



# **Websense Manager 說明**

Websense® Web Security  
Websense Web Filter

**7.0 版**

©1996–2008, Websense Inc.

All rights reserved.

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2008

Printed in the United States and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

## **Trademarks**

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).

Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

# 目錄

<b>主題 1</b>	<b>快速入門</b> .....	<b>15</b>
	概覽 .....	16
	使用 <b>Websense Manager</b> .....	16
	登入 <b>Websense Manager</b> .....	17
	瀏覽 <b>Websense Manager</b> .....	19
	檢閱、儲存及放棄變更 .....	20
	今天：自午夜算起的健全度、安全性及數值 .....	21
	自訂今天頁面 .....	22
	記錄：最後 30 天 .....	23
	節省的時間與頻寬 .....	24
	自訂記錄頁面 .....	25
	您的訂閱 .....	26
	透過 <b>MyWebsense</b> 入口網站管理帳戶 .....	26
	啟動 <b>Websense Web Protection Services™</b> .....	27
	設定帳戶資訊 .....	27
	<b>Websense Master Database</b> .....	29
	即時資料庫更新 .....	29
	即時安全性更新™ .....	30
	設定資料庫下載 .....	30
	測試網路配置 .....	31
	<b>Websense 技術支援</b> .....	32
<b>主題 2</b>	<b>網際網路使用量篩選器</b> .....	<b>33</b>
	篩選類別和通訊協定 .....	34
	特殊類別 .....	35
	風險等級 .....	36
	安全性通訊協定群組 .....	39
	<b>Instant Messaging Attachment Manager</b> .....	39
	篩選動作 .....	39
	使用配額時間來限制網際網路存取 .....	40
	密碼覆寫 .....	41
	搜尋篩選 .....	42
	使用篩選器 .....	42

	建立類別篩選器.....	43
	編輯類別篩選器.....	44
	建立通訊協定篩選器.....	45
	編輯通訊協定篩選器.....	46
	<b>Websense</b> 定義的類別和通訊協定篩選器.....	48
	類別和通訊協定篩選器範本.....	48
	設定 <b>Websense</b> 篩選設定.....	49
<b>主題 3</b>	<b>用戶端</b> .....	53
	使用用戶端.....	54
	使用電腦與網路.....	55
	使用使用者與群組 .....	56
	目錄服務.....	56
	<b>Windows NT Directory / Active Directory</b> (混合模式).....	57
	<b>Windows Active Directory</b> (原生模式).....	57
	<b>Novell eDirectory</b> 與 <b>Sun Java System Directory</b> .....	58
	進階目錄設定.....	59
	使用自訂 <b>LDAP</b> 群組.....	60
	新增或編輯自訂 <b>LDAP</b> 群組.....	60
	新增用戶端.....	61
	搜尋目錄服務.....	62
	變更用戶端設定.....	62
	將用戶端移到角色 .....	63
<b>主題 4</b>	<b>網際網路篩選政策</b> .....	65
	預設政策.....	66
	使用政策.....	67
	建立政策.....	68
	編輯政策.....	68
	將政策指派到用戶端.....	70
	篩選順序.....	71
	篩選網站.....	72
<b>主題 5</b>	<b>封鎖頁面</b> .....	75
	通訊協定封鎖訊息 .....	76
	使用封鎖頁面.....	77
	自訂封鎖訊息.....	77
	變更訊息框架的大小.....	78
	變更封鎖頁面上顯示的標誌.....	79
	使用封鎖頁面內容變數.....	79
	還原至預設封鎖頁面.....	81

建立替代封鎖訊息 .....	81
使用位於其他電腦上的替代封鎖頁面 .....	81
<b>主題 6 使用報告評估篩選政策.....</b>	<b>83</b>
報告概覽 .....	84
網際網路瀏覽時間是什麼？ .....	85
簡報報告 .....	86
複製簡報報告 .....	88
定義報告篩選器.....	88
選取報告的用戶端 .....	89
選取報告的類別 .....	90
選取報告的通訊協定 .....	91
選取報告的動作 .....	92
設定報告選項 .....	92
確認報告篩選器定義 .....	94
使用我的最愛 .....	94
產生簡報報告 .....	95
排程簡報報告 .....	96
設定排程 .....	97
選取要排程的報告 .....	98
設定日期範圍 .....	99
選取輸出選項 .....	99
檢視排程工作清單.....	100
檢視工作記錄 .....	101
調查報告.....	102
摘要報告 .....	103
多層級摘要報告 .....	106
靈活的細節報告 .....	107
靈活的細節報告欄位 .....	109
使用者活動細節報告.....	111
使用者每日活動細節 .....	112
使用者每月活動細節 .....	113
類別對應 .....	114
標準報告 .....	116
我的最愛調查報告 .....	118
將報告儲存到我的最愛 .....	118
產生或刪除我的最愛報告 .....	119
修改我的最愛報告 .....	119
排程調查報告 .....	120
管理排程的調查報告工作.....	122
異常值報告 .....	122
輸出至檔案 .....	123

	列印調查報告 .....	124
	存取自行報告.....	124
<b>主題 7</b>	<b>使用即時選項分析內容.....</b>	<b>127</b>
	資料庫下載.....	128
	掃描選項.....	129
	分類內容與掃描威脅 .....	129
	檔案掃描.....	131
	抽除內容.....	132
	優化掃描.....	133
	即時掃描活動的報告 .....	134
	即時掃描如何記錄.....	135
<b>主題 8</b>	<b>篩選遠端用戶端.....</b>	<b>137</b>
	<b>Remote Filtering</b> 的運作方式.....	138
	網路內部.....	139
	網路外部.....	140
	識別遠端使用者.....	141
	伺服器通訊若失敗.....	141
	虛擬私人網路 (VPN).....	142
	設定 <b>Remote Filtering</b> 設定 .....	143
<b>主題 9</b>	<b>優化篩選政策.....</b>	<b>145</b>
	將使用者限制於定義的網際網路網站清單 .....	145
	限制存取篩選器與篩選優先權.....	146
	建立限制存取篩選器.....	147
	編輯限制存取篩選器.....	148
	從「編輯政策」頁面新增網站 .....	149
	將篩選器和政策複製到角色 .....	149
	建立篩選器元件.....	151
	使用類別.....	152
	編輯類別及其屬性.....	152
	檢閱所有自訂的類別屬性 .....	153
	進行全域類別篩選變更 .....	153
	重新命名自訂類別 .....	154
	建立自訂類別.....	154
	根據關鍵字篩選.....	156
	定義關鍵字 .....	157
	重新定義特定網站的篩選.....	158
	定義未篩選的 URL .....	159
	重新分類 URL .....	160

使用通訊協定.....	160
篩選通訊協定.....	161
編輯自訂通訊協定.....	162
新增或編輯通訊協定識別碼.....	162
重新命名自訂通訊協定.....	163
進行全域通訊協定篩選變更.....	163
建立自訂通訊協定.....	164
新增到 <b>Websense</b> 定義的通訊協定.....	166
使用 <b>Bandwidth Optimizer</b> 管理頻寬.....	166
設定預設的 <b>Bandwidth Optimizer</b> 限制.....	167
根據檔案類型管理流量.....	168
使用檔案類型.....	169
新增自訂檔案類型.....	170
新增副檔名到檔案類型.....	170
使用正規表示式.....	170
使用「工具箱」來驗證篩選行為.....	171
URL 類別.....	172
檢查政策.....	172
測試篩選.....	172
URL 存取.....	173
調查使用者.....	173
識別要檢查政策或測試篩選的使用者.....	173
<b>主題 10</b> 使用者識別.....	<b>175</b>
無障礙識別.....	175
遠端使用者的無障礙識別.....	176
手動驗證.....	177
設定使用者識別方法.....	177
設定特定電腦的驗證規則.....	179
定義使用者識別設定的例外.....	179
修訂使用者識別設定的例外.....	180
安全手動驗證.....	181
產生密碼和憑證.....	182
啟動安全手動驗證.....	183
接受用戶端瀏覽器內的憑證.....	184
<b>DC Agent</b> .....	185
設定 <b>DC Agent</b> .....	186
<b>Logon Agent</b> .....	187
設定 <b>Logon Agent</b> .....	188
<b>RADIUS Agent</b> .....	190

處理 RADIUS 流量 .....	191
設定 RADIUS 環境 .....	191
設定 RADIUS Agent .....	192
設定 RADIUS 用戶端 .....	193
設定 RADIUS 伺服器 .....	194
<b>eDirectory Agent .....</b>	<b>194</b>
特殊配置考量 .....	195
設定 eDirectory Agent .....	196
新增 eDirectory 伺服器複本 .....	197
設定 eDirectory Agent 使用 LDAP .....	198
啓動完整的 eDirectory 伺服器查詢 .....	198
設定多個代理程式 .....	199
為每個代理程式實例配置不同的設定 .....	201
INI 檔案參數 .....	202
設定代理程式忽略特定的使用者名稱 .....	203
<b>主題 11 委派管理 .....</b>	<b>205</b>
管理角色簡介 .....	206
管理員簡介 .....	206
超級管理員 .....	207
委派管理員 .....	208
具有多個角色的管理員 .....	209
管理角色快速入門 .....	210
通知管理員 .....	212
委派管理員工作 .....	212
檢視您的使用者帳戶 .....	213
檢視您的角色定義 .....	213
新增用戶端到「用戶端」頁面 .....	214
建立政策和篩選器 .....	214
將政策套用至用戶端 .....	216
產生報告 .....	216
啟用 Websense Manager 的存取權限 .....	216
目錄帳戶 .....	216
Websense 使用者帳戶 .....	218
新增 Websense 使用者帳戶 .....	218
變更 Websense 使用者的密碼 .....	219
使用委派管理 .....	220
新增角色 .....	221
編輯角色 .....	221
新增管理員 .....	224
新增受管理的用戶端 .....	225



管理角色衝突 .....	226
特殊考量 .....	227
多個存取 <b>Websense Manager</b> 的管理員 .....	228
定義所有角色的篩選限制 .....	229
建立「篩選器鎖定」 .....	230
鎖定類別 .....	230
鎖定通訊協定 .....	231
<b>主題 12</b> <b>Websense Server 管理</b> .....	<b>233</b>
<b>Websense 產品元件</b> .....	<b>234</b>
篩選元件 .....	235
報告元件 .....	237
使用者識別元件 .....	237
瞭解 <b>Policy Database</b> .....	238
使用 <b>Policy Server</b> .....	239
新增及編輯 <b>Policy Server</b> 實例 .....	239
在多 <b>Policy Server</b> 環境中運作 .....	240
變更 <b>Policy Server IP</b> 位址 .....	240
使用 <b>Filtering Service</b> .....	242
檢閱 <b>Filtering Service</b> 詳細資料 .....	243
檢閱 <b>Master Database</b> 下載狀態 .....	243
可繼續的 <b>Master Database</b> 下載 .....	244
檢視並匯出稽核記錄 .....	244
停止和啓動 <b>Websense</b> 服務 .....	245
警示 .....	246
流量控制 .....	247
設定一般警示選項 .....	248
設定系統警示 .....	249
設定類別使用警示 .....	250
新增類別使用警示 .....	250
設定通訊協定使用警示 .....	251
新增通訊協定使用警示 .....	252
檢閱目前的系統狀態 .....	252
備份與還原 <b>Websense</b> 資料 .....	253
排程備份 .....	255
執行立即備份 .....	256
維護備份檔案 .....	257
還原 <b>Websense</b> 資料 .....	257
終止已排程的備份 .....	258

	指令參考.....	259
<b>主題 13</b>	<b>報告管理.....</b>	<b>261</b>
	計畫您的配置.....	262
	管理報告工具的存取.....	262
	基本配置.....	263
	將類別指派到風險等級.....	264
	設定報告偏好設定.....	265
	設定用於記錄的 <b>Filtering Service</b> .....	265
	<b>Log Server Configuration</b> 公用程式.....	267
	設定 <b>Log Server</b> 連接.....	268
	設定 <b>Log Server</b> 資料庫選項.....	269
	設定資料庫連接.....	270
	設定記錄快取檔案.....	271
	設定合併選項.....	272
	設定 <b>WebCatcher</b> .....	274
	<b>WebCatcher</b> 驗證.....	276
	停止和啟動 <b>Log Server</b> .....	276
	記錄資料庫簡介.....	277
	資料庫工作.....	278
	管理記錄資料庫.....	278
	記錄資料庫管理設定.....	279
	設定變換選項.....	280
	設定完整 <b>URL</b> 記錄.....	281
	設定網際網路瀏覽時間選項.....	282
	設定記錄資料庫維護選項.....	283
	設定記錄資料庫分割區建立.....	284
	設定可用的分割區.....	285
	檢視錯誤記錄.....	286
	設定調查報告.....	287
	資料庫連接與報告預設值.....	287
	顯示與輸出選項.....	289
	自行報告.....	291
<b>主題 14</b>	<b>網路配置.....</b>	<b>293</b>
	硬體配置.....	294
	<b>Network Agent</b> 配置.....	295
	設定全域設定.....	296
	設定本機設定.....	297
	設定網路卡設定.....	298
	設定網路卡的監控設定.....	299

新增或編輯 IP 位址 .....	300
驗證 Network Agent 配置 .....	301
<b>主題 15 疑難排解 .....</b>	<b>303</b>
安裝與訂閱問題 .....	303
Websense 「狀態」顯示訂閱問題 .....	303
更新之後，在 Websense Manager 中找不到使用者 .....	304
Master Database 問題 .....	304
正在使用初始篩選資料庫 .....	304
Master Database 已超過 1 星期沒有更新 .....	305
Master Database 未下載 .....	305
訂閱密碼 .....	306
網際網路存取 .....	306
驗證防火牆或代理伺服器設定 .....	307
磁碟空間不足 .....	307
記憶體不足 .....	308
限制應用程式 .....	309
Master Database 下載未在正確時間執行 .....	309
聯繫「技術支援部」詢問資料庫下載問題 .....	309
篩選問題 .....	310
Filtering Service 沒有執行 .....	310
無法使用 User Service .....	311
錯將網站分類為「資訊科技」 .....	311
沒有對關鍵字進行封鎖 .....	311
自訂或限制存取篩選器 URL 未按預期篩選 .....	312
使用者無法如預期地存取通訊協定或應用程式 .....	312
未如預期地封鎖 FTP 要求 .....	312
Websense 軟體未套用使用者或群組政策 .....	313
遠端使用者沒有經過正確政策的篩選 .....	313
Network Agent 問題 .....	313
未安裝 Network Agent .....	313
Network Agent 沒有執行 .....	313
Network Agent 沒有監控任何網路卡 .....	314
Network Agent 無法與 Filtering Service 通訊 .....	314
更新 Filtering Service IP 位址或 UID 資訊 .....	315
使用者識別問題 .....	315
疑難排解 DC Agent .....	316
使用者錯誤地由預設政策篩選 .....	316
手動變更 DC Agent 與 User Service 權限 .....	317
疑難排解 Logon Agent .....	318
群組原則物件 .....	318

在 Linux 上執行 User Service .....	319
網域控制站能見度 .....	319
NetBIOS .....	319
使用者設定檔問題 .....	320
疑難排解 eDirectory Agent .....	320
啟用 eDirectory Agent 診斷 .....	321
eDirectory Agent 對 eDirectory Server 連線的計數錯誤 ...	322
以主控台模式執行 eDirectory Agent .....	322
疑難排解 RADIUS Agent .....	322
以主控台模式執行 RADIUS Agent .....	323
遠端使用者沒有獲得進行手動驗證的提示 .....	324
遠端使用者沒有獲得正確篩選 .....	324
封鎖訊息問題 .....	324
封鎖檔案類型沒有顯示封鎖頁面 .....	325
使用者收到瀏覽器錯誤而不是封鎖頁面 .....	325
顯示空白頁面而不是封鎖頁面 .....	326
通訊協定封鎖訊息未如預期地顯示 .....	326
顯示通訊協定封鎖訊息而不是封鎖頁面 .....	326
記錄、狀態訊息及警示問題 .....	327
我在哪裡可以找到 Websense 元件的錯誤訊息？ .....	327
Websense 健全度警示 .....	327
單一要求產生了兩個 Log 記錄 .....	328
Policy Server 與 Policy Database 問題 .....	328
忘記密碼 .....	328
無法登入 Policy Server .....	329
Websense Policy Database 服務無法啟動 .....	329
委派管理問題 .....	329
無法從角色刪除受管理的用戶端 .....	330
登入錯誤顯示有其他人已登入我的電腦 .....	330
有些使用者無法存取「未篩選的 URL」清單上的網站 .....	330
已重新分類的網站根據錯誤的類別篩選 .....	330
我無法建立自訂通訊協定 .....	330
報告問題 .....	331
Log Server 沒有執行 .....	331
沒有為 Policy Server 安裝 Log Server .....	332
記錄資料庫未建立 .....	333
記錄資料庫無法使用 .....	333
記錄資料庫大小 .....	334
Log Server 沒有在記錄資料庫中記錄資料 .....	334
更新 Log Server 連線密碼 .....	335

設定 <b>Microsoft SQL Server 2005</b> 的使用者權限 .....	335
<b>Log Server</b> 無法連接到目錄服務 .....	336
網際網路瀏覽時間報告中的資料不準確 .....	336
頻寬比預期的更大 .....	336
有些通訊協定要求沒有記錄 .....	337
所有報告都是空的 .....	337
資料庫分割區 .....	337
<b>SQL Server Agent</b> 工作 .....	337
<b>Log Server</b> 配置 .....	338
「今天」或「記錄」頁面上沒有顯示圖表 .....	338
無法存取某些報告功能 .....	338
<b>Microsoft Excel</b> 輸出缺少某些報告資料 .....	339
將簡報報告輸出儲存為 <b>HTML</b> .....	339
調查報告搜尋問題 .....	339
一般調查報告問題 .....	340
疑難排解工具 .....	340
「 <b>Windows 服務</b> 」對話方塊 .....	340
<b>Windows</b> 事件檢視器 .....	340
<b>Websense</b> 記錄檔 .....	341



# 1

## 快速入門

Websense 軟體為業界所有部門 (從商業部門到教育部門、政府部門，及更高部門) 的網路管理員提供控制與監控到網際網路之網路流量的功能。

- ◆ 可在最大程度上減少員工存取令人不快、不適當或與工作無關的網際網路資料所耗費的停機時間。
- ◆ 使因不當存取造成的網路資源誤用及合法動作威脅降至最低。
- ◆ 在網路上新增穩固的安全性層級，使網路免受潛在的間諜軟體、惡意軟體、駭客入侵及其他入侵的侵害。

可在此處找到下列資訊：

基本 Websense 配置	執行網際網路篩選
<ul style="list-style-type: none"><li>• <a href="#">使用 Websense Manager</a>，第 16 頁</li><li>• <a href="#">您的訂閱</a>，第 26 頁</li><li>• <a href="#">Websense Master Database</a>，第 29 頁</li><li>• <a href="#">驗證 Network Agent 配置</a>，第 301 頁</li></ul>	<ul style="list-style-type: none"><li>• <a href="#">篩選類別和通訊協定</a>，第 34 頁</li><li>• <a href="#">新增用戶端</a>，第 61 頁</li><li>• <a href="#">使用政策</a>，第 67 頁</li><li>• <a href="#">將政策指派到用戶端</a>，第 70 頁</li></ul>

也可以了解如何：

評估配置	優化篩選政策
<ul style="list-style-type: none"><li>• <a href="#">今天：自午夜算起的健全度、安全性及數值</a>，第 21 頁</li><li>• <a href="#">記錄：最後 30 天</a>，第 23 頁</li><li>• <a href="#">簡報報告</a>，第 86 頁</li><li>• <a href="#">調查報告</a>，第 102 頁</li><li>• <a href="#">使用「工具箱」來驗證篩選行為</a>，第 171 頁</li></ul>	<ul style="list-style-type: none"><li>• <a href="#">建立自訂類別</a>，第 154 頁</li><li>• <a href="#">重新定義特定網站的篩選</a>，第 158 頁</li><li>• <a href="#">將使用者限制於定義的網際網路網站清單</a>，第 145 頁</li><li>• <a href="#">根據關鍵字篩選</a>，第 156 頁</li><li>• <a href="#">根據檔案類型管理流量</a>，第 168 頁</li><li>• <a href="#">使用 Bandwidth Optimizer 管理頻寬</a>，第 166 頁</li></ul>

## 概覽

---

Websense 軟體與整合裝置 (包括代理伺服器、防火牆、路由器及快取設備) 一起使用，提供引擎與配置工具，以便開發、監控及強制執行網際網路存取政策。

同時，還有一系列的 Websense 元件 (描述於 [Websense 產品元件](#)，第 234 頁中) 提供網際網路篩選、使用者識別、警示、報告及疑難排解功能。

本 Websense 軟體版本中包含的新功能概覽可在[版本資訊](#)中找到，此版本資訊可在 [Websense 支援入口網站](#)中取得。

在安裝之後，Websense 軟體會套用預設政策以監控網際網路使用量，但是不會封鎖要求。在您定義自己的政策並將其指派到用戶端之前，此政策會控管網路中所有用戶端的網際網路存取。即使在您建立自訂篩選設定之後，當用戶端未受到任何其他政策控管時，就會隨時套用「預設」政策。如需詳細資訊，請參閱 [預設政策](#)，第 66 頁。

會在下列章節中描述建立篩選器、新增用戶端、定義政策以及將政策套用到用戶端的程序：

- ◆ [網際網路使用量篩選器](#)，第 33 頁
- ◆ [用戶端](#)，第 53 頁
- ◆ [網際網路篩選政策](#)，第 65 頁

Websense Manager 是一個以瀏覽器為基礎的單一工具，為 Websense 軟體的一般配置、政策管理及報告功能提供中央式圖形介面。如需詳細資訊，請參閱 [使用 Websense Manager](#)，第 16 頁。

可以定義 Websense Manager 的存取層級，讓特定管理員僅能管理特定的用戶端群組，或允許個人針對他們自己的網際網路使用量製作報告。如需詳細資訊，請參閱 [委派管理](#)，第 205 頁。

## 使用 Websense Manager

---

相關主題：

- ◆ [登入 Websense Manager](#)，第 17 頁
- ◆ [瀏覽 Websense Manager](#)，第 19 頁
- ◆ [今天：自午夜算起的健全度、安全性及數值](#)，第 21 頁
- ◆ [記錄：最後 30 天](#)，第 23 頁



Websense Manager 是中央式配置介面，用來自訂篩選行為、監控網際網路使用、產生網際網路使用報告，以及管理 Websense 軟體配置與設定。這個以網路為基礎工具可在下列 2 種支援的瀏覽器上執行：

- ◆ Microsoft Internet Explorer 7
- ◆ Mozilla Firefox 2

雖然可能可以使用其他瀏覽器來啟動 Websense Manager，但使用支援的瀏覽器可獲得完整的功能及正確的應用程式顯示。

要啟動 Websense Manager，請執行下列某項操作：

- ◆ 在 Windows 電腦上：
  - 前往**開始 > 所有程式 > Websense**，然後選取 **Websense Manager**。
  - 連按兩下 Websense Manager 桌面圖示。
- ◆ 在您網路中任一部電腦上，開啓支援的瀏覽器並輸入下列內容：  
`https://<IP 地址>:9443/mng`

使用 Websense Manager 電腦的 IP 位址取代 *<IP 地址>*。

如果無法在預設連接埠上連線到 Websense Manager，請參考 Websense Manager 電腦上的 **tomcat.log** 檔案 (預設位於 **C:\Program Files\Websense\tomcat\logs\** 或 **/opt/Websense/tomcat/logs/** 目錄) 以便確認連接埠。

如果使用的是正確的連接埠，但依然無法從遠端電腦連線到 Websense Manager，請確認防火牆允許該連接埠的通訊。

與 Websense Manager 之間以瀏覽器為基礎的通訊，會使用 SSL 連線以確保安全。此連線使用 Websense, Inc. 核發的安全性憑證。由於支援的瀏覽器並未將 Websense, Inc. 識別為已知的憑證授權單位，因此第一次從新的瀏覽器啟動 Websense Manager 時會顯示憑證錯誤。要避免看到此錯誤，可以在瀏覽器中安裝或永久接受該憑證。如需指示，請參閱 [Websense 知識庫](#)。

接受安全性憑證之後，瀏覽器視窗中就會顯示 Websense Manager 登入頁面 (請參閱 [登入 Websense Manager](#))。

## 登入 Websense Manager

相關主題：

- ◆ [使用 Websense Manager](#)
- ◆ [瀏覽 Websense Manager](#)，第 19 頁
- ◆ [今天：自午夜算起的健全度、安全性及數值](#)，第 21 頁
- ◆ [記錄：最後 30 天](#)，第 23 頁

安裝後，登入 Websense Manager 的第一個使用者具有完整的管理存取權。該使用者名稱為 **WebsenseAdministrator**，而且不可變更。WebsenseAdministrator 密碼會在安裝期間設定。

要登入，請先啓動 Websense Manager (請參閱[使用 Websense Manager](#))。在登入頁面上：

1. 選取 **Policy Server** 以便管理。  
如果環境僅包含一個 Policy Server，則預設會選取此環境。
2. 選取**帳戶類型**：
  - 要使用 Websense 使用者帳戶 (例如 WebsenseAdministrator) 登入，請按一下 **Websense 帳戶** (預設)。
  - 要使用網路認證登入，請按一下**網路帳戶**。
3. 輸入**使用者名稱及密碼**，然後按一下**登入**。

