica, 150 scansione per minacce, 153 script di accesso attivazione di NetBIOS, 380 problemi di profilo utente, 381

problemi di visibilità del controller di dominio, 380 Security Gateway, 279 Server, 161 server proxy configurazione download del database, 35 uso di Log Server, 327 server Trap Configurazione avvisi SNMP, 294 servizi interruzione e riavvio, 290 servizi di directory configurazione, 65 configurazione per l'accesso a Websense Manager, 256 Connessione a Log Server, 401 NT Directory / Active Directory di Windows (modalità mista), 65 ricerca, 71 Servizi, finestra di dialogo, 406 sessione di navigazione, 335 sessione, navigazione, 335 set di caratteri MBCS, 362 utilizzato con LDAP, 68 sicurezza, categoria, 40 sicurezza, pagina di blocco, 313 SiteWatcher, 30 Software Websense componenti, 276 soglia tempo di lettura, 334 sottoscrizioni MyWebsense, portale, 29 scadute, 29 superate, 29 sovrascrittura password, 47 sovrascrivi azione categorie, 181 protocolli, 192 spazio su disco requisiti del database di registrazione, 310 requisiti del download del database, 366 uso dei rapporti di presentazione, 101 spostamento a un ruolo diverso, 72 client, 248

spostamento siti in un'altra categoria, 188 SOL Server autorizzazioni, 397 SQL Server Agent processo, 402 stampa Cronologia, pagina, 27 Oggi, pagina, 24 pagina Oggi, 300 rapporti di presentazione, 112 rapporti investigativi, 146 Stampa criteri su file, 77 Stato Avvisi, 299 Cronologia, 25 Oggi, 22 Registro di controllo, 289 stato Websense, 299 Avvisi, 299 Cronologia, 25 Oggi, 22 Registro di controllo, 289 stime risparmio larghezza di banda, 28 risparmio tempi, 28 strumenti Accesso URL, 203 categoria degli URL, 202 opzione Trova utente, 204 Verifica criterio, 202 Verifica filtri, 203 Verifica utente, 203 strumenti di diagnostica e risoluzione problemi Servizi, finestra di dialogo, 406 visualizzatore eventi, 406 websense.log, 407 strumento Accesso URL, 203 strumento categoria degli URL, 202 Super Administrator aggiunta di client ai ruoli, 248 autorizzazioni, 243 Blocco filtro, effetto, 271 copia criteri, 249 copia filtri, 249 eliminazione ruolo, 242, 269

parziale, 244 passaggio da un ruolo a un altro, 245 qualifica totale, 244, 262 ruolo, 241, 242, 243 spostamento dei client da un ruolo, 248, 249 WebsenseAdministrator, 18 Super Administrator, qualifica totale, 262 supporto TCP e UDP, 54 supporto VPN, 167

Т

tempo assegnato, 46 applet, 47 applicazione ai client, 46 in un ambiente con molteplici Policy Server, 284 sessioni, 46 tempo di lettura, 335 tempo di navigazione Internet (IBT), 99, 334 Tempo di navigazione in Internet (IBT - Internet browse time) processo database, 99 spiegazione, 99 tempo di navigazione in Internet (IBT - Internet browse time) rapporti, 334 tempo di navigazione in Internet (IBT) e consolidamento, 401 tempo di lettura, 334, 335 ThreatWatcher, 30 timeout creazione rapporti, 398 disattivo per Websense Manager, 24 timeout sessione, 19 tipi di file, 179 aggiunta, 199 blocco, 46 blocco per i ruoli, 273 modifica, 199 titolo rapporto, rapporti di presentazione, 108 titolo, rapporti di presentazione, 108

U

URL autorizzati per tutti gli utenti, 187

URL non filtrati, 179, 186 definizione, 187 non applicato, 393 URL personalizzati definiti, 186 priorità di filtraggio, 186 URL ricategorizzati, 186 aggiunta, 188 modifica, 188 spiegazione, 178 URL senza blocco, 187 Usage Monitor, 278 User Service, 64, 281 uso di blocchi più restrittivi filtri per restrizioni di accesso, 173 uso di un blocco più restrittivo, 173 utente, 241, 242 utente con qualifica parziale di Super Administrator, 244 utente con qualifica totale di Super Administrator, 244 utente predefinito, 242, 243 eliminazione, 242 utenti, 61, 64 autenticazione manuale, 207 identificazione, 205 identificazione trasparente, 205 identificazione utente remoto, 165 utenti mancanti dopo l'aggiornamento, 362 utenti remoti, identificazione, 165 utilità configurazione Log Server, 316 utilità di backup, 300 Utilità di configurazione Log Server, 316 utilità di ripristino, 300 Utilizza filtri personalizzati, 68 utilizza tempo assegnato, 46 pagina di blocco, pulsante, 45

V

valutazione criteri di filtraggio, 97 Verifica criterio Trova utenti, 204 Verifica criterio, strumento, 202 Verifica filtri Trova utenti, 204 Verifica filtri, strumento, 203 Verifica utente, strumento, 203 visite definiti, 322 registrazione, 310, 322 Visualizza modifiche in sospeso, 21 visualizzatore eventi, 406 visualizzazione dettagli rapporti investigativi, 127 VPN, 167 split-tunneled, 167

W

WebCatcher, 325 Websense Explorer per Linux, 97, 311 Websense Manager, 17, 278 accesso, 18 accesso amministrativo, 255 accesso con l'account di rete, 255 accesso simultaneo da parte degli amministratori, 270 accesso tramite l'account utente di Websense, 257 disattivazione timeout, 24 intestazione di Websense, 20 lancio, 17 navigazione, 20 timeout sessione, 19 Websense Master Database, 32 Websense Web Protection Services[™], 30 websense.log, 407 WebsenseAdministrator, 18, 243 eliminazione, 242 password, 243 Windows Servizi, finestra di dialogo, 406 visualizzatore eventi, 406

X

XLS, formato registro di controllo, 289