現在已登入 Websense Manager。

- ◆ 如果這是首次登入 Websense Manager，系統會提供啓動「快速入門」教學課程的選項。強烈建議 Websense 軟體的新手，或此版本的 Websense 軟體的新手完成「快速入門」教學課程。
- ◆ 如果使用「委派管理」，而且已經建立管理角色，系統可能會提示選取角色以便管理。如需詳細資訊，請參閱[委派管理](#)，第 205 頁。

在使用者介面中執行最後一個動作 (在頁面之間切換、輸入資訊、快取變更或儲存變更) 30 分鐘後，Websense Manager 工作階段就會結束。在工作階段結束前 5 分鐘，會顯示警告訊息。

- ◆ 如果頁面上有未快取的變更，或快取的變更正在擱置中，那麼這些變更會在工作階段結束時遺失。請記得按一下**確定**以便快取，以及按一下**全部儲存**以儲存並執行所有變更。
- ◆ 如果在同一個瀏覽器視窗的多個標籤中開啓 Websense Manager，則所有實例會共用同一個工作階段。如果其中一個標籤的工作階段逾時，則所有標籤的工作階段都會逾時。
- ◆ 如果在同一個電腦的多個瀏覽器視窗中開啓 Websense Manager，則在**下列情況下**，所有實例會共用同一個工作階段：
  - 使用的瀏覽器是 Microsoft Internet Explorer，並使用 Ctrl-N 捷徑來開啓 Websense Manager 的新實例。
  - 使用的瀏覽器是 Mozilla Firefox。

如果其中一個視窗的工作階段逾時，則所有視窗的工作階段都會逾時。

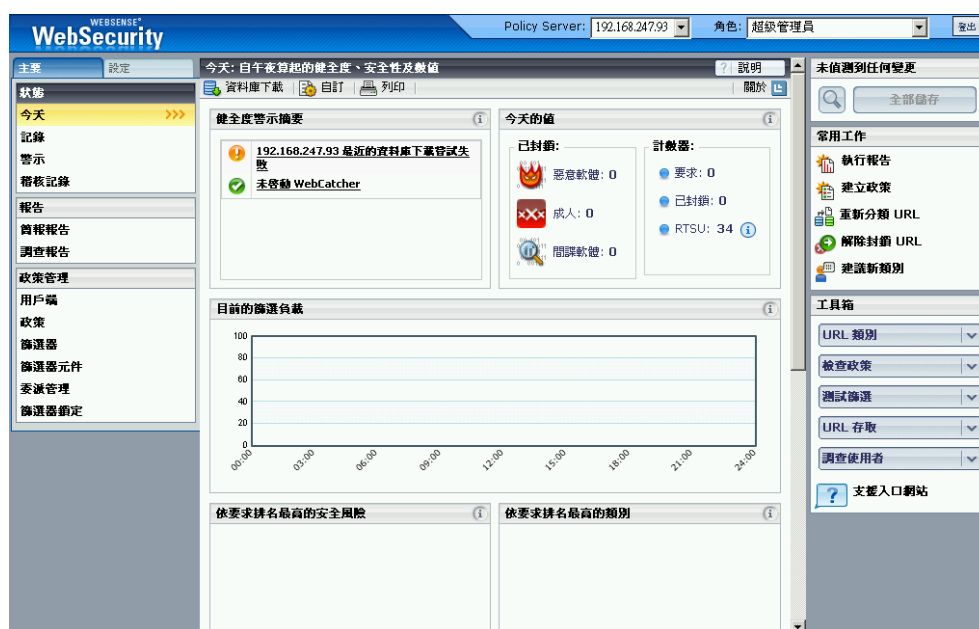
- ◆ 如果啓動多個相互獨立的 Internet Explorer 視窗，然後以不同的 Websense Manager 管理員的身份來透過這些視窗登入，那麼這些視窗**不會**共用工作階段。如果其中一個視窗逾時，其他視窗不會受到影響。

如果在未登出 Websense Manager 的情況下關閉瀏覽器，或者用來存取 Websense Manager 的遠端電腦意外關機，則可能暫時將用戶鎖定。Websense 軟體會在約 2 分鐘內偵測此問題並結束中斷的工作階段，然後用戶就可再次登入。

## 瀏覽 Websense Manager

Websense Manager 介面可分為 4 個主要區域：

1. Websense 標題
2. 左側瀏覽窗格
3. 右側捷徑窗格
4. 內容窗格



Websense 標題會顯示：

- ◆ 目前登入了哪一個 **Policy Server** (請參閱[使用 Policy Server](#)，第 239 頁)
- ◆ 目前的管理**角色** (請參閱[管理角色簡介](#)，第 206 頁)
- ◆ **登出**按鈕，在準備結束管理工作階段時使用

Websense Manager 中顯示的內容會根據登入之使用者所授予的權限而變化。例如，對於僅具有報告權限的使用者，則不會顯示伺服器配置設定或政策管理工具。如需詳細資訊，請參閱[委派管理](#)，第 205 頁。

本節將說明 WebsenseAdministrator 及其他具有「超級管理員」權限之使用者可使用的選項。

**左側瀏覽窗格**有兩個標籤：**主要**及**設定**。使用**主要**標籤可以存取狀態、報告及政策管理功能。使用**設定**標籤可管理 Websense 帳戶及執行全域系統管理工作。

**右側捷徑窗格**包含有用工具與常用管理工具的連結。也可在此處檢閱及儲存在 Websense Manager 中執行的所有變更。

- ◆ 瀏覽窗格的頂部會指示是否還有未儲存的已快取的變更。使用 Websense Manager 時，「變更」列會指示是否有**擱置中的變更**。

在大多數情況下，在 Websense Manager 中執行工作並按下**確定**時，變更就會被快取。(有時必須在下層頁面與主頁上按一下「確定」才會快取變更)。

快取變更後，按一下**全部儲存**以儲存並執行變更。要在儲存之前檢視快取的變更 (請參閱 [檢閱、儲存及放棄變更](#)，第 20 頁)，請按一下**檢視擱置中的變更**按鈕。此為「全部儲存」左側的較小按鈕。

- ◆ **常用工作**提供經常執行之管理工作的捷徑。按一下清單中的項目，可跳至執行該工作的頁面。
- ◆ **工具箱**包含快速查閱工具，可用來驗證篩選設定。如需詳細資訊，請參閱 [使用「工具箱」來驗證篩選行為](#)，第 171 頁。

## 檢閱、儲存及放棄變更

在 Websense Manager 中執行工作並按下**確定**時，變更就會被快取。使用**檢視擱置中的變更**頁面可檢閱已快取的變更。



### 重要

避免連按兩次或連按三次「確定」按鈕。快速按多下相同按鈕可能會導致 Mozilla Firefox 的顯示出現問題，只能結束並重新開啓瀏覽器才能解決此問題。

針對單一區域的功能所做的變更，通常會組成快取清單中的單一項目。例如，如果新增 6 個用戶端並刪除 2 個用戶端，快取清單只會表示已針對用戶端執行變更。另一方面，針對單一「設定」頁面的變更，可能會變成快取清單中的多個項目。使用單一「設定」頁面來設定多個 Websense 軟體功能時，就會發生此狀況。

- ◆ 要儲存所有快取的變更，按一下**儲存所有變更**。
- ◆ 要放棄所有已快取的變更，按一下**取消所有變更**。

選擇「全部儲存」或「全部取消」後，右側捷徑窗格中的「變更」列就會適當地更新，而且會返回所選擇的最後一個頁面。「全部儲存」與「全部取消」功能都無法執行還原。

使用「稽核記錄」可檢閱 Websense Manager 中執行之變更的詳細資訊。如需詳細資訊，請參閱 [檢視並匯出稽核記錄](#)，第 244 頁。

## 今天：自午夜算起的健全度、安全性及數值

相關主題：

- ◆ [瀏覽 Websense Manager](#)，第 19 頁
- ◆ [記錄: 最後 30 天](#)，第 23 頁
- ◆ [自訂今天頁面](#)，第 22 頁
- ◆ [警示](#)，第 246 頁

登入 Websense Manager 時，會先顯示狀態 > 今天：自午夜算起的健全度、安全性及數值頁面。它會顯示篩選軟體的目前狀態，並以圖解說明多達 24 小時的網際網路篩選活動，從上午 12:01 開始 (根據記錄資料庫電腦上的時間)。

在頁面頂端，有 2 個摘要區段提供目前狀態的快速概覽：

- ◆ **健全度警示摘要**會顯示 Websense 軟體的狀態。如果摘要中顯示錯誤或警告，按一下警示訊息可開啓「警示」頁面，其中可取得更詳細的資訊 (請參閱[檢閱目前的系統狀態](#)，第 252 頁)。  
「健全度警示摘要」中的資訊每 30 秒更新一次。
- ◆ 在**今天的值**之下，可檢視 Websense 篩選今天如何保護網路的範例，也可檢視處理的網際網路要求的總數，以及其他重要活動總計。

在摘要資訊之下，有多達 4 個圖表提供有關篩選活動的資訊。可以存取這些圖表的人員包括「超級管理員」，以及獲得檢視「今天」頁面中的報告之權限的委派管理員。請參閱[編輯角色](#)，第 221 頁。

這些圖表中的資訊每 2 分鐘更新一次。可能需要向下捲動才能看到所有圖表。

圖表名稱	說明
目前的篩選負載	檢視處理到記錄資料庫的已篩選網際網路流量的數量，每 10 分鐘顯示一次。
依要求排名最高的安全風險	查看今天收到最多要求的「安全風險」有哪些類別，並且判斷篩選政策是否為您的網路提供適當的防護。
依要求排名最高的類別	查看今天存取最多次的類別。取得高階概況，瞭解潛在的安全、頻寬或生產力的疑慮。
依風險等級政策強制執行	查看今天各個風險等級有多少允許及封鎖的要求 (請參閱 <a href="#">風險等級</a> ，第 36 頁)。評估目前的政策是否有效，或者是否需要變更。
依頻寬排名最高的通訊協定	瞭解今天在您的網路中有哪些通訊協定使用了最多頻寬。使用這項資訊評估頻寬需求，以及是否可能需要政策變更。
要求安全風險網站的電腦	查看今天有哪些電腦存取了「安全風險」網站。您可能要檢查這些電腦，確定沒有感染任何病毒或間諜軟體。

圖表名稱	說明
封鎖最多次的使用者	檢視哪些使用者要求最常被封鎖的網站，深入瞭解組織的網際網路使用是否符合規範。
排名最高的尚未歸類網站	瞭解今天有哪些 Websense Master Database 未分類的網站受到最多次存取。移至常用工作 > 重新分類 URL，將網站指派到篩選類別。

按一下任一個橫條圖，即可開啓調查報告，提供更多詳細資訊。

頁面上方會出現三個按鈕：

- ◆ **資料庫下載**，僅供「超級管理員」使用，可開啓檢視 Master Database 下載狀態的頁面，或開始下載 (請參閱 [檢閱 Master Database 下載狀態](#)，第 243 頁)。
- ◆ **自訂**，僅供「超級管理員」使用，可開啓一個頁面，能夠在其中變更在頁面上顯示的圖表 (請參閱 [自訂今天頁面](#)，第 22 頁)。
- ◆ **列印**，適用於所有管理員，可開啓另一個視窗，其中含有「今天」頁面上顯示之圖表的可供列印版本。使用瀏覽器選項來列印此頁面，如此即可不列印出主要 Websense Manager 視窗中的所有瀏覽選項。

在網際網路活動與篩選圖表之下，**Filtering Service 摘要**會顯示與目前 Policy Server 相關的每個 Filtering Service 的狀態。按一下「Filtering Service IP 位址」，即可檢視關於 Filtering Service 實例的詳細資訊。

基於安全的緣故，在不進行任何活動的 30 分鐘後，Websense Manager 工作階段將會結束。不過可以選擇繼續監控篩選與警示資料：標記「今天」頁面底部的**持續監控**「今天」、「記錄」及「警示」狀態。在關閉瀏覽器或瀏覽至其他 Websense Manager 頁面之前，這 3 頁的資訊會繼續正常更新。



### 重要

如果啓用監控選項並停留在「今天」、「記錄」及「警示」頁面中超過 30 分鐘，那麼當嘗試瀏覽到其他 Websense Manager 頁面時，將會返回「登入」頁面。

啓用此選項時，務必確定在 30 分鐘逾時時間結束之前，儲存所有快取的變更。

## 自訂今天頁面

相關主題：

- ◆ [今天：自午夜算起的健全度、安全性及數值](#)，第 21 頁
- ◆ [自訂記錄頁面](#)，第 25 頁

使用今天 > 自訂 頁面最多可針對「狀態」>「今天」頁面選擇 4 個圖表。僅具有無條件政策權限的「超級管理員」(包括 WebsenseAdministrator) 可自訂「今天」頁面。

所選圖表會顯示在所有「超級管理員」，以及有權檢視「今天」頁面上的圖表之委派管理員的「今天」頁面上。請參閱[編輯角色](#)，第 221 頁。

有些圖表可能會顯示機密資訊，例如使用者名稱或 IP 位址。請確定所選圖表對於可能檢視它們的所有管理員是恰當的。

要選擇圖表，可標記或清除圖表名稱旁邊的核取方塊。完成標記選擇時，按一下**確定**以返回「今天」頁面並檢視圖表。要返回「今天」頁面但不執行變更，則按一下**取消**。

如需每個圖表所顯示之資訊的簡短說明，請參閱[今天：自午夜算起的健全度、安全性及數值](#)，第 21 頁。

## 記錄：最後 30 天

相關主題：

- ◆ [今天：自午夜算起的健全度、安全性及數值](#)，第 21 頁
- ◆ [瀏覽 Websense Manager](#)，第 19 頁
- ◆ [自訂記錄頁面](#)，第 25 頁

使用**狀態 > 記錄：最後 30 天**頁面可取得過去 30 天之內的篩選行為概覽。該頁面中的圖表會在每天上午 12:01 更新，以將前一天的資料併入，如同記錄資料庫電腦上的時間所決定的。

圖表與摘要表格所涵蓋的確實時段取決於 Websense 軟體已篩選的時間。在安裝 Websense 軟體的第一個月之內，該頁面會顯示從安裝之日至今的天數。第一個月之後，報告會涵蓋今天之前的 30 天。

頁面頂端的**估計值**會提供 Websense 軟體的時間與頻寬節省的估計值，以及封鎖的對類別之要求的摘要，這些類別對於許多組織是很重要的。

將滑鼠放在**時間**或**頻寬**項目(在「已節省」之下)上，就會看見如何計算估計值的解釋(請參閱[節省的時間與頻寬](#)，第 24 頁)。可以按一下**自訂**變更計算數值的方式。

**已封鎖的要求**區域會列出多種與許多組織相關的類別，並顯示在時段內已封鎖的對每個類別之要求的總數，進一步說明 Websense 軟體如何保護網路。

委派管理員可能看不到下列描述的圖表，這取決於授予角色的報告權限。請參閱[編輯角色](#)，第 221 頁。

該頁面最多包括 4 個圖表，並具有反白顯示篩選。可能需要向下捲動才能看到所有圖表。圖表中的資訊每天更新一次。按一下圖表即可啟動調查報告，提供更多詳細資訊。

圖表名稱	說明
依要求的網際網路活動	檢視每天處理到記錄資料庫的已篩選網際網路要求的數量。
依要求排名最高的安全風險	查看哪些「安全風險」類別最近受到存取，並且判斷篩選政策是否為您的網路提供適當的防護。
依要求排名最高的類別	查看存取最多次的類別。取得高階概況，瞭解潛在的安全、頻寬或生產力的疑慮。
排名最高的尚未歸類網站	瞭解有哪些 Websense Master Database 未分類的網站受到最多次存取。移至常用工作 > 重新分類 URL，將網站指派到篩選類別。
依頻寬排名最高的通訊協定	瞭解最近在您的網路中有哪些通訊協定使用了最多頻寬。使用這項資訊評估頻寬需求以及可能的政策變更。
依風險等級政策強制執行	查看最近各個風險等級有多少允許及封鎖的要求（請參閱 <a href="#">風險等級</a> ，第 36 頁）。評估目前的政策是否有效，或者是否需要變更。
封鎖最多次的使用者	查看哪些使用者的網際網路要求最常被封鎖。深入瞭解組織的網際網路使用是否符合規範。
政策強制執行摘要	概略瞭解最近允許的要求、存取「安全風險」等級網站而受到封鎖的要求，以及存取其他網站而受到封鎖的要求。考慮篩選有哪些方面需要更詳細的評估。

頁面上方會出現兩個按鈕：

- ◆ **自訂**，僅供「超級管理員」使用，可開啓一個頁面，能夠在其中變更在頁面上顯示的圖表，以及變更計算評估節省的方法（請參閱 [自訂記錄頁面](#)，第 25 頁）。
- ◆ **列印**，適用於所有管理員，可開啓另一個視窗，其中有「記錄」頁面上顯示之圖表的可列印版本。使用瀏覽器選項來列印此頁面，如此即可不列印出主要 Websense Manager 視窗中的所有瀏覽選項。

## 節省的時間與頻寬

除了 Websense 篩選所提供之改善的安全性以外，它也可以協助將浪費在非生產性網際網路活動的時間與頻寬減到最少。

「估計值」區域的「已節省」區段代表這些時間與頻寬節省的估計值。這些數值的計算方式如下：

- ◆ **節省的時間**：一般每次到訪所用時間乘以已封鎖的網站。一開始，Websense 軟體會使用預設值作為使用者檢視要求之網站所用時間（以秒為單位）的平均數。已封鎖的網站數值代表在「記錄」頁面涵蓋的時間範圍內所封鎖之要求的總數。



- ◆ 節省的頻寬：一般每次到訪所用頻寬乘以已封鎖的網站的數目。一開始，Websense 軟體會使用預設值作為平均網站所使用的位元組的平均數。已封鎖的網站數值代表在「記錄」頁面涵蓋的時間範圍內所封鎖之要求的總數。

如需如何變更這些計算中使用之數值以反映貴組織的使用量的資訊，請參閱 [自訂記錄頁面](#)，第 25 頁。

## 自訂記錄頁面

相關主題：

- ◆ [記錄: 最後 30 天](#)，第 23 頁
- ◆ [自訂今天頁面](#)，第 22 頁

使用 [記錄 > 自訂](#) 頁面可決定要在「狀態」>「記錄」頁面上顯示的圖表，並決定如何計算時間與頻寬節省。

標記要包含在「記錄」頁面中的每個圖表名稱 (最多 4 個) 旁的核取方塊。如需每個圖表的簡短說明，請參閱 [記錄: 最後 30 天](#)，第 23 頁。僅具有無條件政策權限的「超級管理員」(包括 `WebsenseAdministrator`) 可以自訂「記錄」頁面上的圖表。

有些圖表可能會顯示機密資訊，例如使用者名稱。請確定所選圖表對於可能檢視它們的所有管理員是恰當的。

「超級管理員」與委派管理員都可以自訂時間與頻寬節省的計算方式。在說明時間與頻寬節省的計算方式的快顯視窗中，按一下 [自訂](#) 連結，委派管理員即可存取這些欄位。

輸入新的平均時間與頻寬測量用作計算基礎：

選項	說明
每個封鎖網頁的平均節省秒數	輸入貴組織估計使用者檢視單獨網頁時所花費的平均秒數。 Websense 軟體會將這個值乘以封鎖的頁面數，來決定「記錄」頁面中顯示的時間節省。
每個封鎖網頁的平均節省頻寬 [KB]	輸入所檢視之頁面的平均大小 (以 KB 為單位)。 Websense 軟體會將這個值乘以封鎖的頁面數，來決定「記錄」頁面中顯示的頻寬節省。

完成標記變更後，按一下 **確定** 以返回「記錄」頁面並檢視新的圖表或時間與頻寬估計。要返回「記錄」頁面但不執行變更，則按一下 **取消**。

## 您的訂閱

Websense 訂閱以每個用戶端為基礎核發。用戶端就是網路中的使用者或電腦。

購買訂閱時，會透過電子郵件為您提供一個訂閱密碼。每個密碼僅針對一個 Websense Policy Server 的安裝有效。如果安裝多個 Policy Server，則每個 Policy Server 都需要單獨的密碼。

在可以開始篩選之前，必須輸入有效的訂閱密碼 (請參閱 [設定帳戶資訊](#)，第 27 頁)。這樣就可以下載 Master Database (請參閱 [Websense Master Database](#)，第 29 頁)，然後供 Websense 軟體篩選用戶端。

在第一個成功的資料庫下載後，Websense Manager 會顯示訂閱所包括的用戶端數目。

Websense 軟體每天都會維護受篩選之用戶端的訂閱表格。而且會在每天晚上清除訂閱表格。清除表格之後，當用戶端第一次執行網際網路要求時，表格中會輸入該用戶端的 IP 位址。

當表格中所列的用戶端的數量達到訂閱等級時，先前沒有列出的所有要求網際網路存取的用戶端就會超出訂閱。如果發生此情況，超出訂閱等級的用戶端會被完全封鎖而無法存取網際網路，或被授予未篩選的網際網路存取，這取決於您的設定。同樣地，當訂閱到期時，所有用戶端會被完全封鎖或未篩選，這取決於您的設定。

要設定訂閱超出或到期時的篩選行為，請參閱 [設定帳戶資訊](#)，第 27 頁。

要設定 Websense 軟體在訂閱到達或超出其限制時傳送電子郵件警告，請參閱 [設定系統警示](#)，第 249 頁。

受篩選的類別的數量取決於您的 Websense 訂閱。Websense 軟體會篩選所有由訂購啟動之類別中的所有網站。

## 透過 MyWebsense 入口網站管理帳戶

Websense, Inc. 有一個客戶入口網站，位於 [www.mywebsense.com](http://www.mywebsense.com)，可以用它來存取產品更新、修補程式、產品新聞、試用版及 Websense 軟體的技術支援資源。

建立帳戶時，系統會提示您輸入所有的 Websense 訂閱密碼。這有助於確保存取資訊、警示及有關您的 Websense 產品及版本的修補程式。

具有 MyWebsense 帳戶之後，如果因為遺失 Websense Administrator 密碼而無法登入 Websense Manager，只要按一下 Websense Manager 登入頁面上的 **忘記密碼** 即可。系統會提示您登入 MyWebsense，然後指示您產生與啟動新密碼。



### 重要

要求新密碼時，在 MyWebsense 入口網站中選擇的訂閱密碼必須與在 Websense Manager 的「帳戶」頁面上輸入的密碼一致。

貴組織的多個成員可以建立與同一個訂閱密碼相關的 MyWebsense 登入。

要從 Websense Manager 之內存取 MyWebsense 入口網站，請前往 [說明 > MyWebsense](#)。

## 啓動 Websense Web Protection Services™

Websense Web Security 訂閱包括存取 Websense Web Protection Services：SiteWatcher™、BrandWatcher™ 及 ThreatWatcher™。啓動這些服務之後，它們會開始運作以保護貴組織的網站、商標及 Web Server。

服務	說明
SiteWatcher	貴組織的網站被惡意程式碼感染時，此服務會警告您立即採取行動以保護可能造訪網站的客戶、潛在客戶及夥伴。
BrandWatcher	<ul style="list-style-type: none"> <li>貴組織的網站或商標成爲網路釣魚或惡意鍵盤記錄的攻擊目標時，此服務會發出警告。</li> <li>它會提供網際網路安全情報、攻擊詳細資訊及其他與安全有關的資訊，讓您得以採取行動、通知客戶，並將對公共關係的影響降到最小。</li> </ul>
ThreatWatcher	<ul style="list-style-type: none"> <li>提供從駭客角度對貴組織的 Web Server 的觀察、掃描已知弱點及潛在威脅。</li> <li>報告風險等級及透過以網路爲基礎的入口網站提供建議。</li> <li>協助在惡意攻擊發生在您的 Web Server 之前防止它們。</li> </ul>

登入 MyWebsense 入口網站以啓動 Websense Protection Services。啓動 ThreatWatcher 後，登入 MyWebsense 存取已註冊之 Web Server 的威脅報告。

## 設定帳戶資訊

相關主題：

- ◆ [您的訂閱](#)，第 26 頁
- ◆ [設定資料庫下載](#)，第 30 頁
- ◆ [使用通訊協定](#)，第 160 頁

使用 **設定 > 帳戶** 頁面可輸入及檢視訂閱資訊，以及變更新來存取 Websense Manager 的 WebsenseAdministrator 密碼。WebsenseAdministrator 是預設的主管理帳戶，用來管理 Websense 軟體。

也可以在此頁面啓用 Websense 軟體，以將通訊協定使用資料以匿名方式傳送至 Websense, Inc.。此資訊可能用來更新 Websense Master Database，Websense Master Database 收集了超過 3600 萬個網際網路網站及 100 個以上的通訊協定定義（如需詳細資訊，請參閱 [Websense Master Database](#)，第 29 頁）。

- 在安裝 Websense 軟體之後，或在任何時刻收到新的訂閱密碼時，請使用 **訂閱密碼** 欄位來輸入密碼。  
輸入新的訂閱密碼並按一下「確定」之後，會自動下載 Master Database。

2. 下載第一個 Master Database 之後，會顯示下列資訊：

密碼到期	目前訂閱的結束日期。在此日期之後，必須更新訂閱才能繼續下載 Master Database 及篩選網路。
已訂閱的網路使用者	可篩選的網路內使用者的數目。
已訂閱的遠端使用者	網路之外可篩選的使用者的數目 (需要選用的 Remote Filtering 功能)。

3. 選擇**訂閱到期或超出時封鎖使用者**以便：

- 當訂閱到期時封鎖所有使用者的網際網路存取。
- 當使用者超出已訂閱使用者的數目時，封鎖那些使用者的所有網際網路存取。

如果未選擇此選項，當這些情況發生時，使用者可以獲得未篩選的網際網路存取。

4. 若要變更 WebsenseAdministrator 密碼，請先提供目前的密碼，然後輸入並確認新密碼。
- 密碼長度必須為 4 至 25 個字元。密碼區分大小寫，而且可以包含字母、數字、特殊字元及空格。
  - 強烈建議為 WebsenseAdministrator 帳戶建立強式密碼。密碼應該至少包含 8 個字元，並且至少包含一個大寫字母、小寫字母、數字及特殊字元。
5. 標記**傳送類別與通訊協定資料到 Websense, Inc.** 可讓 Websense 軟體收集有關 Websense 定義之類別與通訊協定的使用資料，並將資料以匿名方式提交到 Websense, Inc.。

此使用資料可協助 Websense, Inc. 不斷加強 Websense 軟體的篩選功能。

## Websense Master Database

相關主題：

- ◆ [即時資料庫更新](#)，第 29 頁
- ◆ [即時安全性更新™](#)，第 30 頁
- ◆ [篩選類別和通訊協定](#)，第 34 頁
- ◆ [使用 Filtering Service](#)，第 242 頁
- ◆ [檢閱 Master Database 下載狀態](#)，第 243 頁
- ◆ [可繼續的 Master Database 下載](#)，第 244 頁

Websense Master Database 儲存了用來提供篩選網際網路內容之基礎的類別及通訊協定定義 (請參閱[篩選類別和通訊協定](#)，第 34 頁)。

- ◆ **類別**用來根據相似內容對網站分組 (依照 URL 與 IP 位址來識別)。
- ◆ **通訊協定**定義會將相似用途 (例如傳送檔案或傳送即時訊息) 的網際網路通訊協定分組。

在 Websense 軟體安裝期間，會安裝限制版本的篩選資料庫，但是建議儘速下載完整的 Master Database，以啓用完整的網際網路篩選功能。若是第一次下載 Master Database，請在**設定 > 帳戶**頁面上輸入您的訂閱密碼 (請參閱[設定帳戶資訊](#)，第 27 頁)。

如果 Websense 軟體必須透過代理伺服器才能執行下載，也請使用**設定 > 資料庫下載**頁面來設定代理伺服器設定 (請參閱[設定資料庫下載](#)，第 30 頁)。

下載完整資料庫可能需要幾分鐘到 60 分鐘以上，這取決於多種因素，例如網際網路連線速度、頻寬、可用記憶體及可用磁碟空間。

在第一次下載之後，Websense 軟體會根據您建立的排程來下載資料庫變更 (請參閱[設定資料庫下載](#)，第 30 頁)。由於 Master Database 會經常更新，因此在預設情況下，排程會每天下載資料庫。

如果超過 14 天沒有下載 Master Database，則 Websense 軟體將不會篩選網際網路要求。

要在任何時候啓動資料庫下載，或檢視最後一次資料庫下載的狀態、最後一次下載的日期或目前的資料庫版本編號，請前往**狀態 > 今天**，並按一下**資料庫下載**。

## 即時資料庫更新

除了已排程的下載，Websense 軟體還會視需要對資料庫執行緊急更新。例如，即時更新可能會用來將暫時分類錯誤的網站重新分類。這些更新可確保網站與通訊協定都經過適當篩選。

Websense 軟體每小時都會檢查資料庫更新。

最新的更新會列在**狀態 > 警示**頁面上 (請參閱[檢閱目前的系統狀態](#)，第 252 頁)。

## 即時安全性更新™

除了接收標準的即時資料庫更新，Websense Web Security 使用者也可以啓用「即時安全性更新」在 Websense, Inc. 發佈 Master Database 的安全相關的更新時，立即接收更新。

「即時安全性更新」可提供新增的保護層級，防止網際網路式的安全威脅。在這些更新發佈後儘速安裝它們，有助於降低下列弱點造成的威脅：新型網路釣魚(身份詐欺)詐騙、流氓應用程式及感染主要網站或應用程式的惡意程式碼。

Filtering Service 每隔 5 分鐘就會檢查安全性更新，但是只有在發生安全威脅時才會傳送更新，因此實際上更新並非是經常性的，不過更新會盡可能不中斷一般網路活動。

使用 [設定 > 資料庫下載](#) 頁面可啓用「即時安全性更新」(請參閱 [設定資料庫下載](#)，第 30 頁)。

## 設定資料庫下載

相關主題：

- ◆ [設定帳戶資訊](#)，第 27 頁
- ◆ [Websense Master Database](#)，第 29 頁
- ◆ [檢閱 Master Database 下載狀態](#)，第 243 頁

使用 [設定 > 資料庫下載](#) 頁面可建立自動下載 Master Database 的排程。此外，該頁面也提供了關於 Websense 軟體為下載資料庫而必須通過的代理伺服器或防火牆的重要資訊。

1. 選擇 **下載日** 以進行自動下載。

必須至少每隔 14 天下載一次 Master Database，Websense 軟體才能持續不斷地進行篩選。如果取消選擇所有下載日，Websense 軟體會在下載資料庫 7 天後自動嘗試下載。



### 注意

啓用「即時安全性更新」時，則會停用下載日(請參閱 [步驟 3](#))。這樣每天都會自動執行下載，以確保安全性更新可獲得最新的標準資料庫。

2. 為 **下載時間範圍** 選擇開始時間 (**從**) 與結束時間 (**到**)。如果沒有選擇時間，則會在 21:00 (9pm) 與 06:00 (6am) 之間執行資料庫下載。

Websense 軟體會在這段時間內隨機選擇時間以聯絡 Master Database 伺服器。要設定下載失敗的警示，請參閱[設定系統警示](#)，第 249 頁。



#### 注意

下載或更新 Master Database 後，由於資料庫會載入本機記憶體，因此 CPU 使用量可能高達 90%。

3. (Websense Web Security) 選擇**啟動即時安全性更新**可讓 Websense 軟體每 5 分鐘檢查一次 Master Database 的安全性更新。偵測到安全性更新時會立即下載。

「即時安全性更新」可快速保護網路，使其免受下列弱點的威脅：新型網路釣魚 (身份詐欺) 詐騙、流氓應用程式及感染主要網站或應用程式的惡意程式碼。

4. 如果 Websense 軟體必須透過代理伺服器或代理防火牆 (並非與 Websense 軟體通訊的整合產品) 才能存取網際網路，則選擇**使用代理伺服器或防火牆**以便下載 Master Database。然後設定下列各項：

伺服器 IP 或名稱	輸入代理伺服器或防火牆所在電腦的 IP 位址或名稱。
連接埠	輸入資料庫下載必須通過的連接埠號碼 (預設為 8080)。

5. 如果步驟 4 中設定的代理伺服器或防火牆需要驗證才能連線網際網路，那麼選擇**使用驗證**，然後輸入 Websense 軟體用來獲得網際網路存取的使用者名稱和密碼。



#### 注意

如果已選擇「使用驗證」，則必須將代理伺服器或防火牆設定為接受純文字或基本驗證，以便啟用 Master Database 下載。

預設會將使用者名稱和密碼予以編碼，以便符合 Policy Server 電腦的地區設定的字元集。這個編碼程序可以透過[設定 > 目錄服務](#)頁面來手動設定 (請參閱[進階目錄設定](#)，第 59 頁)。

## 測試網路配置

為了執行網際網路要求篩選，Websense 軟體必須知道進出您網路中的電腦的網際網路流量。使用「網路流量偵測器」來確保篩選軟體可以看到這個網際網路通訊。如需指示，請參閱[驗證 Network Agent 配置](#)，第 301 頁。

如果「流量偵測器」無法查看網路中的所有區段，請參閱[網路配置](#)，第 293 頁以取得配置指示。

## Websense 技術支援

---

Websense, Inc. 致力於使客戶滿意。隨時可以前往 Websense 技術支援網站取得最新版本資訊，從而存取知識庫或產品文件，或提出支援要求。

[www.websense.com/SupportPortal/](http://www.websense.com/SupportPortal/)

在上班時間提出線上要求的回應時間約為 4 小時。對於在下班時間提出的要求，會在下一個工作日回應。

也可以使用電話協助。如需透過電話要求取得快速且有效的解答，請準備好下列各項：

- ◆ Websense 訂閱密碼
- ◆ 存取 Websense Manager
- ◆ 存取執行 Filtering Service 與 Log Server 的電腦，以及資料庫伺服器 (Microsoft SQL Server 或 MSDE)
- ◆ 存取 Websense 記錄資料庫的權限
- ◆ 熟悉您的網路架構，或找到具有此知識的人
- ◆ 執行 Filtering Service 與 Websense Manager 的電腦規格
- ◆ 在 Filtering Service 電腦上執行的其他應用程式的清單

對於嚴重的問題，可能需要其他資訊。

週一至週五正常上班時間可以使用標準電話協助，電話號碼如下：

- ◆ 美國加州聖地牙哥：**+1 858.458.2940**
- ◆ 英國倫敦：**+44 (0) 1932 796244**

請查看上述的支援網站以了解辦公時間及其他支援選項。

日本的客戶如需最快速服務，請聯絡經銷商。



# 2

## 網際網路使用量篩選器

### 相關主題

- ◆ [篩選類別和通訊協定](#)，第 34 頁
- ◆ [使用篩選器](#)，第 42 頁
- ◆ [設定 Websense 篩選設定](#)，第 49 頁
- ◆ [網際網路篩選政策](#)，第 65 頁
- ◆ [優化篩選政策](#)，第 145 頁

政策控管使用者的網際網路存取。政策是一種排程它告知 Websense 軟體篩選網站和網際網路應用程式之存取的方式與時間。最簡單的政策由下列幾項組成：

- ◆ **類別篩選器**用於將動作 (允許、封鎖) 套用至網站類別
- ◆ **通訊協定篩選器**用於將動作套用至網際網路應用程式和非 HTTP 通訊協定
- ◆ 決定強制執行每個篩選器的時間的排程

以政策為基礎的篩選可讓您將不同層級的網際網路存取指派給用戶端 (網路中的使用者、群組和電腦)。首先，建立篩選器來定義精確的網際網路存取限制，然後使用篩選器來建構政策。

在首次安裝時，Websense 軟體會建立**預設**政策，並在輸入訂閱密碼後立即用它來開始監控網際網路要求 (請參閱 [預設政策](#)，第 66 頁)。「預設」政策最初會允許所有要求。



### 注意

如果從舊版 Websense 軟體升級，則會保留現有的政策設定。請在升級後檢閱政策以確認它們仍然適用。

若要將不同的篩選限制套用至不同用戶端，請從定義類別篩選器開始。可能需要定義的內容是：

- ◆ 一個類別篩選器，用於封鎖對所有網站的存取，但「商業與經濟」、「教育」和「新聞媒體」類別中的網站除外
- ◆ 第二個類別篩選器用於允許所有網站但具有安全風險及包含成人資訊的網站除外

- ◆ 第三個類別篩選器用於監控對網站的存取但是不會封鎖網站 (請參閱 [建立類別篩選器](#), 第 43 頁)

在定義這些類別篩選器時可能還需要定義如下內容：

- ◆ 一個通訊協定篩選器用於封鎖對「即時訊息傳送與聊天」、「P2P 檔案共用」、「以 Proxy 規避封鎖」和「串流媒體」等通訊協定群組的存取
- ◆ 第二個通訊協定篩選器用於允許所有非 HTTP 通訊協定，但與以 Proxy 規避封鎖相關的通訊協定除外
- ◆ 第三個通訊協定篩選器用於允許所有非 HTTP 通訊協定 (請參閱 [建立通訊協定篩選器](#), 第 45 頁)

完成定義符合貴組織之網際網路存取規範的一組篩選器後，您便可將它們新增至政策，以及套用至用戶端 (請參閱 [網際網路篩選政策](#), 第 65 頁)。

## 篩選類別和通訊協定

Websense Master Database 會將類似網站 (透過 URL 和 IP 位址識別) 組織到**類別**中。每個類別都有一個描述性名稱，例如「成人資訊」、「賭博」或「端對端檔案共用」。您也可以建立自己的自訂類別，以便分組與貴組織有特別關係的網站 (請參閱 [建立自訂類別](#), 第 154 頁)。Master Database 類別和使用者定義的類別共同構成網際網路篩選的基礎。

Websense, Inc. 不對 Master Database 中的類別或網站進行價值判斷。類別旨在為與訂閱客戶相關的網站建立有用的群組。它們並非用來辨識任何網站或網站群組，或是發佈這些網站的人員或利益團體，且不應被理解為如此。同樣地，附加至 Websense 類別的標籤只是方便的速記，並非用來對如此分類之主題或網站表達任何意見或態度、核准或其他情況，也不應將其理解為如此。

Master Database 類別的最新清單可從以下網址取得：

[www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php](http://www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php)

要建議將某個網站新增至 Master Database 請按一下 Websense Manager 右側捷徑窗格中的**建議新類別**或造訪：

[www.websense.com/SupportPortal/SiteLookup.aspx](http://www.websense.com/SupportPortal/SiteLookup.aspx)

登入 MyWebsense 入口網站後系統會將您引導至「Site Lookup and Category Suggestion (網站查閱和類別建議)」工具。

在 Websense Manager 中建立**類別篩選器**時，需要選擇要封鎖及允許哪些類別。

除了保存 URL 類別外，Websense Master Database 還包含用於管理非 HTTP 網際網路流量的通訊協定群組。每個通訊協定群組定義了相似類型的網際網路通訊協定 (如 FTP 或 IRC) 和應用程式 (如 AOL Instant Messenger 或 BitTorrent)。這些定義最快會每晚確認並更新一次。

與類別一樣，您可以定義用於網際網路篩選的自訂通訊協定。

Master Database 通訊協定的最新清單可從以下網址取得：

[www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php](http://www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php)

建立**通訊協定篩選器**時需要選擇要封鎖及允許哪些通訊協定。



#### 注意

您必須安裝 Network Agent 才能啓用以通訊協定為基礎的篩選。

某些 Websense 定義的通訊協定允許封鎖以外部伺服器 (例如特定的即時訊息傳送伺服器) 為目的地的出站網際網路流量。只有具有動態指派之連接埠號碼，而且由 Websense 定義的通訊協定，才能作為出站流量封鎖。

### 新類別和通訊協定

將新類別和通訊協定新增至 Master Database 時會分別為其指派預設篩選動作例如**允許**或**封鎖** (請參閱 [篩選動作](#)，第 39 頁)。

- ◆ 預設動作會套用至所有已啓用的類別和通訊協定篩選器 (請參閱 [使用篩選器](#)，第 42 頁)。編輯已啓用的篩選器可變更類別或通訊協定的篩選方式。
- ◆ 預設動作以特定的意見反應為基礎，這些意見反應涉及有疑問的網站或通訊協定是否普遍被視為具商業適宜性。

您可以設定 Websense 軟體來產生系統警示，並在每當有新的類別或通訊協定新增至 Master Database 時通知您。如需詳細資訊，請參閱 [警示](#)，第 246 頁。

## 特殊類別

Master Database 包含一些特殊類別有助於管理特定類型的網際網路使用量。下列類別可在所有 Websense 軟體版本中使用：

- ◆ **特殊事件**類別用於分類被視為熱門主題的網站有助於管理網際網路流量中與事件相關的瞬增流量。例如，官方世界盃網站通常會顯示在「體育運動」類別中，不過在世界盃決賽期間會移至「特殊事件」類別。  
「特殊事件」類別的更新會在已排程的下載期間新增至 Master Database。網站會在短時間內新增至此類別，之後它們會被移至其他類別或從 Master Database 中刪除。
- ◆ **生產力**類別著重在預防費時的行為。
  - 廣告
  - 免費軟體，軟體下載
  - 即時訊息傳送
  - 線上經紀與交易
  - 上網式賺錢

- ◆ **頻寬**類別著重在節省網路頻寬。
  - 網際網路廣播與電視
  - 網際網路電話
  - 端對端檔案共用
  - 個人網路儲存，備份
  - 串流媒體

Websense Web Security 包含其他安全性類別：

- ◆ **Websense 安全性篩選** (也簡稱為**安全性**) 著重在包含可略過病毒偵測軟體程式之惡意程式碼的網站。預設會封鎖此類別中的網站。
  - 遠端監控程式網路
  - 鍵盤側錄
  - 惡意網站
  - 網路釣魚
  - 潛在惡意軟體
  - 間諜軟體
- ◆ **延伸的防護**著重在潛在的惡意網站。預設會封鎖「高風險的漏洞」和「新興的探測」下層類別中的網站。
  - **高風險的漏洞**包含偽裝其真實本質或身份識別的網站，或是包含潛藏有害意圖之元素的網站。
  - **新興的探測**保存已發現的會裝載已知的潛在入侵程式碼之網站。
  - **潛在有害的內容**包含可能只具有少許 (或完全沒有) 有用內容的網站。

「延伸的防護」群組會根據信譽來篩選潛在的惡意網站。網站信譽取決於潛在的惡意活動的早期徵兆。例如，攻擊者可能會以包含常見拼字錯誤的 URL 或類似合法 URL 的 URL 為目標。這類網站可用來在更新傳統篩選器以反映這些網站具有惡意前，將惡意軟體散佈給使用者。

Websense 安全性研究偵測到潛在的威脅時，會先將它加入「延伸的防護」類別，直到 Websense 百分之百確定該網站的最後分類為止。

## 風險等級

相關主題：

- ◆ [將類別指派到風險等級](#)，第 264 頁
- ◆ [簡報報告](#)，第 86 頁
- ◆ [調查報告](#)，第 102 頁

Websense Master Database 會依據**風險等級**將類別分組。風險等級指出類別群組中的網站可能引發之弱點的類型或層級。

風險等級主要用於報告。「今天」和「記錄」頁面包含會按照風險等級顯示網際網路活動的圖，且可產生根據風險等級來組織的簡報或調查報告。

風險等級可能也有助於建立類別篩選器。例如，一開始「基本安全性」類別篩選器會封鎖「安全風險」等級中的所有預設類別。建立自己的類別篩選器時，可以使用風險等級群組做為指導，以協助決定是否應該允許、封鎖、或以某些方式限制某個類別。

Websense 軟體包含 5 個風險等級，列示如下。根據預設，Websense 軟體會將下列類別分組到各個風險等級中。

- ◆ 某個類別可能出現在多個風險等級中，或沒有被指派至任何風險等級。
- ◆ 您可在 Master Database 中定期變更群組。

### 法律責任

成人資訊 (包括「成人內容」、「女仕內衣與泳裝」、「裸體」和「性」)

頻寬 > 端對端檔案共用

賭博

違法或嫌疑行為

資訊科技 > 駭客入侵與以 Proxy 規避封鎖

暴力衝突，極端主義

種族歧視

惡俗

暴力

武器

### 網路頻寬損失

頻寬 (包括「網際網路廣播與電視」、「網際網路電話」、「端對端檔案共用」、「個人網路儲存，備份」和「串流媒體」)

娛樂 > MP3 與音效下載服務

生產力 > 廣告以及免費軟體與軟體下載

### 商業使用量

商業與經濟 (包括「金融資料與服務」)

教育 > 教學資源以及參考材料

政府 (包括「軍事」)

資訊科技 (包括「電腦安全」、「搜尋引擎與入口網站」和「URL 轉換網站」)

旅行

交通工具

## 安全風險

頻寬 > 端對端檔案共用

延伸的防護 (包括「高風險的漏洞」、「新興的探測」和「潛在有害的內容」) [*Websense Web Security*]

資訊科技 > 駭客入侵與以 Proxy 規避封鎖

生產力 > 免費軟體，軟體下載

安全 (包括「遠端監控程式網路」、「鍵盤側錄」、「惡意網站」、「網路釣魚」、「潛在惡意軟體」和「間諜軟體」)

## 生產力損失

墮胎 (包括「母親決定權」與「胎兒生存權」)

成人資訊 > 性教育

倡議團體

頻寬 > 網際網路廣播與電視、端對端檔案共用以及串流媒體

藥物 (包括「濫用藥物」、「大麻」、「處方藥」以及「補充藥物/非規製合成藥物」)

教育 (包括「文化機構」與「教育機構」)

娛樂 (包括 MP3 與音效下載服務)

賭博

遊戲

政府 > 政治團體

健全度

資訊科技 > 網站代管

網際網路通訊 (包括「一般 Email」、「組織 Email」、「文字和媒體傳訊」和「網上聊天」)

求職

新聞媒體 (包括「可選期刊」)

生產力 (包括「免費軟體，軟體下載」、「即時訊息傳送」、「留言板與論壇」、「線上經紀與交易」和「上網式賺錢」)

宗教 (包括「非傳統宗教、秘術與民間傳說」與「傳統宗教」)

購物 (包括「網上拍賣」與「房地產」)

社會組織 (包括「職業與工人組織」、「服務與慈善組織」以及「社會與附屬組織」)

社會與生活時尚 (包括「煙酒」、「同性戀，雙性戀」、「嗜好」、「個人/約會」、「餐飲」以及「社交網路和個人網站」)

特殊事件

體育運動 (包括「狩獵運動，射擊俱樂部」)

旅行

交通工具

「超級管理員」可以在**設定 > 風險等級**頁面上，變更指派至各個風險等級的類別 (請參閱 [將類別指派到風險等級](#)，第 264 頁)。

## 安全性通訊協定群組

除了「安全性」和「延伸的防護」類別外 Websense Web Security 還包含另外兩個通訊協定，用於協助偵測及防範間諜軟體和惡意程式碼，或是透過網際網路傳輸的內容。

- ◆ **惡意流量**通訊協定群組包含**遠端監控程式網路**通訊協定，其目標是封鎖 Bot 爲了嘗試與 Botnet 連線以遂行惡意目的而產生的命令與控制流量。
- ◆ **惡意流量 – 僅監控**通訊協定群組用於識別可能與惡意軟體相關的流量。
  - **郵件自動產生蠕蟲**會追蹤可能由以電子郵件爲基礎的蠕蟲攻擊所產生的出站 SMTP 流量。
  - **其他惡意流量**會追蹤疑似與惡意應用程式相關的入站和出站流量。

預設會封鎖「惡意流量」通訊協定群組，而且可在通訊協定篩選器中設定此群組（請參閱[編輯通訊協定篩選器](#)，第 46 頁）。可記錄「惡意流量 – 僅監控」通訊群組以產生報告，但無法套用任何其他篩選動作。

## Instant Messaging Attachment Manager

Instant Messaging (IM) Attachment Manager 是選用功能。如果訂閱此功能，便可限制與 AOL/ICQ、Microsoft (MSN) 和 Yahoo 等 IM 用戶端的檔案共用。這樣就可以允許 IM 流量，同時封鎖 IM 用戶端的附件傳送。

即時訊息傳送檔案附件是包含多個 IM 用戶端之定義的通訊協定群組。啓用 IM Attachment Manager 時，這些通訊協定會顯示在所有已啓用之通訊協定篩選器內的通訊協定清單中，以及「編輯通訊協定」頁面上。

IM 附件篩選可同時套用至內部和外部流量。要啓用內部流量篩選，請在**設定 > Network Agent > 全域**頁面上，定義要監控的網路部份（請參閱[設定全域設定](#)，第 296 頁）。

## 篩選動作

類別和通訊協定篩選器會指派一個**動作**給每個類別或通訊協定。這是 Websense 篩選軟體在回應用戶端的網際網路要求時所採取的動作。套用至類別和通訊協定的動作包括：

- ◆ **封鎖**要求。使用者會收到封鎖頁面或封鎖訊息，且無法檢視網站或使用網際網路應用程式。
- ◆ **允許**要求。使用者可以檢視網站或使用網際網路應用程式。
- ◆ 在封鎖或允許要求之前，評估目前的**頻寬**使用量。啓用此動作且頻寬使用量達到指定的臨界值時，會封鎖特定類別或通訊協定更進一步的網際網路要求。請參閱[使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁。

其他動作只能套用至類別。



#### 注意

當個別用戶端(使用者、群組和電腦)由多個 Policy Server 管理時，就不應使用「確認」和「配額」選項。

與這些功能相關的時間資訊不會在 Policy Server 之間共用，且授予受影響用戶端的網際網路存取可能比預期的更多或更少。

- ◆ **確認** – 使用者會收到封鎖頁面，要求他們確認是否基於商業目的存取該網站。使用者按一下**繼續**便可檢視該網站。  
按一下「繼續」會啟動計時器。在設定的時段內(預設為 60 秒)，使用者可造訪「確認」類別中的其他網站，而不會再收到其他封鎖頁面。該時段結束後，瀏覽任何其他「確認」網站會產生其他封鎖頁面。  
您可在**設定 > 篩選**頁面上變更預設時間。
- ◆ **配額** – 使用者會收到封鎖頁面，詢問他們是否要使用配額時間來檢視網站。使用者按一下**使用配額時間**便可檢視該網站。  
按一下「使用配額時間」會啟動兩個計時器 配額工作階段計時器和總配額配置計時器。
  - 如果使用者在預設**工作階段**期間(預設為 10 分鐘)內要求其他配額網站，便可造訪這些網站而不會收到其他封鎖頁面。
  - **總配額**時間是以每日為基礎來配置。一旦時間用盡，每個用戶端都必須等到次日才能存取配額類別中的網站。在**設定 > 篩選**頁面上設定預設的每日配額配置(預設為 60 分鐘)。也可將每日配額配置個別授予用戶端。如需詳細資訊，請參閱[使用配額時間來限制網際網路存取](#)，第 40 頁。
- ◆ **封鎖關鍵字** – 定義關鍵字並啟用關鍵字封鎖時，如果使用者要求的網站 URL 中包含已封鎖的關鍵字，則不允許存取該網站。請參閱[根據關鍵字篩選](#)，第 156 頁。
- ◆ **封鎖檔案類型** – 啟用檔案類型封鎖時，如果使用者嘗試下載類型遭封鎖的檔案，則會收到封鎖頁面，且不會下載該檔案。請參閱[根據檔案類型管理流量](#)，第 168 頁。

## 使用配額時間來限制網際網路存取

使用者按一下「使用配額時間」後，便可在配額工作階段結束前檢視任何配額類別中的網站。預設配額工作階段時間(透過**設定 > 篩選**頁面來設定)為 10 分鐘。



#### 注意

個別用戶端由多個 Policy Server 管理時，就不應使用「配額」選項。

與此功能相關的時間資訊不會在 Policy Server 之間共用，且授予受影響用戶端的網際網路存取可能比預期的更多或更少。



一旦配額工作階段結束，對配額網站的要求便會產生另一個配額封鎖訊息。尚未用盡其每日配額配置的使用者可以啟動新的配額工作階段。

設定配額時間後，當使用者要求配額類別中的網站時，Websense 軟體會使用優先順序清單來決定如何回應。該軟體會尋找為下列對象所設定的配額時間：

1. 使用者
2. 電腦或網路用戶端
3. 使用者所屬的群組

如果使用者是多個群組的成員 Websense 軟體會根據**設定 > 篩選**頁面上的**使用更為嚴格的封鎖**設定來授予配額時間（請參閱**設定 Websense 篩選設定**，第 49 頁）。

4. 預設配額時間

網際網路 Applet (例如 Java 或 Flash Applet) 可能不會如預期般回應配額時間限制。即使是從配額受限的網站存取 Applet，在瀏覽器中執行的 Applet 仍可在超過設定的配額工作階段時間後繼續執行。

這是因為這類 Applet 已完全下載至用戶端電腦，並且就像應用程式一樣執行，而不需要再與原始主機伺服器通訊。不過，如果使用者按一下瀏覽器的「重新整理」按鈕，Websense 軟體便會偵測到與主機伺服器的通訊，然後根據適用的配額限制來封鎖要求。

## 密碼覆寫

密碼覆寫可讓具有有效密碼的使用者存取被 Websense 軟體封鎖的網站。您可將密碼覆寫授予個別用戶端 (使用者、群組、電腦或網路)。

啟用密碼覆寫選項時 Websense 封鎖訊息會包含密碼欄位。輸入有效密碼的用戶端可在有限的時間內存取已封鎖的網站。



### 注意

個別用戶端由多個 Policy Server 管理時，就不應使用密碼覆寫選項。

與此功能相關的時間資訊不會在 Policy Server 之間共用，且授予受影響用戶端的網際網路存取可能比預期的更多或更少。

密碼覆寫選項透過**設定 > 篩選**頁面啟用 (請參閱**設定 Websense 篩選設定**，第 49 頁)。

可透過**政策管理 > 用戶端**頁面將密碼覆寫權限授予特定用戶端 (請參閱**新增用戶端**，第 61 頁或**變更用戶端設定**，第 62 頁)。

## 搜尋篩選

「搜尋篩選」是某些搜尋引擎所提供的功能，可協助限制顯示給使用者的不當搜尋結果的數目。

通常情況下，網際網路搜尋引擎的結果中可能包含與符合搜尋條件之網站相關的縮圖影像。如果這些縮圖與已封鎖的網站相關，Websense 軟體會防止使用者存取完整網站，不過不會阻止搜尋引擎顯示影像。

啟用「搜尋篩選」時，Websense 軟體會啟動搜尋引擎功能，以阻止在搜尋結果中顯示與已封鎖之網站相關的縮圖影像。啟用「搜尋篩選」會同時影響本機和遠端篩選用戶端。

Websense, Inc. 維護了一份具有「搜尋篩選」功能的搜尋引擎的資料庫。在該資料庫中新增或移除搜尋引擎時會產生警示 (請參閱 [警示](#)，第 246 頁)。

「搜尋篩選」透過 [設定 > 篩選](#) 頁面啟動。如需詳細資訊，請參閱 [設定 Websense 篩選設定](#)，第 49 頁。

## 使用篩選器

相關主題：

- ◆ [篩選類別和通訊協定](#)，第 34 頁
- ◆ [網際網路篩選政策](#)，第 65 頁
- ◆ [建立類別篩選器](#)，第 43 頁
- ◆ [建立通訊協定篩選器](#)，第 45 頁
- ◆ [建立限制存取篩選器](#)，第 147 頁

使用 Websense Manager 中的 [政策管理 > 篩選器](#) 頁面來檢視、建立及修改類別和通訊協定篩選器，以及使用其他篩選工具。

「篩選器」頁面分為 3 個主要區段：

- ◆ **類別篩選器** 決定要封鎖及允許哪些類別。
- ◆ **通訊協定篩選器** 決定要封鎖及允許哪些非 HTTP 通訊協定。  
您必須安裝 Network Agent 才能啓用以通訊協定為基礎的篩選。
- ◆ **限制存取篩選器** 定義已允許網站的限制清單 (請參閱 [將使用者限制於定義的網際網路網站清單](#)，第 145 頁)。

類別、通訊協定和限制存取篩選器構成 **政策** 的組成要素。每個政策由至少一個類別 (或限制存取篩選器) 以及一個通訊協定篩選器組成，並按照特定排程套用至選取的用戶端。

- ◆ 要檢閱或編輯現有類別、通訊協定或限制存取篩選器，請按一下篩選器名稱。如需詳細資訊，請參閱：
  - [編輯類別篩選器](#)，第 44 頁
  - [編輯通訊協定篩選器](#)，第 46 頁
  - [編輯限制存取篩選器](#)，第 148 頁
- ◆ 要建立新的類別、通訊協定或限制存取篩選器，請按一下**新增**。如需詳細資訊，請參閱：
  - [建立類別篩選器](#)，第 43 頁
  - [建立通訊協定篩選器](#)，第 45 頁
  - [建立限制存取篩選器](#)，第 147 頁

要複製現有篩選器，請標記篩選器名稱旁的核取方塊，然後按一下**複製**。複本會以原始篩選器名稱加上號碼來唯一命名，然後新增至篩選器清單。可按照編輯任何其他篩選器的方式來編輯該複本。

如果已建立委派管理角色 (請參閱 [委派管理](#)，第 205 頁)「超級管理員」可將其所建立的篩選器複製到其他角色，以供委派管理員使用。

要將篩選器複製到其他角色，首先請標記篩選器名稱旁的核取方塊，然後按一下**複製到角色**。如需詳細資訊，請參閱 [將篩選器和政策複製到角色](#)，第 149 頁。

## 建立類別篩選器

相關主題：

- ◆ [使用篩選器](#)，第 42 頁
- ◆ [編輯類別篩選器](#)，第 44 頁

可使用**政策管理 > 篩選器 > 新增類別篩選器**頁面建立新的類別篩選器。可以使用預先定義的範本，或製作現有類別篩選器的複本，以用作新篩選器的基礎。

1. 輸入唯一的**篩選器名稱**。名稱長度必須介於 1 到 50 個字元之間，且不能包含下列任何字元：
 

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

篩選器名稱可包含空格、橫線和單引號。
2. 輸入篩選器的簡短**說明**。此說明會顯示在「篩選器」頁面之「類別篩選器」區段中的篩選器名稱旁，且應說明篩選器的目的。
 

適用於篩選器名稱的字元限制也適用於說明，但有 2 個例外：說明可包含句點 (.) 和逗號 (,)。
3. 從下拉式清單中選取項目，以決定是否要使用範本或製作現有篩選器的複本。如需範本的詳細資訊，請參閱 [類別和通訊協定篩選器範本](#)，第 48 頁。
4. 若要查看及編輯新篩選器，請按一下**確定**。篩選器會新增至「篩選器」頁面上的**類別篩選器**清單中。

要自訂篩選器，請按一下篩選器名稱，然後繼續[編輯類別篩選器](#)。

## 編輯類別篩選器

相關主題：

- ◆ [篩選類別和通訊協定](#)，第 34 頁
- ◆ [篩選動作](#)，第 39 頁
- ◆ [使用配額時間來限制網際網路存取](#)，第 40 頁
- ◆ [密碼覆寫](#)，第 41 頁
- ◆ [使用篩選器](#)，第 42 頁
- ◆ [使用類別](#)，第 152 頁

可使用[政策管理](#) > [篩選器](#) > [編輯類別篩選器](#) 頁面變更現有類別篩選器。



### 重要

編輯類別篩選器時，所做的變更會影響強制執行篩選器的每個政策。

強制執行其他委派管理角色中名稱相同之類別篩選器的政策則不受影響。

篩選器名稱和說明顯示在頁面頂端。

- ◆ 按一下**重新命名**可變更篩選器名稱。
- ◆ 只要在**說明**欄位中鍵入相關內容即可變更篩選器說明。

使用此篩選器的政策旁的數字顯示有多少政策目前使用選取的篩選器。如果已啟用類別篩選器，按一下**檢視政策**可取得強制執行篩選器的政策的清單。

頁面底部會顯示類別清單，以及目前套用至每個類別的動作。

1. 選取**類別**清單中的項目以檢視類別資訊，或變更與所選類別相關的篩選動作。
2. 在變更套用至類別的動作前，可使用**類別細節**區段來檢閱與該類別相關的任何特殊屬性。
  - 要檢閱指派給類別的已重新分類或未篩選 URL (如果有)，請按一下**查看此類別中的自訂 URL**。請參閱[重新定義特定網站的篩選](#)，第 158 頁。
  - 要檢閱指派給類別的關鍵字，請按一下**查看此類別中的關鍵字**。請參閱[根據關鍵字篩選](#)，第 156 頁。
  - 要檢閱用來為類別定義自訂 URL 或關鍵字的正規表示式，請按一下**查看此類別中的正規表示式**。
3. 可使用類別清單底部的按鈕變更套用至所選類別的動作。如需可用動作的詳細資訊，請參閱[篩選動作](#)，第 39 頁。

委派管理員無法變更與由「超級管理員」鎖定的類別相關的動作。如需詳細資訊，請參閱[定義所有角色的篩選限制](#)，第 229 頁。

4. 可使用「類別」清單右邊的核取方塊將進階篩選動作套用至選取的類別：
  - 要變更使用關鍵字來篩選所選類別的方式，請標記或清除**封鎖關鍵字**。請參閱[根據關鍵字篩選](#)，第 156 頁。
  - 要決定使用者是否能從所選類別中的網站存取特定類型的檔案，請標記或清除**封鎖檔案類型**。請參閱[根據檔案類型管理流量](#)，第 168 頁。  
如果已選擇封鎖檔案類型，請選取一個或多個要封鎖的檔案類型。
  - 要指定是否根據特定頻寬臨界值來限制對類別中網站的存取，請標記或清除**運用 Bandwidth Optimizer 封鎖**。請參閱[使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁。  
如果已選擇根據頻寬封鎖，請指定要使用的臨界值限制。
5. 重複步驟 1 到 3 以變更套用至其他類別的篩選動作。
6. 在編輯篩選器後，請按一下**確定**以快取所做的變更，並返回「篩選器」頁面。按一下**全部儲存**才能使變更生效。

要啟動新的類別篩選器，請將它新增至政策，並將政策指派給用戶端。請參閱[網際網路篩選政策](#)，第 65 頁。

## 建立通訊協定篩選器

相關主題：

- ◆ [篩選類別和通訊協定](#)，第 34 頁
- ◆ [篩選動作](#)，第 39 頁
- ◆ [編輯通訊協定篩選器](#)，第 46 頁
- ◆ [使用通訊協定](#)，第 160 頁

可使用**政策管理 > 篩選器 > 新增通訊協定篩選器**頁面定義新的通訊協定篩選器。可以使用預先定義的範本，或製作現有通訊協定篩選器的複本，以用作新篩選器的基礎。

1. 輸入唯一的**篩選器名稱**。名稱長度必須介於 1 到 50 個字元之間，且不能包含下列任何字元：  
 \* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,  
 篩選器名稱可包含空格、橫線和單引號。
2. 輸入篩選器的簡短**說明**。此說明會顯示在「篩選器」頁面之「通訊協定篩選器」區段中的篩選器名稱旁，且應說明篩選器的目的。  
 適用於篩選器名稱的字元限制也適用於說明，但有 2 個例外：說明可包含句點 (.) 和逗號 (,)。
3. 從下拉式清單中選取項目，以決定是否要使用範本 (請參閱[類別和通訊協定篩選器範本](#)，第 48 頁) 或製作現有篩選器的複本作為新篩選器的基礎。

4. 若要查看及編輯新篩選器，請按一下**確定**。篩選器會新增至「篩選器」頁面上的**通訊協定篩選器**清單中。

要完成自訂新篩選器，請繼續[編輯通訊協定篩選器](#)。

## 編輯通訊協定篩選器

相關主題：

- ◆ [篩選類別和通訊協定](#)，第 34 頁
- ◆ [建立通訊協定篩選器](#)，第 45 頁
- ◆ [篩選動作](#)，第 39 頁
- ◆ [使用通訊協定](#)，第 160 頁
- ◆ [使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁

可使用**政策管理 > 篩選器 > 編輯通訊協定篩選器**頁面變更現有通訊協定篩選器。



### 重要

在此所做的變更會影響所有強制執行此篩選器的政策。

強制執行其他委派管理角色中名稱相同之通訊協定篩選器的政策則不受影響。

篩選器名稱和說明顯示在頁面頂端。

- ◆ 按一下**重新命名**可變更篩選器名稱。
- ◆ 只要在**說明**欄位中鍵入相關內容即可變更篩選器說明。

**使用此篩選器的政策**旁的數字顯示有多少政策目前使用選取的篩選器。如果已啟用通訊協定篩選器，按一下**檢視政策**可取得強制執行篩選器的政策的清單。

頁面底部會顯示通訊協定清單，以及目前套用至每個通訊協定的動作。

若要變更篩選和記錄通訊協定的方式：

1. 在**通訊協定**清單中選取一個通訊協定。所選通訊協定的進階篩選動作會顯示在清單右側。

2. 可使用「通訊協定」清單底部的**允許**和**封鎖**按鈕變更套用至所選通訊協定的動作。

**注意**

Websense 軟體可封鎖以 TCP 為基礎的通訊協定要求，但無法封鎖以 UDP 為基礎的通訊協定要求。

某些應用程式同時使用以 TCP 和 UDP 為基礎的訊息。如果應用程式的原始網路要求是透過 TCP 提出的，然後使用 UDP 傳送後續資料，則 Websense 軟體會封鎖初始的 TCP 要求，並因而封鎖後續的 UDP 流量。

即使已允許 UDP 要求，該要求也可能會記錄為遭封鎖。

要將相同動作套用至選定通訊協定群組中的其他通訊協定，請按一下**套用到群組**。

3. 如果需要可用於警示或報告之選定通訊協定的使用資訊，請標記**記錄通訊協定資料**核取方塊。
4. 要在使用此通訊協定時加上頻寬限制，請按一下**運用 Bandwidth Optimizer 封鎖**，然後套用要使用的頻寬臨界值。如需詳細資訊，請參閱[使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁。
5. 在編輯篩選器後，請按一下**確定**以快取所做的變更，並返回「篩選器」頁面。按一下**全部儲存**才能使變更生效。

要啟動新的通訊協定篩選器，請將它新增至政策，並將政策套用至用戶端 (請參閱[網際網路篩選政策](#)，第 65 頁)。

**注意**

可以建立會在特定時間開始強制執行通訊協定篩選器的政策。如果使用者在該篩選器生效前啟動通訊協定工作階段，則只要工作階段仍在繼續，那麼即使篩選器封鎖該通訊協定，使用者還是能繼續存取該通訊協定。一旦使用者終止工作階段，則對該通訊協定的其他要求都會被封鎖。

## Websense 定義的類別和通訊協定篩選器

Websense 軟體包括數個範例類別和通訊協定篩選器。可以按原樣使用這些篩選器，或修改它們以符合自己的篩選需要。如果不需要預先定義的篩選器，也可以將其中許多篩選器刪除。

預先定義的類別篩選器包括：

- ◆ 基本
- ◆ 基本安全性
- ◆ 全部封鎖
- ◆ 預設
- ◆ 僅監控
- ◆ 全部允許

雖然可將「全部封鎖」和「全部允許」類別篩選器新增至政策，不過它們並未列在「篩選器」頁面上。這些篩選器扮演特殊的篩選角色，且無法刪除或編輯它們。篩選網際網路要求時，Websense 軟體會先檢查是否可套用「全部封鎖」或「全部允許」篩選器，然後再執行任何其他篩選檢查（請參閱[篩選網站](#)，第 72 頁）。

預先定義的通訊協定篩選器包括：

- ◆ 基本安全性
- ◆ 預設
- ◆ 僅監控
- ◆ 全部允許

「全部允許」通訊協定篩選器與其等同的類別篩選器一樣，不會在「篩選器」頁面上列出，且無法編輯或刪除。執行篩選時也會排定優先順序。

可以編輯「預設」類別和通訊協定篩選器，但無法將其刪除。在升級的環境中，如果「預設」政策中存有差距，則會使用「預設」篩選器來篩選未套用任何政策的要求。

## 類別和通訊協定篩選器範本

要建立新的類別或通訊協定篩選器時，可以先在「篩選器」頁面上製作現有篩選器的複本、在「新增篩選器」頁面上選取現有篩選器作為模型，或使用篩選器範本。

Websense 軟體包含 5 個類別篩選器範本：

- ◆ **僅監控**和**全部允許**會允許所有類別。
- ◆ **全部封鎖**會封鎖所有類別。
- ◆ **基本**會封鎖最常封鎖的類別並允許其餘類別。
- ◆ **預設**會將「封鎖」、「允許」、「繼續」和「配額」等動作套用至類別。



- ◆ **基本安全性**只會封鎖「安全性風險」等級中的預設類別 (請參閱[風險等級](#)，第 36 頁)。

Websense 軟體也包含 3 個通訊協定篩選器範本：

- ◆ **僅監控和全部允許**會允許所有通訊協定。
- ◆ **基本安全性**會封鎖「P2P 檔案共用」和「以 Proxy 規避封鎖」通訊協定，以及即時訊息傳送檔案附件 (如有訂閱) 和「惡意流量」(Websense Web Security)。
- ◆ **預設**會封鎖即時訊息傳送通訊協定，以及「P2P 檔案共用」、「以 Proxy 規避封鎖」、即時訊息傳送檔案附件 (如有訂閱) 和「惡意流量」(Websense Web Security)。

雖然可修改或刪除大多數由 Websense 定義的類別和通訊協定篩選器，但無法編輯或移除範本。同樣可視需要建立任意數目的自訂篩選器，但無法建立新範本。

範本無法修改，不過它們提供了重新參考由 Websense 定義的篩選器所套用之原始篩選動作的固定方法。例如，「一般」類別和通訊協定篩選器範本套用的動作，與原始「預設」類別和通訊協定篩選器套用的動作相同。這表示永遠可透過建立使用範本預設值的篩選器，來還原原始的 Websense 篩選配置。

如需使用範本來建立新篩選器的指示，請參閱[建立類別篩選器](#)，第 43 頁或[建立通訊協定篩選器](#)，第 45 頁。

## 設定 Websense 篩選設定

相關主題：

- ◆ [篩選類別和通訊協定](#)，第 34 頁
- ◆ [用戶端](#)，第 53 頁
- ◆ [封鎖頁面](#)，第 75 頁
- ◆ [篩選動作](#)，第 39 頁
- ◆ [密碼覆寫](#)，第 41 頁
- ◆ [篩選順序](#)，第 71 頁
- ◆ [使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁
- ◆ [根據關鍵字篩選](#)，第 156 頁

使用**設定 > 篩選**頁面，可建立各種不同篩選功能的基本設定。

在 **Bandwidth Optimizer** 下輸入所需的資訊，以根據可用頻寬來篩選網際網路使用量。如需以頻寬為基礎的篩選的詳細資訊，請參閱[使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁。

1. 要指定**網際網路連線速度**，請執行下列某項：
  - 從下拉式清單中選取標準速度。
  - 在文字欄位中以每秒千位元 (Kbps) 為單位輸入網路速度。
2. 使用**網路的預設頻寬**欄位，輸入要在啓用網路頻寬篩選時使用的預設臨界值 (網路總流量的百分比)。
3. 使用**每一通訊協定的預設頻寬**欄位，輸入要在啓用通訊協定頻寬篩選時使用的預設臨界值。

使用**一般篩選區段**，來決定套用多個群組政策時如何篩選使用者、指定關鍵字搜尋選項，以及設定密碼覆寫、繼續和配額工作階段行爲。

1. 要決定套用多個群組政策時如何篩選使用者，請標記或清除**使用限制最強的群組政策** (請參閱[篩選順序](#)，第 71 頁)。
  - 選取該選項時，會套用具有限制最強之篩選設定的政策。換言之，如果某個適用的群組政策封鎖對類別的存取，但另一個政策允許存取，則使用者對該類別中網站的要求會被封鎖。
  - 未選取該選項時，會使用最寬鬆的設定。
2. 選取下列**關鍵字搜尋選項**中的一個 (請參閱[根據關鍵字篩選](#)，第 156 頁)。

僅 CGI	關鍵字出現在 CGI 查詢字串 (位在網址中的「?」之後) 中時封鎖網站。 範例： <a href="http://search.yahoo.com/search?p=test">search.yahoo.com/search?p=test</a> 當選取此選項時 Websense 軟體不會在「?」之前搜尋關鍵字。
僅 URL	當關鍵字出現在 URL 中時封鎖網站。如果要求的網址包含 CGI 查詢字串，Websense 軟體只會在「?」之前搜尋關鍵字。
URL 和 CGI	當關鍵字出現在網址中任何位置時封鎖網站。如果存在 CGI 查詢字串，Websense 軟體會在「?」之前和之後搜尋關鍵字。
停用關鍵字封鎖	請小心使用。 <b>停用關鍵字封鎖</b> 會關閉所有關鍵字封鎖，即使已在類別篩選器中選取 <b>封鎖關鍵字</b> 也一樣。

3. 在**密碼覆寫逾時**欄位中，輸入使用者在選取密碼覆寫後可存取所有類別中的網站的最長時間 (以秒為單位最長 3600 秒預設為 60 秒) (請參閱[密碼覆寫](#)，第 41 頁)。
4. 在**繼續逾時**欄位中，輸入使用者在按一下「繼續」後，可存取「確認」動作所控管之類別中的網站的最長時間 (以秒為單位，最長 3600 秒，預設為 60 秒) (請參閱[篩選動作](#)，第 39 頁)。
5. 在**配額工作階段長度**欄位中輸入時間間隔 (最長 60 分鐘，預設為 10 分鐘) 使用者可在該時間間隔內造訪配額限制類別中的網站 (請參閱[使用配額時間來限制網際網路存取](#)，第 40 頁)。

使用者按一下「使用配額時間」按鈕後，工作階段便會開始。

6. 輸入所有使用者的**預設每日配額時間** (最長 240 分鐘，預設為 60 分鐘)。

要變更個別使用者的配額時間，請前往**政策 > 用戶端**頁面。

變更「配額工作階段長度」和「預設每日配額時間」後，會計算並顯示**預設每日配額工作階段**。

使用**封鎖訊息**區段，輸入為以瀏覽器為基礎的封鎖訊息的最上層框架所建立之替代型 HTML 封鎖頁面的 URL 或路徑 (請參閱[建立替代封鎖訊息](#)，第 81 頁)。

- ◆ 不同頁面可用於不同的通訊協定：**FTP**、**HTTP** (包括 **HTTPS**) 和 **Gopher**。
- ◆ 將這些欄位保留空白，以使用 Websense 軟體所提供的預設封鎖訊息，或該訊息的自訂版本 (請參閱[自訂封鎖訊息](#)，第 77 頁)。

在**搜尋篩選**底下，選取**啟動搜尋篩選**，使 Websense 軟體啟動特定搜尋引擎的內建設定，以便與已封鎖網站相關的縮圖影像和其他明確內容不會顯示在搜尋結果中 (請參閱[搜尋篩選](#)，第 42 頁)。

此功能支援的搜尋引擎顯示在區段底部。

完成設定「篩選」設定後，請按一下**確定**以快取變更。按一下**全部儲存**才能使變更生效。



# 3

## 用戶端

您可以自訂 Websense 軟體如何篩選來自特定使用者或電腦的要求，方法是將那些使用者或電腦新增為 Websense Manager 中的**用戶端**。用戶端可以是：

- ◆ **電腦**：您網路中的個別電腦，以 IP 位址定義。
- ◆ **網路**：電腦群組，全部以一個 IP 位址範圍定義。
- ◆ **使用者**：支援的目錄服務中的使用者、群組或網域帳戶。

一開始，Websense 軟體會以同樣方式篩選所有用戶端，也就是使用**預設政策** (請參閱**預設政策**，第 66 頁)。當您將用戶端新增到 Websense Manager 的「用戶端」頁面中之後，就可以將特定篩選政策指派到該用戶端。

如果可能有多個政策要套用 (例如一個政策指派到使用者，而另一個政策指派到電腦)，Websense 軟體會如下列所述判斷要強制執行哪一個政策：

1. 套用指派到發出要求之**使用者**的政策。如果該政策在要求的時間沒有排程篩選器，就會使用下一個適用的政策。
2. 如果沒有特定於使用者的政策，或該政策在要求的時間沒有啓用的篩選器，就會尋找指派到執行要求之**電腦** (第一) 或**網路** (第二) 的政策。
3. 如果沒有特定於電腦或網路的政策，或政策在要求的時間沒有啓用的篩選器，則會尋找指派到該使用者所屬之任一**群組**的政策。如果使用者屬於多個群組，Websense 軟體會考量所有套用的群組政策 (請參閱**篩選順序**，第 71 頁)。
4. 如果沒有群組政策，則會尋找指派到使用者之**網域** (OU) 的政策。
5. 如果找不到適用的政策，或政策在要求的時間沒有強制執行類別篩選器，則會強制執行用戶端所指派之角色的**預設政策**。

如需有關 Websense 軟體如何將篩選政策套用到用戶端的詳細資訊，請參閱**篩選網站**，第 72 頁。

## 使用用戶端

相關主題：

- ◆ [用戶端](#)，第 53 頁
- ◆ [使用電腦與網路](#)，第 55 頁
- ◆ [使用使用者與群組](#)，第 56 頁
- ◆ [新增用戶端](#)，第 61 頁
- ◆ [變用戶端設定](#)，第 62 頁

使用**政策管理** > **用戶端**頁面來檢視有關現有用戶端的資訊、新增、編輯或刪除用戶端，或將用戶端移動至委派管理角色。

如果您是委派管理員，必須在您的受管理用戶端清單中新增用戶端，才能在「用戶端」頁面上看到它們。如需指示，請參閱[新增用戶端](#)，第 61 頁。

用戶端分為 3 個群組：

- ◆ **目錄**，包含來自您目錄服務的使用者、群組及網域 (請參閱[使用使用者與群組](#)，第 56 頁)。
- ◆ **網路**，可以由單一政策所管理的受篩選網路中的 IP 位址範圍 (請參閱[使用電腦與網路](#)，第 55 頁)。
- ◆ **電腦**，在受篩選網路中的個別電腦，由 IP 位址識別 (請參閱[使用電腦與網路](#)，第 55 頁)。

按一下用戶端類型旁邊的加號 (+) 可以檢視所選擇類型的現有用戶端清單。每一個用戶端清單包括：

- ◆ 用戶端名稱、IP 位址或 IP 位址範圍。
- ◆ 目前指派到用戶端的**政策**。直到您指派其他政策之前，會一直使用**預設政策** (請參閱[網際網路篩選政策](#)，第 65 頁)。
- ◆ 用戶端是否可以使用**密碼覆寫**選項以檢視封鎖的網站 (請參閱[密碼覆寫](#)，第 41 頁)。
- ◆ 用戶端是否分配了自訂的**配額時間量** (請參閱[使用配額時間來限制網際網路存取](#)，第 40 頁)。

若要尋找特定的用戶端，瀏覽樹狀結構中的適當節點。

若要編輯用戶端政策、密碼覆寫、配額時間及驗證設定，選取清單中一或多個用戶端，然後按一下**編輯**。如需詳細資訊，請參閱[變用戶端設定](#)，第 62 頁。

若要新增用戶端，或將政策套用到目前沒有顯示在「用戶端」頁面中的受管理用戶端，按一下**新增**，然後前往[新增用戶端](#)，第 61 頁以獲得詳細資訊。

如果您已建立了委派管理角色 (請參閱 [委派管理](#)，第 205 頁)，「超級管理員」可以將他們的用戶端移至其他角色。首先勾選用戶端項目旁的核取方塊，然後按一下 **移至角色**。當用戶端移至委託管理角色時，套用到該用戶端的政策與篩選器也會複製到該角色。如需詳細資訊，請參閱 [將用戶端移到角色](#)，第 63 頁。

如果您已設定 Websense 軟體與以 LDAP 為基礎的目錄服務通訊，**管理自訂 LDAP 群組** 按鈕會顯示在頁面頂端的工具列中。按一下這個按鈕以 LDAP 屬性為基礎來新增或編輯群組 (請參閱 [使用自訂 LDAP 群組](#)，第 60 頁)。

若要從 Websense Manager 移除用戶端，選取用戶端並按一下 **刪除**。

## 使用電腦與網路

相關主題：

- ◆ [使用用戶端](#)，第 54 頁
- ◆ [使用使用者與群組](#)，第 56 頁
- ◆ [新增用戶端](#)，第 61 頁
- ◆ [將政策指派到用戶端](#)，第 70 頁

在 Websense Manager 中，**電腦** 指的是與受篩選電腦相關聯的 IP 位址 (例如 10.201.3.1)。**網路** 指的是與受篩選電腦群組相關聯的 IP 位址範圍 (例如 10.201.3.2 - 10.201.3.44)。

您可以將政策指派到電腦和網路用戶端，正如將政策指派到使用者、群組或網域用戶端一樣。

- ◆ 例如，將政策指派到不需要使用者登入，或可以使用來賓帳戶存取的 **電腦**。
- ◆ 將政策指派到 **網路** 可以將相同的篩選政策一次套用到數個電腦。

**除非** 您已將政策指派到已登入的使用者，否則當您將政策指派到電腦或網路時，不論誰登入受篩選電腦，都會強制執行該政策。此電腦或網路政策的優先權高於可以套用到使用者的任何 **群組** 政策。

## 使用使用者與群組

相關主題：

- ◆ [使用用戶端](#)，第 54 頁
- ◆ [目錄服務](#)，第 56 頁
- ◆ [使用自訂 LDAP 群組](#)，第 60 頁
- ◆ [使用電腦與網路](#)，第 55 頁
- ◆ [新增用戶端](#)，第 61 頁
- ◆ [將政策指派到用戶端](#)，第 70 頁

爲了將政策套用到您網路中個別的使用者與群組，請設定 Websense 軟體存取您的目錄服務，以便獲得目錄物件 (使用者、群組、網域及組織單位) 資訊。

Websense 軟體可以與 Windows NT Directory / Active Directory (混合模式) 通訊，也可以與透過輕量級目錄存取協定 (Lightweight Directory Access Protocol, LDAP) 存取的 Windows Active Directory、Novell eDirectory 及 Sun Java System Directory 通訊。



### 注意

當您使用以 LDAP 爲基礎的目錄服務時，不支援重複的使用者名稱。請確定在多個網域中沒有出現相同的使用者名稱。

此外，如果您使用 Windows Active Directory 或 Sun Java System Directory，則不支援採用空白密碼的使用者名稱。請確定所有使用者皆已指定密碼。

Websense User Service 會將資訊從目錄服務傳遞至 Policy Server 與 Filtering Service，以使用來套用篩選政策。

Websense, Inc. 建議在 Windows 電腦上安裝 User Service (雖然它可以安裝在 Linux 電腦上)。一般而言，該電腦就是安裝 Policy Server 的電腦。

若要設定 Websense 軟體與您的目錄服務通訊，請參閱 [目錄服務](#)。

## 目錄服務

目錄服務是儲存有關網路使用者與資源之資訊的工具。您必須先設定 Websense 軟體從您的目錄服務擷取資訊，然後才可以將使用者用戶端 (使用者、群組、網域或組織單位) 新增到 Websense Manager。

使用 [設定 > 目錄服務](#) 頁面以識別您網路中使用的目錄服務。針對每個 Policy Server，您只能設定一種目錄服務的設定。



首先，從「目錄」清單選取目錄服務。您所做的選擇會決定頁面上會顯示哪些設定。

如需配置指示，請參閱下列適當章節：

- ◆ [Windows NT Directory / Active Directory \(混合模式\)](#)，第 57 頁
- ◆ [Windows Active Directory \(原生模式\)](#)，第 57 頁
- ◆ [Novell eDirectory 與 Sun Java System Directory](#)，第 58 頁

## Windows NT Directory / Active Directory (混合模式)

如果您的目錄服務是 Windows NT Directory 或混合模式的 Active Directory，則不需要進一步的配置。

如果您使用其他的目錄服務，可能需要在本畫面中提供其他資訊；不過這情況很少見。這只會發生在下列情況：

- ◆ 使用 DC Agent 做為無障礙識別 (請參閱 [DC Agent](#)，第 185 頁)
- 及
- ◆ 在 Linux 電腦上執行 User Service

如果您的配置符合上述情況，請提供列在「Windows NT Directory / Active Directory (混合模式)」之下的管理認證。如果您的安裝不使用此配置，那麼管理認證欄位會停用。

## Windows Active Directory (原生模式)

Windows Active Directory 會將使用者資訊儲存在一或多個全域目錄中。全域目錄可讓個人與應用程式找到 Active Directory 網域中的物件 (使用者、群組等等)。

為了使 Websense 軟體與「原生模式的 Active Directory」通訊，您必須提供有關您網路中全域目錄伺服器的資訊。

1. 按一下「全域目錄伺服器」清單旁邊的**新增**。接著會顯示「新增全域目錄伺服器」頁面。
2. 使用**伺服器 IP 或名稱**欄位來識別全域目錄伺服器：
  - 如果您已經設定多個全域目錄伺服器進行容錯移轉，請輸入 DNS 網域名稱。
  - 如果您的全域目錄伺服器尚未設定進行容錯移轉，請輸入要新增之伺服器的 IP 位址或主機名稱 (如果您的網路中已啟用名稱解析的話)。
3. 輸入 Websense 軟體應該用來與全域目錄通訊的**連接埠** (預設為 **3268**)。
4. 或者，也可以輸入 Websense 軟體應該用來搜尋使用者資訊的**根環境**。如果您提供值，該值必須是您網域中的有效內容。
  - 如果您指定通訊連接埠為 3268 或 3269，則不需要提供根環境。
  - 如果您指定的連接埠為 389 或 636，則必須提供根環境。

- 如果「根環境」欄位留空，Websense 軟體會從目錄服務的最上層開始搜尋。



#### 注意

避免在多個網域中出現相同的使用者名稱。如果 Websense 軟體發現使用者有重複的帳戶名稱，就無法無障礙地識別該使用者。

5. 指定 Websense 軟體應該使用哪個管理帳戶從目錄服務擷取使用者名稱與路徑資訊。此帳戶必須能夠查詢並讀取目錄服務，但不需要變更目錄服務的能力或者為網域管理員。

選取**依元件劃分的識別名稱**或**完整的識別名稱**來指定您希望用什麼方式輸入帳戶資訊。

- 如果您選取「依元件劃分的識別名稱」，輸入管理帳戶的**顯示名稱**、**帳戶密碼**、**帳戶資料夾**及**DNS 網域名稱**。請使用管理使用者名稱的一般名稱 (cn) 形式，而非使用者 ID (uid) 形式。



#### 注意

**帳戶資料夾**欄位不支援具有組織單位 (ou) 標記的值 (例如，*ou=Finance*)。如果您的管理帳戶名稱含有 ou 標記，輸入管理帳戶的完整識別名稱。

- 如果您選取「完整的識別名稱」，在**使用者識別名稱**欄位中將識別名稱做為單一字串輸入 (例如，*cn=Admin*、*cn=Users*、*ou=InfoSystems*、*dc=company*、*dc=net*)，然後提供該帳戶的**密碼**。
6. 按一下**確定**。
  7. 針對每一個全域目錄伺服器，重複上述程序。
  8. 按一下**進階目錄設定**，然後前往[進階目錄設定](#)，第 59 頁。

## Novell eDirectory 與 Sun Java System Directory

若要從目錄服務擷取資訊，Websense 軟體需要具有管理員權限的使用者帳戶之識別名稱、根環境及密碼。

1. 在**伺服器 IP**欄位中輸入目錄伺服器電腦的 IP 位址。
2. 輸入 Websense 軟體將會用來與目錄通訊的**連接埠**號碼。預設值是 389。
3. 如果您的目錄要求管理員權限才能進行唯讀存取，輸入**管理員識別名稱**與**密碼**。
4. 或者，也可以輸入 Websense 軟體搜尋使用者資訊時應該使用的**根環境**。例如，*o=domain.com*。

縮小內容範圍可以加快擷取使用者資訊的速度與效率。



#### 注意

避免在多個網域中出現相同的使用者名稱。如果 Websense 軟體發現使用者有重複的帳戶名稱，就無法無障礙地識別該使用者。

5. 按一下 **進階目錄設定**，然後前往 [進階目錄設定](#)，第 59 頁。

## 進階目錄設定

相關主題：

- ◆ [Windows Active Directory \(原生模式\)](#)，第 57 頁
- ◆ [Novell eDirectory 與 Sun Java System Directory](#)，第 58 頁

這些設定可以用來定義下列內容：

- ◆ Websense 軟體如何搜尋目錄服務，以尋找使用者、群組及網域資訊
- ◆ Websense 軟體是否使用加密的連線來與目錄服務通訊
- ◆ Websense 應該使用哪一個字元集來編碼 LDAP 資訊

針對所有以 LDAP 為基礎的目錄服務，視需要設定這些設定。

1. 如果您在目錄服務中自訂物件等級類型（屬性名稱），請核取**使用自訂篩選器**。預設的篩選器字串會顯示在「篩選器」欄位中。
2. 編輯現有的篩選器字串，代替特定於您目錄的物件等級類型。例如，如果您的目錄使用 **dept** 之類的物件等級類型，而不是使用 **ou**（組織單位），請在「網域搜尋篩選器」欄位中插入新的值。

屬性永遠是搜尋目錄服務內容時所使用的字串。自訂篩選器提供此處所述的功能。

- **使用者搜尋篩選器**可決定 User Service 如何搜尋使用者。
  - **群組搜尋篩選器**可決定 User Service 如何搜尋群組。
  - **網域搜尋篩選器**可決定 User Service 如何搜尋網域或組織單位。
  - **使用者的群組搜尋篩選器**可決定 User Service 如何將使用者與群組相關聯。
3. 若要保護 Websense 軟體與目錄服務之間的通訊安全，請核取**使用 SSL**。
  4. 若要決定 Websense 軟體用來編碼 LDAP 資訊的字元集，請選取 **UTF-8** 或 **MBCS**。  
MBCS，或稱為多位元組字元集，經常用來編碼東亞語言，例如中文、日文及韓文。
  5. 按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## 使用自訂 LDAP 群組

相關主題：

- ◆ [使用使用者與群組](#)，第 56 頁
- ◆ [目錄服務](#)，第 56 頁
- ◆ [新增或編輯自訂 LDAP 群組](#)，第 60 頁

使用**管理自訂 LDAP 群組**頁面可根據您的目錄服務中定義的屬性來管理自訂群組。只有當您設定 Websense 軟體與以 LDAP 為基礎的目錄服務通訊時，此選項才可以使用。



### 重要

當您新增 LDAP 群組至 Websense Manager 時，群組定義會由啓用的 Policy Server 儲存，而且不會影響其他 Policy Server 實例。若要新增 LDAP 群組至多個 Policy Server，使用 Websense Manager 來登入每個 Policy Server 並輸入資訊。

如果您新增自訂 LDAP 群組，然後變更目錄服務或變更目錄伺服器的位置，那麼現有的群組會變成無效。您必須再次新增群組，然後將每一個群組定義為用戶端。

- ◆ 若要新增群組，按一下**新增** (請參閱[新增或編輯自訂 LDAP 群組](#)，第 60 頁)。
- ◆ 若要變更清單中的項目，按一下其群組名稱上 (請參閱[新增或編輯自訂 LDAP 群組](#))。
- ◆ 若要移除項目，請先選取它，然後按一下**刪除**。

當您完成變更自訂 LDAP 群組時，按一下**確定**來快取變更並返回上一頁。按一下**全部儲存**才能使變更生效。

## 新增或編輯自訂 LDAP 群組

使用**新增自訂 LDAP 群組**頁面，根據您已在目錄服務中定義的任何屬性在 Websense Manager 中定義群組。使用**編輯自訂 LDAP 群組**頁面以變更現有的定義。



### 重要

如果您新增自訂 LDAP 群組，然後變更目錄服務或變更目錄伺服器的位置，那麼現有的群組會變成無效。您必須再次新增群組，然後將每一個群組定義為用戶端。

1. 輸入或變更**群組名稱**。使用可清楚指示 LDAP 群組目的之描述性名稱。群組名稱不分大小寫，且必須為唯一。

- 輸入或變更在您的目錄服務中定義此群組的說明。例如：

(WorkStatus=parttime)

在此範例中，**WorkStatus** 是指示雇用狀態的使用者屬性，而 **parttime** 這個值則是指示該使用者為兼職員工。

- 按一下**確定**以返回「管理自訂 LDAP 群組」頁面。新的或修訂後的項目會顯示在清單中。
- 新增或編輯另一個項目，或按一下**確定**以快取所做的變更並返回上一頁。按一下**全部儲存**才能使變生效。

## 新增用戶端

相關主題：

- ◆ [使用用戶端](#)，第 54 頁
- ◆ [使用電腦與網路](#)，第 55 頁
- ◆ [使用使用者與群組](#)，第 56 頁
- ◆ [搜尋目錄服務](#)，第 62 頁
- ◆ [變更用戶端設定](#)，第 62 頁

使用**政策管理 > 用戶端 > 新增用戶端**頁面來新增使用者、群組、電腦及網路用戶端至 Websense Manager，如此一來，您就可以為它們指派政策。

如果您已登入委派管理角色，那麼只能夠新增在您的受管理用戶端清單中顯示的用戶端。在新增受管理用戶端到「用戶端」頁面的過程中，您必須指派政策給它們。

- 識別一或多個用戶端：
  - 若要新增使用者、群組或網域用戶端，瀏覽**目錄樹狀結構**以尋找您目錄服務中的項目。如果您是使用以 LDAP 為基礎的目錄服務，也可以按一下**搜尋**來啟用目錄搜尋工具（請參閱[搜尋目錄服務](#)，第 62 頁）。
  - 若要新增電腦或網路用戶端，輸入 **IP 位址**或 **IP 位址範圍**。任何兩個網路定義不得重疊，但是網路用戶端可以包括分別識別為電腦用戶端的 IP 位址。在這種重疊的情況下，指派到該電腦的政策優先權高於指派到網路的政策。
- 按一下箭頭按鈕 (>) 將每個用戶端新增至**已選擇用戶端**清單。
- 若要從「已選擇用戶端」清單中移除項目，選取該用戶端，然後按一下**移除**。
- 選取**政策**以指派到「已選擇用戶端」清單中的所有用戶端。
- 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變生效。

那些用戶端會新增至**政策管理 > 用戶端**頁面上適當的清單。若要變更指派到一或多個用戶端的政策，或設定其他用戶端設定，請選取每個用戶端項目，然後按一下**編輯**。如需詳細資訊，請參閱[變更用戶端設定](#)，第 62 頁。

## 搜尋目錄服務

如果您已設定 Websense 軟體與以 LDAP 為基礎的目錄服務通訊，可以使用搜尋功能來識別使用者，以便將其新增為 Websense Manager 中的用戶端。新增受管理的用戶端和管理員至委派管理角色時，也可以使用搜尋。

若要搜尋目錄服務以便擷取使用者、群組及組織單位資訊：

1. 按一下**搜尋**。
2. 輸入全部或部分的使用者、群組或組織單位**名稱**。
3. 使用**類型**清單來指示您要尋找的目錄項目的類型 (使用者、群組、OU 或全部)。在大型目錄服務中，選取**全部**可能導致搜尋花費相當長時間。
4. 瀏覽**搜尋內容**樹狀目錄來指定要搜尋目錄的哪個部分。越精確的內容越有助於加快搜尋速度。
5. 按一下**開始**。  
接著會顯示搜尋結果清單。
6. 在搜尋結果中選擇一或多個項目，然後按一下向右箭頭 (>) 將每個選擇新增為用戶端或管理員。
7. 按一下**新搜尋**以輸入另一組搜尋條件。
8. 按一下**瀏覽**以返回瀏覽目錄。
9. 完成變更之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

## 變更用戶端設定

使用**政策管理 > 用戶端 > 編輯用戶端**頁面以變更一或多個用戶端的政策與驗證設定。如果您在按「編輯」之前選取了多個用戶端，那麼您在「編輯用戶端」頁面上所做的配置變更會套用到所有選擇的用戶端。

1. 選取**政策**以套用到已選擇的用戶端。在指派其他政策之前，會使用「預設」政策來管理用戶端。
2. 若要允許使用者藉由輸入密碼來覆寫 Websense 封鎖頁面，按一下「密碼覆寫」下的**開啓**，然後輸入並確認密碼。  
若要移除用戶端的密碼覆寫權限，按一下**關閉**。
3. 若要分配自訂的**配額時間**量給已選擇的用戶端，按一下**自訂**，然後輸入要指派的配額時間分鐘數。  
若要還原至預設配額設定，按一下**預設**。
4. 按一下**確定**來快取變更並返回「用戶端」頁面。按一下**全部儲存**才能使變更生效。

新的用戶端設定會顯示為**政策管理 > 用戶端**頁面上的用戶端清單的一部分。

## 將用戶端移到角色

「超級管理員」可以使用**將用戶端移到角色**頁面，將一或多個用戶端移到委派管理角色。一旦用戶端移動之後，該用戶端會顯示在「受管理的用戶端」清單以及「用戶端」頁面的目標角色中。

- ◆ 套用到「超級管理員」角色中的用戶端的政策及它所強制執行的篩選器會複製到委派管理角色。
- ◆ 委派管理員可以變更套用至他們的受管理用戶端的政策。
- ◆ 「篩選器鎖定」限制並不會影響「超級管理員」管理的用戶端，但是會影響委派管理角色中的受管理用戶端。
- ◆ 如果將群組、網域或組織單位做為受管理用戶端新增到角色，那麼該角色中的委派管理員可以將政策指派到群組、網域或組織單位中的個別使用者。
- ◆ 如果將網路 (IP 位址範圍) 做為受管理用戶端新增到角色，那麼該角色中的委派管理員可以將政策指派到該網路中的個別電腦。
- ◆ 同一個用戶端不能移到多個角色。

若要將已選擇的用戶端移到委派管理角色：

1. 從**選擇角色**下拉式清單中選取一個目的角色。
2. 按一下**確定**。

此時會顯示一個彈出式對話方塊，指示正在移動選擇的用戶端。移動作業可能需要一些時間才會完成。

3. 按一下**全部儲存**才能使變更生效。

如果在移動過程中，已選擇角色中的委派管理員以具有政策存取權的方式登入，他們必須登出 **Websense Manager** 然後再次登入，才能看到他們「受管理的用戶端」清單中的新用戶端。





# 4

## 網際網路篩選政策

相關主題：

- ◆ [網際網路使用量篩選器](#)，第 33 頁
- ◆ [用戶端](#)，第 53 頁
- ◆ [預設政策](#)，第 66 頁
- ◆ [使用政策](#)，第 67 頁
- ◆ [篩選順序](#)，第 71 頁

政策控管使用者的網際網路存取。政策由下列項目組成：

- ◆ 類別篩選器，用於將動作 (允許、封鎖) 套用至網站類別 (請參閱[篩選類別和通訊協定](#)，第 34 頁)
- ◆ 限制存取篩選器，用於允許僅存取有限的網站 (請參閱[將使用者限制於定義的網際網路網站清單](#)，第 145 頁)
- ◆ 通訊協定篩選器，用於將動作套用至網際網路通訊協定 (請參閱[篩選類別和通訊協定](#)，第 34 頁)
- ◆ 排程，用於決定何時強制執行每個類別篩選器或限制存取篩選器及通訊協定篩選器。

新的 Websense 軟體安裝包括 3 個預先定義的政策：

- ◆ **預設**會篩選沒有其他政策管理的所有用戶端的網際網路存取。輸入訂閱密碼後，Websense 軟體會立即開始強制執行此政策 (請參閱[預設政策](#)，第 66 頁)。
- ◆ **無限制**會對網際網路提供沒有限制的存取。在預設情況下，此政策不會套用至任何用戶端。
- ◆ **範例 – 一般使用者**會顯示如何在一個政策中套用多重類別及通訊協定篩選器，以便在不同時間提供不同等級的篩選限制。此政策用於「新使用者快速入門」教學課程中，示範編輯政策與套用政策至用戶端的程序。

以這些政策的原貌使用任何一個政策、編輯它們以適合您的組織或建立您自己的政策。

## 預設政策

---

相關主題：

- ◆ [網際網路篩選政策](#)，第 65 頁
- ◆ [使用政策](#)，第 67 頁
- ◆ [篩選順序](#)，第 71 頁

安裝 Websense 軟體時，**預設**政策會在您輸入訂閱密碼之後，立即開始監控網際網路的使用情況。「預設」政策最初會允許所有要求。



### 注意

如果從舊版 Websense 軟體升級，則會保留現有的政策設定。請在升級後檢閱政策以確認它們仍然適用。

建立並套用自已的篩選政策時，預設政策會繼續扮演安全網路的角色，篩選沒有其他政策管理的所有用戶端的網際網路存取。

在新安裝中，預設政策必須提供 24 小時全年無休的網際網路篩選涵蓋範圍 (強制執行類別或限制存取篩選器及通訊協定篩選器 (如果適用) 的組合)。



### 重要

如果從舊版 Websense 軟體升級，可能會有未涵蓋所有時段的預設政策。您並不需要變更預設政策。不過，如果日後編輯政策，除非涵蓋所有時段，否則 Websense 軟體將不允許您儲存變更。

視需要編輯預設政策以符合貴組織的需求。預設政策是無法刪除的。

## 使用政策

相關主題：

- ◆ [網際網路篩選政策](#)，第 65 頁
- ◆ [建立政策](#)
- ◆ [編輯政策](#)
- ◆ [網際網路使用量篩選器](#)
- ◆ [優化篩選政策](#)

使用**政策管理 > 政策**頁面檢閱現有政策資訊。此頁面也可作為下列操作的起點：新增、編輯與刪除政策、複製政策至委派管理角色（僅超級管理員），以及列印有關政策配置的詳細資訊。

「政策」頁面包括現有政策清單。清單包括每個政策的名稱與說明，以及接受政策的使用者、網路及電腦用戶端之數量。

- ◆ 若要新增政策，按一下**新增**，然後參閱[建立政策](#)，第 68 頁，以獲得詳細資訊。
- ◆ 若要編輯政策，在清單中按一下政策名稱，然後參閱[編輯政策](#)，第 68 頁，以獲得詳細資訊。
- ◆ 若要檢視政策篩選了哪些用戶端，按一下「使用者」、「網路」或「電腦」欄位中的數字。用戶端資訊會顯示在彈出式對話方塊中。

若要列印所有政策及其元件（包括篩選器、自訂類別與通訊協定、關鍵字、自訂 URL 及正規表示式）的清單，按一下**將政策列印成檔案**。此功能會以 Microsoft Excel 格式建立政策資訊的詳細試算表。該表格旨在為人力資源專家、經理及其他具有監督權限的人提供一個檢視篩選政策資訊的簡便方式。

如果已建立委派管理角色（請參閱[委派管理](#)，第 205 頁），超級管理員可將其所建立的政策複製到其他角色，以供委派管理員使用。政策所強制執行的篩選器也會一併複製。



### 注意

由於委派管理員是由「篩選器鎖定」所管理，因此全部允許篩選器及強制執行篩選器的政策並不會複製到角色。

若要將政策複製到其他角色，首先請標記政策名稱旁的核取方塊，然後按一下**複製到角色**。如需詳細資訊，請參閱[將篩選器和政策複製到角色](#)，第 149 頁。

## 建立政策

相關主題：

- ◆ [網際網路篩選政策](#)，第 65 頁
- ◆ [使用政策](#)，第 67 頁
- ◆ [編輯政策](#)，第 68 頁
- ◆ [使用篩選器](#)，第 42 頁
- ◆ [將使用者限制於定義的網際網路網站清單](#)，第 145 頁

使用**政策管理 > 政策 > 新增政策**頁面建立新的自訂政策。

1. 輸入唯一的**政策名稱**。政策名稱長度必須介於 1 到 50 個字元之間，且不能包含下列任何字元：

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

政策名稱可包含空格、橫線和單引號。

2. 輸入政策的**說明**。說明應該清楚且詳細，以便有助於長遠的政策管理。適用於政策名稱的字元限制也適用於說明，但有 2 個例外：說明可包含句點 (.) 和逗號 (,)。
3. 若要使用現有政策作為新政策的基礎，請標記以**現有政策為基礎**核取方塊，然後從下拉式清單中選取政策。  
若要以空政策為開始，則不要標記該核取方塊。
4. 按一下**確定**來快取變更並前往編輯政策頁面。  
使用編輯政策頁面以完成新政策的定義。請參閱[編輯政策](#)，第 68 頁。

## 編輯政策

相關主題：

- ◆ [網際網路篩選政策](#)，第 65 頁
- ◆ [使用政策](#)，第 67 頁
- ◆ [建立政策](#)，第 68 頁
- ◆ [使用篩選器](#)，第 42 頁
- ◆ [將使用者限制於定義的網際網路網站清單](#)，第 145 頁

使用**政策管理 > 政策 > 編輯政策**頁面來變更現有政策，或完成新政策的定義。

使用該頁面的上面部分來編輯政策名稱與說明：

- ◆ 按一下**重新命名**可變更政策名稱。

- ◆ 只要在**說明**欄位中輸入即可變更篩選器說明。

政策說明下的**用戶端**欄位會列出此政策目前篩選的每個類型 (使用者、電腦及網路) 有多少個用戶端。若要檢視政策管理的用戶端，按一下對應於相關用戶端類型的連結。

若要將此政策指派到其他用戶端，按一下頁面上方工具列中的**套用至用戶端**，然後請參閱[將政策指派到用戶端](#)，第 70 頁。

使用**政策定義**區域來定義此政策在不同時間要套用的篩選器：

1. 若要新增時間區塊到排程，按一下**新增**。
2. 使用排程表格中的**開始與結束**欄位來定義此時間區塊涵蓋的時段。  
若要定義跨越午夜時段的篩選 (例如下午 5 點到上午 8 點)，新增兩個時間區塊到排程中：一個涵蓋從開始時間到午夜的時段，另一個涵蓋從午夜到結束時間的時段。  
Websense 軟體中包含的**範例** — **一般使用者**政策會示範如何定義跨越午夜的篩選時段。
3. 使用**天**欄位來定義此時間區塊包括一週內的哪幾天。若要從清單中選取星期幾，按一下欄位右側的向下鍵。完成選取星期幾時，按一下向上鍵。
4. 使用**類別 / 限制存取篩選器**欄位來選取要在此時間區塊期間強制執行的篩選器。  
若要新增要在此政策中強制執行的新篩選器，選取**建立類別篩選器**或**建立限制存取篩選器**。如需指示，請參閱[建立類別篩選器](#)，第 43 頁或[建立限制存取篩選器](#)，第 147 頁。
5. 使用**通訊協定篩選器**欄位來選取要在此時間區塊期間強制執行的通訊協定篩選器。  
若要新增要在此政策中強制執行的新篩選器，選取**建立通訊協定篩選器**。如需指示，請參閱[建立通訊協定篩選器](#)，第 45 頁。
6. 重複步驟 1 到 5，新增其他時間區塊到排程中。

選取了排程中的所有時間區塊後，編輯政策頁面的下面部分會顯示要在該時間區塊期間強制執行的篩選器。每個篩選器清單包括：

- ◆ 篩選器類型 (類別篩選器、限制存取篩選器或通訊協定篩選器)
- ◆ 篩選器名稱與說明
- ◆ 篩選器內容 (套用了動作的類別或通訊協定，或者允許的網站清單)
- ◆ 強制執行所選篩選器的政策數
- ◆ 可用於編輯篩選器的按鈕

在本頁面上編輯篩選器時，所做的變更會影響強制執行該篩選器的每個政策。在編輯由多個政策強制執行的篩選器之前，按一下**使用此篩選器的政策數**連結來檢視確實受到影響的政策。

顯示在篩選器清單底部的按鈕取決於篩選器類型：

篩選器類型	按鈕
類別篩選器	<ul style="list-style-type: none"> <li>使用<b>允許</b>、<b>封鎖</b>、<b>確認</b>或<b>配額</b>按鈕來變更套用至所選類別的動作（請參閱<b>篩選動作</b>，第 39 頁）。</li> <li>若要變更套用至上層類別及其所有下層類別的動作，請先變更套用至上層類別的動作，然後按一下<b>套用至下層類別</b>。</li> <li>若要啟用關鍵字封鎖、檔案類型封鎖或根據頻寬封鎖，按一下<b>進階</b>。</li> </ul>
限制存取篩選器	<ul style="list-style-type: none"> <li>使用<b>新增網站</b>及<b>新增表示式</b>按鈕來新增允許的 URL、IP 位址或正規表示式到篩選器（請參閱<b>將使用者限制於定義的網際網路網站清單</b>，第 145 頁）。</li> <li>若要從篩選器移除網站，標記 URL、IP 位址或表示式旁的核取方塊，然後按一下<b>刪除</b>。</li> </ul>
通訊協定篩選器	<ul style="list-style-type: none"> <li>使用<b>允許</b>或<b>封鎖</b>按鈕來以變更套用至所選通訊協定的動作（請參閱<b>篩選動作</b>，第 39 頁）。</li> <li>若要變更套用至通訊協定群組中所有通訊協定的動作，變更套用至群組中任何通訊協定的動作，然後按一下<b>套用至群組</b>。</li> <li>若要記錄所選通訊協定的資料或啟用根據頻寬封鎖，按一下<b>進階</b>。</li> </ul>

完成編輯政策時，按一下**確定**來快取變更。按一下**全部儲存**後，才會執行變更。

## 將政策指派到用戶端

相關主題：

- ◆ [網際網路篩選政策](#)，第 65 頁
- ◆ [建立政策](#)，第 68 頁
- ◆ [編輯政策](#)，第 68 頁
- ◆ [用戶端](#)，第 53 頁
- ◆ [新增用戶端](#)，第 61 頁

使用**政策 > 編輯政策 > 將政策套用至用戶端**頁面，將所選政策指派到用戶端。

用戶端清單會顯示所有可用的使用者、電腦及網路用戶端，以及目前指派到每個用戶端的政策。

標記所選政策要篩選之每個用戶端旁的核取方塊，然後按一下**確定**返回編輯政策頁面。再按一次**確定**來快取變更。

按一下**全部儲存**來提示 Websense 軟體開始使用新政策篩選來自所選用戶端的要求。

## 篩選順序

Websense 軟體會使用多個篩選器，以特定順序套用，以便決定是否要允許、封鎖或限制要求的網際網路資料。

Websense 軟體會針對所收到的要求，執行下列動作：

1. 驗證訂閱規範，確認訂閱是目前訂閱及未超過訂閱的用戶端數目。
2. 決定要套用的政策，以下列順序搜尋：
  - a. 指派到**使用者**的政策。
  - b. 指派到正在使用之電腦 **IP 位址** (電腦或網路) 的政策。
  - c. 指派到使用者所屬**群組**的政策。
  - d. 指派到使用者**網域**的政策。
  - e. **預設**政策。系統會使用所找到的第一個適用政策。
3. 根據政策的限制來篩選要求。

在某些情況下，使用者屬於一個以上的群組或網域，但卻沒有套用使用者、電腦或網路政策。在這些情況下，Websense 軟體會檢查指派到每個使用者群組的政策。

- ◆ 如果所有群組具有相同政策，Websense 軟體會根據該政策來篩選要求。
- ◆ 如果其中一個群組有不同的政策，Websense 軟體會根據**設定 > 篩選**頁面上的**使用更為嚴格的封鎖**選項來篩選要求。

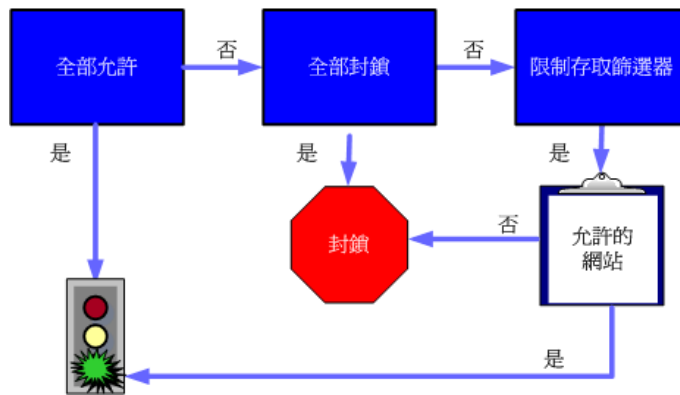
如果核取了**使用更為嚴格的封鎖**，而且任何適用的政策封鎖了存取所要求的類別，Websense 軟體便會封鎖網站。

如果未核取該選項，而且任何適用的政策允許存取所要求的類別，Websense 軟體便會允許網站。

如果適用的政策之一強制執行限制存取篩選器，**使用更為嚴格的封鎖**選項會產生預期以外的不同影響。請參閱[限制存取篩選器與篩選優先權](#)，第 146 頁。

## 篩選網站

Websense 軟體會以如下程序評估政策限制，以決定是否允許或封鎖要求的網站。



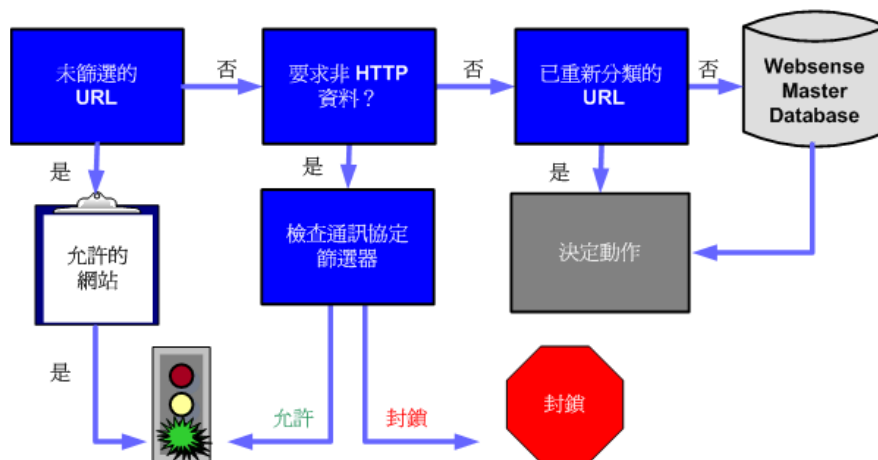
1. 決定在目前的星期日期與時間中，政策要強制執行的**類別篩選器**或**限制存取篩選器**。

- 如果作用中類別篩選器為**全部允許**，則允許網站。
- 如果作用中類別篩選器為**全部封鎖**，則封鎖網站。
- 如果篩選器為**限制存取篩選器**，請檢查篩選器中是否包含 URL 或 IP 位址。如果是，則允許網站。如果不是，則封鎖網站。
- 如果有任何其他的類別篩選器適用，則繼續進行步驟 2。



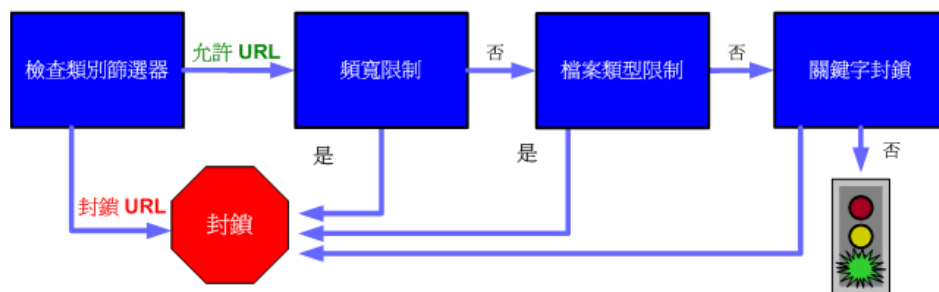
### 注意

Websense 軟體會篩選從網際網路搜尋引擎的快取所存取的 URL，就如同其他 URL 一樣。以這種方式儲存的 URL 會根據作用於其 URL 類別的政策來進行篩選。已快取之 URL 的 Log 記錄會顯示整個快取的 URL，包括所有搜尋引擎參數。



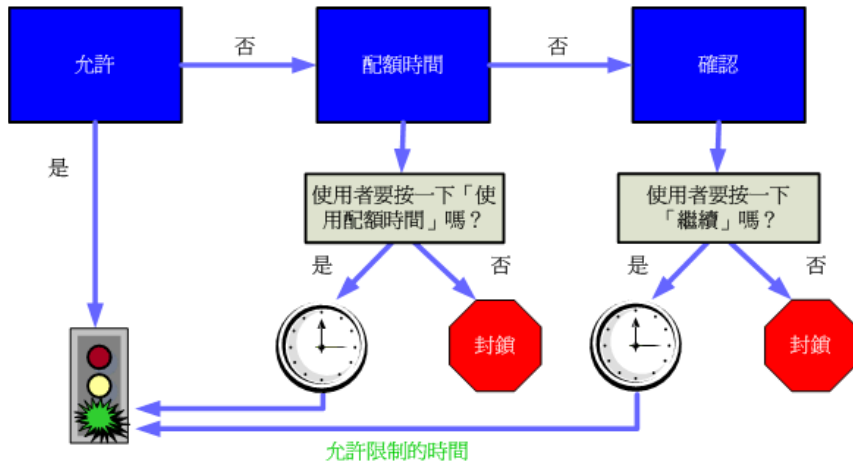


2. 嘗試將網站與**未篩選的 URL** 清單中的項目比對。
  - 如果 URL 出現在清單中，則允許網站。
  - 如果 URL 沒有出現在清單中，則繼續進行步驟 3。
3. 檢查作用中的**通訊協定篩選器**，並判斷是否有任何非 HTTP 通訊協定與要求相關聯。
  - 如果有，將通訊協定篩選設定套用至可能傳送的資料上。
  - 如果沒有，則繼續進行步驟 4。
4. 嘗試將網站與**已重新分類的 URL** 清單中的項目比對。
  - 如果有相符項目，確定網站的類別，然後進行步驟 6。
  - 如果沒有相符項目，則繼續進行步驟 5。
5. 嘗試將網站與**主資料庫**中的項目比對。
  - 如果 URL 出現在主資料庫中，確定網站的類別，然後繼續進行步驟 6。
  - 如果沒有相符項目，將網站分類為其他/尚未歸類，然後繼續進行步驟 6。



6. 檢查作用中的類別篩選器，然後確定套用至包含所要求網站之類別的動作。
  - 如果動作為**封鎖**，則封鎖網站。
  - 如果套用了其他動作，則繼續進行步驟 7。
7. 檢查作用中類別篩選器的 **Bandwidth Optimizer** 設定 (請參閱[使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁)。
  - 如果目前的頻寬使用超過任何設定的限制，則封鎖網站。
  - 如果目前的頻寬使用沒有超過指定的限制或沒有套用以頻寬為基礎的動作，則繼續進行步驟 8。
8. 檢查套用至作用中類別的**檔案類型限制** (請參閱[根據檔案類型管理流量](#)，第 168 頁)。
  - 如果網站中包含具有已封鎖副檔名的檔案，則封鎖存取那些檔案。如果網站本身由已封鎖的檔案類型所構成，則封鎖存取網站。
  - 如果網站不包含具有已封鎖副檔名的檔案，則前往步驟 9。

9. 如果已啓用關鍵字封鎖，則會檢查 URL 與 CGI 路徑中已封鎖的**關鍵字** (請參閱 [根據關鍵字篩選](#)，第 156 頁)。
  - 如果找到已封鎖的關鍵字，則封鎖網站。
  - 如果找不到已封鎖的關鍵字，則繼續進行步驟 10。



10. 根據套用至類別的動作來處理網站。
  - **允許**：允許網站。
  - **依配額限制**：顯示包含可使用配額時間來檢視網站的選項的封鎖訊息，或返回上一頁。
  - **確認**：顯示包含可檢視網站供工作目的之用的選項的封鎖訊息。

Websense 軟體會繼續執行，直到要求的網站遭到封鎖或明確允許。屆時，Websense 軟體不會嘗試任何進一步的篩選。例如，如果要求的網站屬於封鎖的類別，而且包含封鎖的關鍵字，Websense 軟體會在不檢查關鍵字篩選器的情況下在類別層級封鎖該網站。然後 Log Server 會記錄要求因封鎖的類別而封鎖，而非因關鍵字而封鎖。



**注意**

不論網站因什麼原因而封鎖，具有密碼覆寫權限的使用者都可以存取網際網路網站。

# 5

## 封鎖頁面

相關主題：

- ◆ [通訊協定封鎖訊息](#)，第 76 頁
- ◆ [使用封鎖頁面](#)，第 77 頁
- ◆ [建立替代封鎖訊息](#)，第 81 頁
- ◆ [使用位於其他電腦上的替代封鎖頁面](#)，第 81 頁

當 Websense 軟體封鎖網站時，它會在用戶端的瀏覽器中顯示封鎖頁面。如果該網站是因為屬於「安全風險」等級中的類別而遭封鎖（請參閱[風險等級](#)，第 36 頁），則會顯示特別版本的封鎖頁面。

根據預設，封鎖頁面由 3 個主要區段所組成。



- ◆ **標題**說明該網站已遭封鎖。
- ◆ **最上層框架**包含封鎖訊息，顯示所要求的 URL 及封鎖該 URL 的原因。
- ◆ **底部框架**會顯示使用者可用的所有選項，例如返回上一頁的選項，或按一下「[繼續](#)」或「[使用配額時間](#)」按鈕以檢視網站。

封鎖頁面是由 HTML 檔所建構的。您的 Websense 軟體中包含預設的封鎖頁面檔案。您可以使用這些預設檔案或建立自己的自訂版本。

- ◆ 自訂預設檔案以變更封鎖訊息 (請參閱 [使用封鎖頁面](#)，第 77 頁)。
- ◆ 設定 Websense 軟體以使用托管於遠端 Web 伺服器的預設或自訂封鎖訊息 (請參閱 [使用位於其他電腦上的替代封鎖頁面](#)，第 81 頁)。

## 通訊協定封鎖訊息

---

相關主題：

- ◆ [使用封鎖頁面](#)，第 77 頁
- ◆ [建立替代封鎖訊息](#)，第 81 頁
- ◆ [使用位於其他電腦上的替代封鎖頁面](#)，第 81 頁

當使用者或應用程式要求遭封鎖的、非 HTTP 通訊協定時，通常 Websense 軟體會顯示通訊協定封鎖訊息。

不過，當使用者從瀏覽器中要求已封鎖的 FTP、HTTPS 或 Gopher 網站，而且該要求會通過代理伺服器時，則會在瀏覽器中顯示 HTML 式的封鎖頁面。

如果應用程式要求封鎖的通訊協定，使用者也可能從應用程式接收到錯誤訊息，指出該操作無法執行。應用程式錯誤訊息不是由 Websense 軟體產生的。

爲了在 Windows 電腦上顯示通訊協定封鎖訊息，可能需要某些系統配置：

- ◆ 若要在執行 Windows NT、XP 或 200x 的電腦上顯示通訊協定封鎖訊息，則必須啓用 Windows Messenger 服務。根據預設，此服務是停用的。您可以使用「Windows 服務」對話方塊來找出指定電腦上是否執行該服務 (請參閱 [「Windows 服務」對話方塊](#)，第 340 頁)。
- ◆ 若要在 Windows 98 電腦上顯示通訊協定封鎖訊息，您必須啓動 **winpopup.exe**，此檔案位於 Windows 目錄中。從命令提示字元下執行應用程式，或將它複製到「啓動」資料夾，以設定它爲自動啓動。

Linux 電腦上不會顯示通訊協定封鎖訊息。而 HTML 封鎖頁面則是不論何種作業系統皆會顯示。

如果已啓用通訊協定篩選，Websense 軟體篩選器通訊協定會查詢用戶端電腦上是否設定爲顯示通訊協定封鎖訊息。

## 使用封鎖頁面

相關主題：

- ◆ [通訊協定封鎖訊息，第 76 頁](#)
- ◆ [自訂封鎖訊息，第 77 頁](#)
- ◆ [建立替代封鎖訊息，第 81 頁](#)
- ◆ [使用位於其他電腦上的替代封鎖頁面，第 81 頁](#)

用來建立 Websense 封鎖頁面的檔案儲存在 **Websense\BlockPages\en\Default** 目錄中：

- ◆ **master.html** 建構了封鎖頁面的資訊框架，並使用下列檔案其中之一在底部框架中顯示適當的選項。

檔案名稱	內容
blockFrame.html	在封鎖類別中之網站的文字與按鈕（「返回」選項）。
continueFrame.html	套用 <b>確認</b> 動作之類別中的網站的文字與按鈕。
quotaFrame.html	套用 <b>配額</b> 動作之類別中的網站的文字與按鈕。
moreInfo.html	當使用者在封鎖頁面上按一下 <b>詳細資訊</b> 連結時所顯示頁面的內容。

- ◆ **block.html** 包含封鎖訊息最上層框架的文字，其中說明該存取受到限制並列出要求的網站，以及說明該網站為什麼受限制。

## 自訂封鎖訊息

相關主題：

- ◆ [變更訊息框架的大小，第 78 頁](#)
- ◆ [變更封鎖頁面上顯示的標誌，第 79 頁](#)
- ◆ [使用封鎖頁面內容變數，第 79 頁](#)
- ◆ [還原至預設封鎖頁面，第 81 頁](#)

您可以製作預設封鎖頁面檔案的複本，然後使用該複本來自訂使用者會收到的封鎖頁面的最上層框架。

- ◆ 新增有關貴組織網際網路使用政策的資訊。
- ◆ 提供聯絡「人力資源」部或 Websense 管理員取得網際網路使用政策的方法。

1. 瀏覽至 Websense 封鎖頁面目錄：  
<安裝路徑>\BlockPages\en\Default
2. 將封鎖頁面檔案複製到自訂封鎖頁面目錄：  
<安裝路徑>\BlockPages\en\Custom



#### 注意

不要修改 **BlockPages\en\Default** 目錄中的原始封鎖訊息檔案。將它們複製到 **BlockPages\en\Custom** 目錄，然後修改複本。

3. 在文字編輯器 (例如「記事本」或 vi) 中開啓檔案。



#### 警告

請使用純文字編輯器來編輯封鎖訊息檔案。有些 HTML 編輯器會修改 HTML 程式碼，這可能會損毀檔案並導致顯示封鎖訊息時發生問題。

4. 修改文字。檔案中包含指導您執行變更的註解。  
不要修改權杖 (以 \$\* 與 \*\$ 符號括起來) 或 HTML 程式碼的結構。它們可讓 Websense 軟體在封鎖訊息中顯示特定資訊。
5. 儲存檔案。
6. 重新啓動 Filtering Service (如需指示，請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。

## 變更訊息框架的大小

視您要在封鎖訊息中提供的訊息而定，封鎖訊息的預設寬度及最上層框架的高度可能會不恰當。若要變更 **master.html** 檔案中的這些大小參數：

1. 將 **master.html** 從 **Websense\BlockPages\en\Default** 目錄複製到 **Websense\BlockPages\en\Custom**。
2. 在文字編輯器，例如「記事本」或 vi (非 HTML 編輯器) 中開啓檔案。
3. 若要變更訊息框架的寬度，請編輯下列行：  

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

  
視需要變更 **width** 參數的值。
4. 若要使訊息的最上層框架可以捲動，以便顯示其他訊息，請編輯下列行：  

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

  
將 **scrolling** 參數的值變更為 **auto**，即可在訊息文字超過框架高度時顯示捲軸。您也可以變更 **height** 參數的值以變更框架高度。
5. 儲存並關閉檔案。
6. 重新啓動 Filtering Service 以執行變更 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。

## 變更封鎖頁面上顯示的標誌

**master.html** 檔案也包含用來在封鎖頁面上顯示 Websense 標誌的 HTML 程式碼。若要改成顯示貴組織的標誌：

1. 如果尚未複製，將封鎖頁面檔案從 **Websense\BlockPages\en\Default** 目錄複製到 **Websense\BlockPages\en\Custom**。
2. 將含有貴組織標誌的影像檔複製到相同位置。
3. 在文字編輯器，例如「記事本」或 vi (非 HTML 編輯器) 中開啓 **master.html**，並編輯下列行，以貴組織的標誌取代 Websense 標誌：
 

```

```

  - 以含有貴組織標誌的影像檔案名稱取代 **wslogo\_block\_page.png**。
  - 取代 **title** 參數的值，以反映貴組織的名稱。
4. 儲存並關閉檔案。
5. 重新啓動 Filtering Service 以執行變更 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。

## 使用封鎖頁面內容變數

內容變數可控制 HTML 封鎖頁面上顯示的資訊。預設的封鎖頁面程式碼中包含下列變數。

變數名稱	顯示的內容
WS_DATE	目前日期
WS_USERNAME	目前使用者的名稱 (不包括網域名稱)
WS_USERDOMAIN	目前使用者的網域名稱
WS_IPADDR	要求來源電腦的 IP 位址
WS_WORKSTATION	已封鎖之電腦的電腦名稱 (如果未提供名稱，則顯示 IP 位址)

若要使用變數，請在適當 HTML 標記中的 **\$\* \*\$** 符號之間插入變數名稱：

```
<p id="UserName">$*WS_USERNAME*$</p>
```

此處的 *WS\_USERNAME* 是變數。

封鎖訊息程式碼包含其他變數，描述如下。您可能會發現，有些變數對於建構您自己的自訂封鎖訊息很有用。但是，當您在 Websense 定義的封鎖訊息檔案中看到這些變數時，請勿修改它們。因為 Filtering Service 在處理封鎖要求時會使用這些變數，它們必須保留在適當地方。

變數名稱	用途
WS_URL	顯示要求的 URL
WS_BLOCKREASON	顯示為什麼網站被封鎖 (亦即，套用了哪個篩選動作)
WS_ISSECURITY	指出要求的網站是否屬於「安全風險」等級中的任何預設類別。如果為 TRUE，則會顯示安全封鎖頁面。
WS_PWOVERRIDECGIDATA	在封鎖頁面 HTML 程式碼的輸入欄位中，填入有關 <b>密碼覆寫</b> 按鈕的使用資訊
WS_QUOTA_CGIDATA	在封鎖頁面 HTML 程式碼的輸入欄位中，填入有關 <b>使用配額時間</b> 按鈕的使用資訊
WS_PASSWORDOVERRIDE_BEGIN, WS_PASSWORDOVERRIDE_END	表示啟動密碼覆寫功能
WS_MOREINFO	顯示有關要求的網站為什麼被封鎖的詳細資訊 (在按一下 <b>詳細資訊</b> 連結之後顯示)
WS_POLICYINFO	指示管理要求之用戶端的是哪個政策
WS_MOREINFOCGIDATA	將有關 <b>詳細資訊</b> 連結的使用資料傳送到 Filtering Service
WS_QUOTATIME	顯示要求的用戶端剩餘的配額時間量
WS_QUOTAINTERVALTIME	顯示針對要求的用戶端所設定的配額工作階段長度
WS_QUOTABUTTONSTATE	指示是否針對特定要求啟用或停用 <b>使用配額時間</b> 按鈕
WS_SESSIONID	扮演與要求相關聯的內部識別碼
WS_TOPFRAMESIZE	指示由自訂封鎖伺服器 (如果有設定) 傳送之封鎖頁面頂端部分的大小 (以百分比表示)
WS_BLOCKMESSAGE_PAGE	指示封鎖頁面最上層框架所使用的來源
WS_CATEGORY	顯示封鎖之 URL 的類別
WS_CATEGORYID	要求之 URL 類別的唯一識別碼



## 還原至預設封鎖頁面

當您執行自訂的封鎖訊息之後，如果使用者碰到錯誤，您可以還原預設的封鎖訊息，方法如下：

1. 刪除 **Websense\BlockPages\en\Custom** 目錄中的所有檔案。根據預設，Websense 軟體會恢復為使用「預設」目錄中的檔案。
2. 重新啟動 Filtering Service (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。

## 建立替代封鎖訊息

相關主題：

- ◆ [使用封鎖頁面](#)，第 77 頁
- ◆ [自訂封鎖訊息](#)，第 77 頁

您可以建立您自己的 HTML 檔案以提供顯示在封鎖頁面最上層框架中的文字。您可以使用現有的 HTML 檔案、建立全新的替代檔案，或建立 **block.html** 的複本當做範本使用。

- ◆ 分別針對這 3 種通訊協定建立不同的封鎖訊息：HTTP、FTP 及 Gopher。
- ◆ 將檔案存放在 Websense 電腦或您的內部 Web 伺服器上 (請參閱 [使用位於其他電腦上的替代封鎖頁面](#)，第 81 頁)。

在建立替代封鎖訊息檔案時，您必須設定 Websense 軟體以顯示新的訊息 (請參閱 [設定 Websense 篩選設定](#)，第 49 頁)。在此過程中，您可以指定每個可設定的通訊協定分別要使用哪個訊息。

## 使用位於其他電腦上的替代封鎖頁面

相關主題：

- ◆ [使用封鎖頁面](#)，第 77 頁
- ◆ [自訂封鎖訊息](#)，第 77 頁
- ◆ [建立替代封鎖訊息](#)，第 81 頁

除了使用 Websense 封鎖頁面以及自訂最上層框架中的訊息，您還可以建立您自己的 HTML 封鎖頁面，並將它們存放在內部 Web 伺服器上。



### 注意

也可以將封鎖頁面儲存在外部 Web 伺服器上。不過，如果該伺服器托管了 Master Database 中所列的網站，而且該網站屬於封鎖類別，那麼封鎖頁面本身會被封鎖。

有些組織會使用替代的遠端封鎖頁面來隱藏 Websense 伺服器電腦的身份。

遠端封鎖頁面可以是任何 HTML 檔案；它不需要遵循預設 Websense 封鎖頁面的格式。不過，使用此方法建立封鎖頁面會使您無法使用「繼續」、「使用配額時間」及「密碼覆寫」功能；這些功能在 Websense 定義的封鎖頁面（不論預設或自訂）中可以使用。

當檔案放在適當地方時，請編輯 **eimserver.ini** 檔案以指向新的封鎖頁面。

1. 照順序停止 Websense Filtering Service 與 Policy Server 服務 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。
2. 在 Filtering Service 電腦上，瀏覽至 Websense **bin** 目錄 (預設為 \Program Files\Websense\bin 或 /opt/websense/bin)。
3. 建立 **eimserver.ini** 檔案的備份複本，並將它儲存在其他目錄中。
4. 在文字編輯器中開啓 **eimserver.ini** 檔案，並找到 **[WebsenseServer]** 區段 (在檔案的頂端)。
5. 以下列格式輸入存放封鎖頁面之伺服器的主機名稱或 IP 位址：  
UserDefinedBlockPage=http://<主機名稱或 IP 位址>  
必須有 URL 的通訊協定部分 (http://)。
6. 儲存檔案並關閉文字編輯器。
7. 照順序重新啓動 Websense Policy Server 與 Filtering Service。

當服務啓動時，使用者會收到托管於替代電腦上的封鎖頁面。

# 6

## 使用報告評估篩選政策

相關主題：

- ◆ [報告概覽](#)，第 84 頁
- ◆ [簡報報告](#)，第 86 頁
- ◆ [調查報告](#)，第 102 頁
- ◆ [存取自行報告](#)，第 124 頁

Websense Manager 可以提供數個報告工具，用來評估篩選政策的效率 (Websense Manager 和 Websense 報告元件必須安裝在 Windows 伺服器上)。

- ◆ 當您開啓 Websense Manager 時，會首先顯示今天頁面。它會顯示 Websense 軟體的作業狀態，並可顯示自午夜起的網路篩選活動圖表 (請參閱 [今天：自午夜算起的健全度、安全性及數值](#)，第 21 頁)。
- ◆ [記錄](#) 頁面會顯示最多 30 天的網路篩選活動圖表，視記錄資料庫中的資訊量而定。這些圖表不包括今天的活動 (請參閱 [記錄：最後 30 天](#)，第 23 頁)。
- ◆ [簡報報告](#) 與 [調查報告](#) 提供許多選項，可用來產生、自訂及排程報告。如需詳細資訊，請參閱 [報告概覽](#)，第 84 頁。

如果貴組織已在 Linux 伺服器上安裝了 Websense Manager，或選取 Websense Explorer for Linux 報告程式，而不是使用在 Windows 上執行的報告元件，那麼 Websense Manager 就不會顯示報告選項。「今天」和「記錄」頁面上也不會顯示任何網際網路篩選圖表。如需有關安裝該程式及執行報告的詳細資訊，請參閱《[Explorer for Linux 管理員手冊](#)》。

## 報告概覽

相關主題：

- ◆ [使用報告評估篩選政策](#)，第 83 頁
- ◆ [簡報報告](#)，第 86 頁
- ◆ [調查報告](#)，第 102 頁
- ◆ [存取自行報告](#)，第 124 頁

除了「今天」和「記錄」頁面上顯示的圖表之外，Websense 軟體還提供 2 個報告選項：簡報報告和調查報告。



### 注意

在使用委派管理的組織內，有些管理員也許不能存取所有報告功能。請參閱[委派管理](#)，第 205 頁。

**簡報報告**提供報告定義的清單。有些是表格報告，有些則結合了橫條圖和表格。若要產生簡報報告：

1. 從清單中選取報告。
2. 按一下**執行**。
3. 選擇日期範圍。
4. 按一下**立即執行**。

除了產生預先定義的圖表之外，還可複製它們及套用自訂的報告篩選器，用來識別特定用戶端、類別、通訊協定或要包含的動作。將您經常使用的報告定義標記為「我的最愛」，以便於找到。

可將任何簡報報告排程在特定時間執行，或以重複週期方式排程。如需完整的詳細資訊，請參閱[簡報報告](#)，第 86 頁。

**調查報告**可讓您以互動方式瀏覽記錄資料。主頁依照風險等級顯示活動的摘要層級橫條圖。按一下頁面上的不同元件可更新圖表或取得資料的不同檢視。

- ◆ 按一下風險等級名稱，然後選取與該風險等級有關之詳細資訊的較好層級。例如，您可以選取依「法律責任」風險等級的使用者來顯示活動。
- ◆ 按一下結果圖表上的使用者名稱，以檢視有關該使用者的更多詳細資訊。
- ◆ 從[網際網路使用者](#)清單中選取不同選項來以變更摘要橫條圖。
- ◆ 填寫橫條圖正上方的欄位，以便一次顯示兩個層級的資訊。例如，如果要以類別的摘要圖表為開始，可以選取**10**、**使用者**及**5**來顯示前 10 大類別中前 5 位使用者的活動。
- ◆ 按一下橫條或數字可以開啓該項目 (風險等級、類別、使用者或其他) 的細節報告。

- ◆ 按一下**我的最愛報告**以儲存特別有用的報告格式供未來使用，或產生先前儲存的「我的最愛」。

其可能性幾乎沒有限制。如需有關您可用來檢視網際網路使用資料之許多方式的詳細資訊，請參閱[調查報告](#)，[第 102 頁](#)。

## 網際網路瀏覽時間是什麼？

相關主題：

- ◆ [資料庫工作](#)，[第 278 頁](#)
- ◆ [設定網際網路瀏覽時間選項](#)，[第 282 頁](#)

您可以根據網際網路瀏覽時間 (IBT) 來產生簡報報告和調查報告，網際網路瀏覽時間指的是個人在存取網站時花費的時間。沒有任何軟體程式可以識別出從一開啓特定網頁起的確切實際檢視時間。某人可能開啓了一個網站，檢視了幾秒鐘，然後在還沒要求另一個網站之前就去接了辦公電話。另一個人可能花了數分鐘詳細閱讀每個網站，然後才移到下一個網站。

Websense 軟體包含了記錄資料庫工作，以便使用基於特定可設定值的方程式來計算網際網路瀏覽時間 (IBT)。此工作每天執行一次，因此瀏覽時間資訊可能比實際記錄資料要延遲。

對於瀏覽器時間計算而言，使用者開啓瀏覽器時網際網路工作階段即開始。只要使用者至少每 3 分鐘要求其他網站，計算便會繼續 (此預設的閱讀時間臨界值是可設定的)。

如果使用者超過 3 分鐘過後才要求其他網站，網際網路工作階段便會結束。Websense 軟體會計算工作階段總時間，總時間從第一個要求的時間開始，至最後一個要求之後 3 分鐘為止。

如果使用者在超過 3 分鐘之後執行其他要求，新的工作階段便會開始。一般而言，使用者每天的瀏覽時間是由多個工作階段所組成的。

如需有關網際網路瀏覽時間工作及相關配置選項的詳細資訊，請參閱[資料庫工作](#)，[第 278 頁](#)和[設定網際網路瀏覽時間選項](#)，[第 282 頁](#)。

## 簡報報告

相關主題：

- ◆ [複製簡報報告](#)，第 88 頁
- ◆ [複製簡報報告](#)，第 88 頁
- ◆ [使用我的最愛](#)，第 94 頁
- ◆ [產生簡報報告](#)，第 95 頁
- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [檢視排程工作清單](#)，第 100 頁

**報告 > 簡報報告** 頁面會顯示預先定義的圖表和表格報告的清單，每個報告都顯示來自記錄資料庫的特定資訊 ( 請參閱 [記錄資料庫簡介](#)，第 277 頁 )。從這個「報告目錄」選取報告，以顯示簡短說明。

可複製預先定義的報告並自訂報告篩選器，以指定要包括的用戶端、類別、通訊協定及動作。經常用到的報告可標記為「我的最愛」，以協助您更快找到它們。

現在執行任何報告，或在延遲或定期的基礎上排程執行所選報告。選取輸出格式，並將排程報告發佈給所選收件人群組。

如果直接從「簡報報告」頁面以 HTML 格式產生報告，當您移動到其他頁面時，將無法儲存報告。如果以 PDF 或 XLS 格式產生並立即檢視報告，當您關閉檢視程式 (Adobe Reader 或 Microsoft Excel)，將無法儲存報告。

或者，也可選取儲存 PDF 或 XLS 檔案而不是立即顯示它，或使用檢視程式中的「儲存」選項。在這些情況下，確定定期刪除或移動報告檔案以避免出現磁碟空間問題。

排程報告會自動儲存在下列目錄：

< 安裝路徑 > \ReportingOutput

預設安裝路徑為 C:\Program Files\WebSense。

當排程的簡報報告已經執行時，報告檔案會以名為 **presentationreport\_0** 的電子郵件附件傳送給收件人。檔案名稱尾端的數字根據附加的報告數量遞增。請注意，附件的名稱與儲存在 ReportingOutput 目錄中的檔案名稱是不一樣的。若要找到此目錄中的特定報告，搜尋排程工作執行當天所建立的檔案。

報告會在 15 天之後自動從 ReportingOutput 目錄中刪除。如果想要保留報告較長時間，可將它們包括在備份例行程序中，或排程它們以及將用電子郵件傳送的檔案儲存在允許長時間儲存的位置。

視每天產生的報告數量而定，報告檔案可能會佔磁碟空間上的可觀空間。請確定 WebSense Manager 電腦上有足夠多的可用磁碟空間。如果在檔案自動刪除之前 ReportingOutput 目錄已經增長得太大，可以手動刪除檔案。

Websense 軟體會以您選的格式產生報告：PDF (Adobe Reader)、XLS (Microsoft Excel) 或 HTML。如果選擇 HTML 格式，報告會顯示在 Websense Manager 控制窗格中。這些報告將無法列印或儲存至檔案。若要列印或將報告儲存至檔案，請選擇 PDF 或 XLS 輸出格式。

如果選擇 PDF 或 XLS 格式，會有選項讓您將報告檔案儲存至磁碟或以單獨的視窗顯示。



### 重要

若要以 PDF 格式顯示簡報報告，必須在用來存取 Websense Manager 的電腦上安裝 Adobe Reader v7.0 或更新版本。

若要以 XLS 格式顯示簡報報告，必須在用來存取 Websense Manager 的電腦上安裝 Microsoft Excel 2003 或更新版本。

在「簡報報告」頁面上，瀏覽「報告目錄」並選取想要的報告。然後，使用頁面上的控制項來執行報告、建立可自訂報告篩選器的報告複本，以及其他更多操作。

按鈕	動作
只顯示我的最愛	選取此選項可限制「報告目錄」只顯示標記為「我的最愛」的報告。 取消選取此選項可還原完整的報告清單。
編輯報告篩選器	此選項只有在已選取預先定義的報告時才可使用，它可讓您選取要包括在報告中的特定類別、通訊協定、使用者及動作。請參閱 <a href="#">複製簡報報告</a> ，第 88 頁。
複製	製作所選報告的複本並將其新增至「報告目錄」做為自訂報告。請參閱 <a href="#">複製簡報報告</a> ，第 88 頁。 選取自訂報告，然後按一下 <b>編輯報告篩選器</b> 為其設定具體參數。
我的最愛	將選擇的報告標記為「我的最愛」，或移除「我的最愛」指定。請參閱 <a href="#">使用我的最愛</a> ，第 94 頁。 「報告類別」會在標記為「我的最愛」的所有報告的報告名稱旁邊顯示星號。使用 <b>只顯示我的最愛</b> 核取方塊可控制將哪些報告要顯示在「報告目錄」中。
刪除	從「報告目錄」中刪除所選報告複本。不能刪除與軟體一同安裝的預先定義的報告。 如果刪除的報告出現在任何排程工作中，那麼該工作會繼續產生那份報告。
執行	在設定了日期範圍和輸出格式之後產生所選報告。請參閱 <a href="#">產生簡報報告</a> ，第 95 頁。 若要控制自訂報告 (預先定義報告的複本) 的其他方面，請參閱 <a href="#">複製簡報報告</a> ，第 88 頁。 若要將報告排程在不同時間執行或以重複的排程執行，按一下「排程器」。

頁面上方的按鈕提供簡報報告的額外選項。

按鈕	動作
工作佇列	顯示列出已建立之排程工作的頁面以及每個工作的狀態。請參閱 <a href="#">檢視排程工作清單</a> ，第 100 頁。
排程器	定義要在特定時間執行或以重複的排程執行的包含一或多個報告的工作。請參閱 <a href="#">排程簡報報告</a> ，第 96 頁。

## 複製簡報報告

相關主題：

- ◆ [複製簡報報告](#)，第 88 頁
- ◆ [簡報報告](#)，第 86 頁

一開始，**簡報報告**頁面會顯示「報告目錄」，列出與軟體一起安裝的所有預先定義的報告。可透過選取報告然後按一下「執行」，來產生特定時段的任意報告。

這些預先定義的報告也可以做為範本使用，進行複製以便建立自訂的報告篩選器。建立報告篩選器可控制從複本產生報告時，要包括的元素，例如使用者、類別、通訊協定及動作。

複製報告及編輯報告篩選器之後，可複製新的報告以便根據該複本來建立變化。

1. 在「報告目錄」中選取任意報告。
2. 按一下**複製**。  
「報告目錄」中將顯示報告名稱的複本，並加上一個代碼來表示其為複本。
3. 在「報告目錄」中選取複本，然後按一下**編輯報告篩選器**以修改報告的元素。請參閱[複製簡報報告](#)，第 88 頁。

## 定義報告篩選器

相關主題：

- ◆ [複製簡報報告](#)，第 88 頁
- ◆ [產生簡報報告](#)，第 95 頁

報告篩選器用於控制報告中要包括的資訊。例如，您可以選擇將報告限制在所選用戶端、類別、風險等級或通訊協定，或者甚至是所選篩選動作(允許、封鎖等等)。也可為「報告目錄」中的項目賦予新名稱和說明、指定要顯示的自訂標誌以及透過報告篩選器設定其他一般選項。



**注意**

若要使用自訂標誌，必須在定義報告篩選器之前做些準備工作。必須以支援的圖形格式建立需要的圖形，並將檔案放在適當位置。請參閱[自訂報告標誌](#)，第 93 頁。

篩選器中可用的具體選項取決於所選報告。例如，如果選取了群組資訊報告 (例如「依要求排名最高的封鎖群組」)，可控制報告中顯示的群組，但不能選擇個別使用者。

不能變更預先定義報告的篩選器。可編輯預先定義報告的複本的篩選器：

1. 在「報告目錄」中選取報告。
  - 如果「編輯報告篩選器」是停用的，則繼續執行步驟 2。
  - 如果「編輯報告篩選器」是啓用的，則跳到步驟 3。
2. 按一下**複製**得到可自訂的複本。
  - 「報告目錄」中將顯示報告名稱的複本，並加上一個代碼來表示其為複本。
3. 按一下**編輯報告篩選器**按鈕。
  - 將開啓「報告篩選器」頁面，頁面中有可管理報告的不同元素的單獨標籤。在每個標籤上選取想要的項目，然後按**下一步**移動到下一個標籤。如需詳細指示，請參閱：
    - [選取報告的用戶端](#)，第 89 頁
    - [選取報告的類別](#)，第 90 頁
    - [選取報告的通訊協定](#)，第 91 頁
    - [選取報告的動作](#)，第 92 頁
    - [設定報告選項](#)，第 92 頁
4. 在**確認**標籤上，除了儲存報告篩選器之外，還可選擇是否要執行報告或排程報告。請參閱[確認報告篩選器定義](#)，第 94 頁。

## 選取報告的用戶端

相關主題：

- ◆ [選取報告的類別](#)，第 90 頁
- ◆ [選取報告的通訊協定](#)，第 91 頁
- ◆ [選取報告的動作](#)，第 92 頁
- ◆ [設定報告選項](#)，第 92 頁
- ◆ [確認報告篩選器定義](#)，第 94 頁

「簡報報告」>「報告篩選器」頁面上的**用戶端**標籤用於控制要包括在報告中的用戶端。每個報告只能選取一種用戶端類型。例如，對於相同報告，不能一些選取使用者，一些選取群組。

報告定義指定了特定的用戶端類型之後，可以選擇該類型的用戶端或代表更大群組的用戶端。例如，如果您根據「依要求排名最高的封鎖群組」來定義報告的篩選器，則可為報告選取群組、網域或組織單位，但不能選取個別使用者。

如果想要執行所有相關用戶端的報告，則不需要在此標籤上選取任何項目。

1. 從下拉式清單中選取用戶端類型。
2. 從**限制搜尋**清單設定搜尋結果的數目上限。

記錄資料庫中可能有大量使用者、群組或網域，這取決於貴組織中的流量。此選項管理結果清單的長度，以及顯示搜尋結果所需的時間。

3. 輸入一或多個字元以便搜尋，然後按一下**搜尋**。

使用星號(\*)做為萬用字元，表示缺少的字元。例如，J\*n 可能傳回 Jackson、Jan、Jason、Jon、John 等等。

小心定義搜尋字串，以確保為限制搜尋而選取的數目中包含所有想要的結果。

4. 結果清單中會反白顯示一或多個項目，然後按一下向右箭頭按鈕(>) 將它們移至**已選取**清單。
5. 視需要重複步驟 2-4 以進行其他搜尋並新增更多用戶端至「已選取」清單。
6. 完成選取之後，按**下一步**開啓「類別」標籤。請參閱[選取報告的類別](#)，第 90 頁。

## 選取報告的類別

相關主題：

- ◆ [選取報告的用戶端](#)，第 89 頁
- ◆ [選取報告的通訊協定](#)，第 91 頁
- ◆ [選取報告的動作](#)，第 92 頁
- ◆ [設定報告選項](#)，第 92 頁
- ◆ [確認報告篩選器定義](#)，第 94 頁

「簡報報告」>「報告篩選器」頁面上的**類別**標籤用於根據類別或風險等級，控制要包括在報告中的資訊。請參閱[風險等級](#)，第 36 頁。

如果想要執行所有相關類別或風險等級的報告，則不需要在此標籤上選取任何項目。

1. 選取分類：**類別**或**風險等級**。

展開上層類別以便顯示其下層類別。展開風險等級以便檢視目前指派到該風險等級的類別清單。

如果相關報告是針對特定風險等級，則只能選取相關風險等級和它所代表的類別。



### 注意

如果針對報告中命名的風險等級選取了類別的子集合，請考慮修改報告標題以反映您的選擇。

2. 標記每個類別或風險等級的核取方塊，以便執行報告。  
使用清單下方的**全選**和**全部清除**按鈕，使所需的個別選擇數目減至最小。
3. 按一下向右箭頭按鈕 (>) 將您的選擇移至**已選取**清單。  
標記了風險等級之後，按一下向右箭頭會將所有相關聯的類別放進「已選取」清單中。
4. 完成所有選擇之後，按下一步開啓「通訊協定」標籤。請參閱[選取報告的通訊協定](#)，第 91 頁。

## 選取報告的通訊協定

相關主題：

- ◆ [選取報告的用戶端](#)，第 89 頁
- ◆ [選取報告的類別](#)，第 90 頁
- ◆ [選取報告的動作](#)，第 92 頁
- ◆ [設定報告選項](#)，第 92 頁
- ◆ [確認報告篩選器定義](#)，第 94 頁

「簡報報告」>「報告篩選器」頁面上的**通訊協定**標籤用於控制要包括在報告中的通訊協定。

如果想要執行所有相關通訊協定的報告，則不需要在此標籤上選取任何項目。

1. 使用群組名稱旁的圖示展開及摺疊通訊協定群組。
2. 標記每個通訊協定的核取方塊，以便執行報告。  
使用清單下方的**全選**和**全部清除**按鈕，使所需的個別選擇數目減至最小。
3. 按一下向右箭頭按鈕 (>) 將您的選擇移至**已選取**清單。
4. 完成所有選擇之後，按下一步開啓「動作」標籤。請參閱[選取報告的動作](#)，第 92 頁。

## 選取報告的動作

相關主題：

- ◆ [選取報告的用戶端](#)，第 89 頁
- ◆ [選取報告的類別](#)，第 90 頁
- ◆ [選取報告的通訊協定](#)，第 91 頁
- ◆ [設定報告選項](#)，第 92 頁
- ◆ [確認報告篩選器定義](#)，第 94 頁

「簡報報告」>「報告篩選器」頁面上的**動作**標籤用於控制要包括在報告中的精確篩選動作，例如依限制的存取篩選器允許、依配額封鎖。如果報告指定了特定的動作類型（例如「已封鎖」），則對於該報告而言，您將受限於所選類型的動作。

如果想要執行所有相關動作的報告，則不需要在此標籤上選取任何項目。

1. 使用群組名稱旁的圖示展開及摺疊動作群組。
2. 標記每個動作的核取方塊，以便執行報告。

使用清單下方的**全選**和**全部清除**按鈕，使所需的個別選擇數目減至最小。

3. 按一下向右箭頭按鈕 (>) 將您的選擇移至**已選取**清單。
4. 完成所有選擇之後，按**下一步**開啓「選項」標籤。請參閱[設定報告選項](#)，第 92 頁。

## 設定報告選項

相關主題：

- ◆ [自訂報告標誌](#)，第 93 頁
- ◆ [選取報告的用戶端](#)，第 89 頁
- ◆ [選取報告的類別](#)，第 90 頁
- ◆ [選取報告的通訊協定](#)，第 91 頁
- ◆ [選取報告的動作](#)，第 92 頁
- ◆ [設定報告選項](#)，第 92 頁
- ◆ [確認報告篩選器定義](#)，第 94 頁

使用「簡報報告」>「編輯報告篩選器」頁面上的**選項**標籤設定報告的數個方面。

1. 修改「報告目錄」中顯示的**報告目錄名稱**。名稱最長為 85 個字元。  
此名稱不會顯示在報告本身上；它僅用來在「報告目錄」中識別報告格式與篩選器的唯一組合。

2. 修改顯示在報告中的**報告標題**。標題最長為 85 個字元。
3. 修改「報告目錄」中顯示的**說明**。說明最長為 336 個字元。  
說明應該要有助於在「報告目錄」中識別這個報告格式與篩選器的唯一組合。
4. 選取要顯示報告中的標誌。  
將列出相關目錄中所有支援的影像檔。請參閱[自訂報告標誌](#)，第 93 頁。
5. 標記**儲存到我的最愛**核取方塊，將報告列為「我的最愛」。  
「報告目錄」會在「我的最愛」報告旁邊顯示星號。可選取「報告目錄」頁面上的**只顯示我的最愛**來減少列出的報告數目，從而更快移動到特定報告。
6. 標記**只顯示前幾名**核取方塊，然後輸入 1 到 20 的數字來限制報告的項目數目。  
只有當所選報告的格式為「前 N 名」報告時，此選項才會顯示，前 N 名報告的設計目的是為了顯示有限的項目數目。所限制的項目取決於報告。例如，對於「已造訪之排名最高的類別」報告，此項目決定著要報告的類別數目。
7. 完成所有項目和選擇之後，按下一步開啓「確認」標籤。請參閱[確認報告篩選器定義](#)，第 94 頁。

## 自訂報告標誌

預先定義的簡報報告會在左上角顯示 Websense 標誌。複製預先定義的報告並定義其報告篩選器時，可選擇不同的標誌。

1. 以下列格式其中之一建立影像檔：

- |         |         |
|---------|---------|
| • .bmp  | • .jpg  |
| • .gif  | • .jpeg |
| • .jfif | • .png  |
| • .jpe  | • .tiff |

2. 影像檔案名稱 (包括副檔名) 可使用最多 25 個字元。
3. 將影像檔放在下列目錄中：

< 安裝路徑 > \Manager\ReportingTemplates\images

預設安裝路徑為 C:\Program Files\WebSense。

此目錄中所有支援的影像檔會自動顯示在「報告篩選器」頁面之「選項」標籤上的下拉式清單中。影像會自動調整大小以符合放置標誌的空間 (請參閱[設定報告選項](#)，第 92 頁)。



### 注意

不要從此目錄中移除報告篩選器中的作用中影像。如果缺少指定的標誌檔案，將無法產生報告。

## 確認報告篩選器定義

相關主題：

- ◆ [選取報告的用戶端](#)，第 89 頁
- ◆ [選取報告的類別](#)，第 90 頁
- ◆ [選取報告的通訊協定](#)，第 91 頁
- ◆ [選取報告的動作](#)，第 92 頁
- ◆ [設定報告選項](#)，第 92 頁

「簡報報告」>「報告篩選器」頁面上的**確認**標籤可顯示將在「報告目錄」中出現的名稱與說明，而且可讓您選擇如何進行。

1. 檢閱**名稱**和**說明**。

如需任何變更，按一下**上一頁**回到「選項」標籤進行變更 (請參閱[設定報告選項](#)，第 92 頁)。

2. 指示您想要如何進行：

選項	說明
儲存	儲存報告篩選器並返回「報告目錄」。請參閱 <a href="#">簡報報告</a> ，第 86 頁。
儲存並執行	儲存報告篩選器並開啓「執行報告」頁面。請參閱 <a href="#">產生簡報報告</a> ，第 95 頁。
儲存及排程	儲存報告篩選器並開啓「排程報告」頁面。請參閱 <a href="#">排程簡報報告</a> ，第 96 頁。

3. 按一下**完成**執行步驟 2 所做的選擇。

## 使用我的最愛

相關主題：

- ◆ [簡報報告](#)，第 86 頁
- ◆ [產生簡報報告](#)，第 95 頁
- ◆ [排程簡報報告](#)，第 96 頁

您可以將任何簡報報告 (不論是預先定義的還是自訂的) 標記為「我的最愛」。可使用此選項來識別最常產生的報告及想要在「報告目錄」中快速找到的報告。

1. 在[簡報報告](#)頁面上，反白顯示經常產生的報告，或想要能快速找到的報告。

2. 按一下**我的最愛**。

在清單中「我的最愛」報告名稱旁邊會出現星號，從而讓您在顯示所有報告時快速識別它們。

3. 標記「報告目錄」上方的**只顯示我的最愛**核取方塊，可限制清單只顯示標記為「我的最愛」報告。清除此核取方塊可還原完整的報告清單。

如果需求改變且「我的最愛」報告不再經常使用，可以移除「我的最愛」指定。

1. 反白顯示有「我的最愛」星號的報告。

2. 按一下**我的最愛**。

星號會從「報告目錄」中該報告名稱中移除。如果選擇**只顯示我的最愛**，報告就不會出現在清單中。

## 產生簡報報告

相關主題：

- ◆ [簡報報告](#)，第 86 頁
- ◆ [排程簡報報告](#)，第 96 頁

立即產生一個報告，包括如下所示的幾個步驟。



### 注意

在產生 PDF 格式的報告之前，確認用來存取 Websense Manager 的電腦上已安裝 Adobe Reader v7.0 或更新版本。

在產生 XLS 格式的報告之前，確認用來存取 Websense Manager 的電腦上已安裝 Microsoft Excel 2003 或更新版本。

如果沒有安裝適當的軟體，可以選擇儲存檔案。

若要建立具有一或多個報告的工作，以便執行一次，或使用簡報報告排程功能在重複的週期上執行，請參閱[排程簡報報告](#)，第 96 頁。

1. 在**簡報報告**頁面上，反白顯示「報告目錄」樹狀結構中的報告，然後按一下**執行**。
2. 選取報告資料的**開始日期**與**結束日期**。
3. 選取報告的**輸出格式**。

格式	說明
PDF	可攜式文件格式。PDF 檔案需使用 Adobe Reader 檢視。

格式	說明
HTML	超文字標記語言。HTML 可以直接在 Internet Explorer 或 Firefox 瀏覽器中檢視。
XLS	Excel 試算表。XLS 檔案需使用 Microsoft Excel 檢視。

4. 如果選取了**前 N 名**報告，請選擇要進行報告的項目數。
5. 按一下**執行**。

HTML 報告會顯示在內容窗格中。如果選取了 PDF 或 XLS 輸出，可以選擇是否要在單獨的視窗中開啓報告或將報告儲存到磁碟。

6. 若要列印報告，使用顯示報告之程式的列印選項。

爲了獲得最佳結果，請產生 PDF 或 XLS 輸出以便列印。然後，分別使用 Adobe Reader 或 Microsoft Excel 中的列印選項。

可使用 Adobe Reader 或 Microsoft Excel 中的「儲存」功能，儲存以 PDF 或 XLS 格式輸出的報告。

## 排程簡報報告

相關主題：

- ◆ [簡報報告](#)，第 86 頁
- ◆ [產生簡報報告](#)，第 95 頁
- ◆ [檢視排程工作清單](#)，第 100 頁
- ◆ [複製簡報報告](#)，第 88 頁

可以視需要執行簡報報告，也可以使用**簡報報告 > 排程器**頁面建立工作以定義執行一或多個報告的排程。

使用排程工作所建立的報告可透過電子郵件發佈給一或多個收件人。建立排程工作時，請考量電子郵件伺服器是否可以處理報告檔案附件的大小與數量。

若要存取「排程器」：

- ◆ 按一下「簡報報告」頁面頂端的**排程器**按鈕(在「報告目錄」上方)。
- ◆ 爲報告新增或編輯報告篩選器時，請選擇「確認」標籤中的**儲存及排程**，然後按一下**完成**(請參閱[複製簡報報告](#)，第 88 頁)。
- ◆ 按一下「工作佇列」頁面上的工作名稱連結以編輯工作。
- ◆ 按一下「工作佇列」頁面上的**新增**以建立新工作。



「排程器」頁面包含數個標籤，可用來選取報告以便執行報告或排程執行。如需詳細指示，請參閱：

- ◆ [設定排程](#)，第 97 頁
- ◆ [選取要排程的報告](#)，第 98 頁
- ◆ [選取輸出選項](#)，第 99 頁
- ◆ [設定日期範圍](#)，第 99 頁
- ◆ [選取輸出選項](#)，第 99 頁

建立工作之後，可以檢視工作清單，其中會顯示工作的狀態及其他有用資訊。請參閱 [檢視排程工作清單](#)，第 100 頁。

## 設定排程

相關主題：

- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [選取要排程的報告](#)，第 98 頁
- ◆ [選取輸出選項](#)，第 99 頁
- ◆ [設定日期範圍](#)，第 99 頁

在「簡報報告」>「排程」頁面的**排程**標籤上，定義一次執行報告工作或以重複的週期執行。



### 注意

建議將報告工作排程在不同日期或不同時間，以避免記錄資料庫超載及降低記錄與互動式報告的效能。

1. 輸入可唯一識別此排程工作的**工作名稱**。
2. 選取工作的**重複執行模式**和**重複執行選項**。可用的特定選項取決於所選模式。

模式	選項
一次	輸入要執行工作的確切日期，或按一下圖示從行事曆中選取。
每天	沒有其他重複執行選項可用。
每週	標記一週內要執行工作那天的核取方塊。
每月	輸入一個月期間要執行工作的日期。日期必須是介於 1 至 31 之間的數字，而且必須以逗號分隔 (1,10,20)。 若要在每個月的連續日期中執行工作，輸入開始與結束日期，並以連字號分隔 (3-5)。

3. 在**排程時間**下設定要執行工作的開始時間。  
工作會根據執行 **Websense Manager** 之電腦上的時間而開始。



**注意**

若要從今天開始產生排程報告，選取稍晚的時間，讓您在足夠時間在開始時間之前完成工作定義。

4. 在**排程周期**下選取工作的開始日期與結束日期。

選項	說明
無結束日期	工作會根據已建立的排程無限期地繼續執行。 若要在未來某個時間終止工作，編輯或刪除工作。請參閱 <a href="#">檢視排程工作清單</a> ，第 100 頁。
在此次數後結束	選取執行工作的次數。達到該數字之後，工作將不再執行，但它會保留在「工作佇列」中，直到您刪除它。請參閱 <a href="#">檢視排程工作清單</a> ，第 100 頁。
在此日期前結束	設定工作停止執行的日期。在當天或當天之後，都不會執行工作。

5. 按下一步以開啓「報告」標籤。請參閱 [選取要排程的報告](#)，第 98 頁。

## 選取要排程的報告

相關主題：

- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [設定排程](#)，第 97 頁
- ◆ [選取輸出選項](#)，第 99 頁
- ◆ [設定日期範圍](#)，第 99 頁

使用「簡報報告」>「排程器」頁面上的**選取報告**標籤來選取工作報告。

1. 在「報告目錄」樹狀結構中反白顯示此工作的報告。
2. 按一下向右箭頭(>)按鈕，將該報告移至**已選取**清單。
3. 重複步驟 1 和 2，直到此工作的所有報告都顯示在**已選取**清單中。
4. 按下一步以開啓「日期範圍」標籤。請參閱 [設定日期範圍](#)，第 99 頁。

## 設定日期範圍

相關主題：

- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [設定排程](#)，第 97 頁
- ◆ [選取要排程的報告](#)，第 98 頁
- ◆ [選取輸出選項](#)，第 99 頁

使用「簡報報告」>「排程器」頁面上的**日期範圍**標籤來設定工作的日期範圍。可用選項取決於針對**日期範圍**所做的選擇。

日期範圍	說明
所有日期	包括記錄資料庫中可用之所有日期的報告。無需設定其他項目。 當此選項用於重複的工作時，單獨執行的報告中可能有重複的資訊。
特定日期	針對此工作中的報告選擇確切的開始日期 ( <b>從</b> ) 與結束 ( <b>到</b> ) 日期。 此選項非常適合僅執行一次的工作。若針對重複的排程選擇此選項，會造成重複的報告。
相對日期	使用下拉式清單選取報告的時段數字 (本、最後、最後 2 等等) 以及時段的類型 (天、週或月)。例如，工作可以涵蓋「最後 2 週」或「本月」 週，代表的是行事曆週，從星期日到星期六。月，代表的是行事曆月。例如，「本週」會產生從星期天到今天的報告；「本月」會產生從本月第一天到今天的報告；「最後週」會產生前一個星期天到星期六的報告；如此等等。 此選項非常適合以重複排程執行的工作。它可讓您管理每個報告中要顯示多少資料，並將單獨執行的報告中的重複資料減到最少。

設定工作的日期範圍之後，按下一步以顯示「輸出」標籤。請參閱[選取輸出選項](#)，第 99 頁。

## 選取輸出選項

相關主題：

- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [設定排程](#)，第 97 頁
- ◆ [選取要排程的報告](#)，第 98 頁
- ◆ [設定日期範圍](#)，第 99 頁

選取了工作報告之後，使用**輸出**標籤來選擇輸出格式和發佈選項。

1. 選取已完成報告的檔案格式。

格式	說明
PDF	可攜式文件格式。收件人必須擁有 Adobe Reader v7.0 或更新版本才能檢視PDF 報告。
XLS	Excel 試算表。收件人必須擁有 Microsoft Excel 2003 或更新版本才能檢視 XLS 報告。

2. 輸入電子郵件位址以便發佈報告。  
在單獨的行中輸入每個位址。
3. 若有需要，可標記**自訂電子郵件的主旨與內文**核取方塊。然後，爲此工作的發佈電子郵件輸入自訂的**主旨與內文**。
4. 按一下**儲存工作**以儲存及執行工作定義，並顯示「工作佇列」頁面。
5. 檢閱此工作及其他排程工作。請參閱[檢視排程工作清單](#)，第 100 頁。

## 檢視排程工作清單

相關主題：

- ◆ [簡報報告](#)，第 86 頁
- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [選取輸出選項](#)，第 99 頁
- ◆ [排程調查報告](#)，第 120 頁

**簡報報告 > 工作佇列**頁面會列出針對簡報報告所建立的排程工作。此清單會提供每個工作的狀態，以及該工作的基本資訊，例如執行頻率。可從此頁面新增與刪除排程工作、暫時停止工作及執行其他操作。

(若要檢閱調查報告的排程工作，請參閱[管理排程的調查報告工作](#)，第 122 頁。)

清單會提供每個報告的下列資訊。

欄位	說明
工作名稱	工作建立時所指派的名稱。
狀態	下列其中之一： <ul style="list-style-type: none"> <li>• 「已啟動」表示根據已建立的重複執行模式執行的工作。</li> <li>• 「已停用」表示未啟動且未執行的工作。</li> </ul>
重複執行	針對此工作設定的重複執行模式 (一次、每天、每週、每月)。

欄位	說明
記錄	按一下 <a href="#">詳細資訊</a> 連接可開啓所選工作的「工作記錄」頁面。請參閱 <a href="#">檢視工作記錄</a> ，第 101 頁。
下一個排程	下次執行的日期與時間。
擁有者	排程此工作之管理員的使用者名稱。

使用頁面上的選項來管理工作。有些按鈕需要首先標記每個工作名稱旁的核取方塊以便將其包含在內。

選項	說明
工作名稱連結	開啓「排程器」頁面編輯工作定義。請參閱 <a href="#">排程簡報報告</a> ，第 96 頁。
新增工作	開啓「排程器」頁面定義新工作。請參閱 <a href="#">排程簡報報告</a> ，第 96 頁。
刪除	從「工作佇列」中刪除清單中已勾選的所有工作。工作刪除之後便無法還原。 若要暫時停止執行特定工作，使用 <b>停用</b> 按鈕。
立即執行	立即開始執行清單中已勾選的工作。這是定期排程執行的附加選項。
啓動	重新啓動清單中勾選的已停用工作。工作會根據已建立的排程開始執行。
停用	停止繼續執行清單中勾選的已啓用工作。使用此選項暫時停止未來可能想要還原的工作。

## 檢視工作記錄

相關主題：

- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [檢視排程工作清單](#)，第 100 頁

使用[簡報報告](#) > [工作佇列](#) > [工作記錄](#)頁面來檢視最近嘗試執行的所選工作的相關資訊。頁面會分別列出每個報告，提供下列資訊。

欄位	說明
報告名稱	報告上列印的標題。
開始日期	報告開始執行的日期與時間。
結束日期	報告完成的日期與時間。
狀態	報告成功與否的指標。
訊息	有關工作的相關訊息，例如報告是否成功以電子郵件寄出。

## 調查報告

相關主題：

- ◆ [摘要報告](#)，第 103 頁
- ◆ [多層級摘要報告](#)，第 106 頁
- ◆ [靈活的細節報告](#)，第 107 頁
- ◆ [使用者活動細節報告](#)，第 111 頁
- ◆ [標準報告](#)，第 116 頁
- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [排程調查報告](#)，第 120 頁
- ◆ [異常值報告](#)，第 122 頁
- ◆ [輸出至檔案](#)，第 123 頁
- ◆ [資料庫連接與報告預設值](#)，第 287 頁



使用**報告** > **調查報告**頁面以互動方式分析網際網路篩選活動。

一開始，「調查報告」主頁上會依照風險等級顯示活動的摘要報告。使用摘要報告時，透過按一下可用的連結與元素來進行檢視，瀏覽感興趣的區域並一般瞭解有關貴組織網際網路的使用情況。請參閱[摘要報告](#)，第 103 頁。

多層級的摘要報告 (請參閱[多層級摘要報告](#)，第 106 頁) 與靈活的細節報告 (請參閱[靈活的細節報告](#)，第 107 頁) 可讓您從不同角度分析資訊。

可從頁面頂端的連結來存取其他報告檢視與調查報告功能。有關連結的清單及連結所存取的功能，請參閱下表 (並非所有頁面上的所有連結都可使用)。

選項	動作
使用者每日 / 每月活動 細節	顯示對話方塊，讓您定義特定使用者活動的報告，涵蓋一天或一個月。如需詳細資訊，請參閱 <a href="#">使用者活動細節報告</a> ，第 111 頁。
標準報告	顯示預先定義的報告清單，讓您可快速檢視特定的資料組合。請參閱 <a href="#">標準報告</a> ，第 116 頁。
我的最愛報告	可讓您將目前報告儲存到「我的最愛」，並顯視可產生或排程的現有「我的最愛」清單。請參閱 <a href="#">我的最愛調查報告</a> ，第 118 頁。
工作佇列	顯示排程的調查報告工作的清單。請參閱 <a href="#">排程調查報告</a> ，第 120 頁。
異常值	顯示網際網路使用情況與平均值有巨大差異的報告。請參閱 <a href="#">異常值報告</a> ，第 122 頁。

選項	動作
選項	顯示用來針對報告選取不同記錄資料庫的頁面。「選項」頁面也可自訂特定的報告功能，例如在摘要報告中最初顯示的時段及細節報告的預設欄位。請參閱 <a href="#">資料庫連接與報告預設值</a> ，第 287 頁。
	按一下此按鈕 (位於「搜尋」欄位右方)，可將目前報告匯出到與 Microsoft Excel 相容的試算表檔案。 系統會提示您開啓或儲存檔案。若要開啓檔案，則必須安裝 Microsoft Excel 2003 或更新版本。請參閱 <a href="#">輸出至檔案</a> ，第 123 頁。
	按一下此按鈕 (位於「搜尋」欄位右方)，可將目前報告匯出到與 Adobe Reader 相容的 PDF 檔案。 系統會提示您開啓或儲存檔案。若要開啓檔案，則必須安裝 Adobe Reader 7.0 版或更新版本。請參閱 <a href="#">輸出至檔案</a> ，第 123 頁。

請記住，報告受限於記錄資料庫中記錄的資訊。如果停用記錄使用者名稱、IP 位址或所選類別 (請參閱[設定用於記錄的 Filtering Service](#)，第 265 頁)，這些資訊將不會包含在內。同樣地，如果停用記錄特定通訊協定 (請參閱[編輯通訊協定篩選器](#)，第 46 頁)，針對那些通訊協定的要求就不可用。如果希望報告同時顯示網域名稱 (www.domain.com) 與網域中特定頁面的路徑 (/products/productA)，則必須記錄完整的 URL (請參閱[設定完整 URL 記錄](#)，第 281 頁)。

Websense 調查報告受限於執行 Websense Manager 之電腦的處理器與可用記憶體，以及某些網路資源。有些大型報告可能要花費很長時間才能產生。進度訊息包含將報告儲存到「我的最愛」的選項，因此可將它排程在其他時間執行。請參閱[排程調查報告](#)，第 120 頁。

## 摘要報告

相關主題：

- ◆ [多層級摘要報告](#)，第 106 頁
- ◆ [靈活的細節報告](#)，第 107 頁
- ◆ [使用者活動細節報告](#)，第 111 頁
- ◆ [標準報告](#)，第 116 頁
- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [排程調查報告](#)，第 120 頁
- ◆ [異常值報告](#)，第 122 頁
- ◆ [輸出至檔案](#)，第 123 頁

一開始，研究報告頁面會依風險等級提供所有使用者的使用情況摘要報告，顯示來自記錄資料庫的當天活動。此起始橫條圖的測量是「點選次數」(網站被要求的次數)。若要設定此初始摘要報告的時段，請參閱[資料庫連接與報告預設值](#)，第 287 頁。

按一下網頁上可用的各種連結與選項，可快速變更已報告的資訊或向下查看報告的詳細資訊。

1. 從**測量**清單選取下列選項其中之一。

選項	說明
點選次數	URL 被要求的次數。 取決於 Log Server 的設定方式，此數字可能是真實的點選次數，記錄了所要求網站之每個單獨元素的單獨記錄；此數字也可能是造訪次數，它將網站的不同元素結合到一個 Log 記錄中。請參閱 <a href="#">設定記錄快取檔案</a> ，第 271 頁。
頻寬 [KB]	資料量 (以 KB 為單位)，包括使用者的初始要求與網站的回應。此為「已傳送」與「已接收」值的加總。 請記住，有些整合產品不會傳送此資訊到 Websense 軟體。例如，Check Point FireWall-1 與 Cisco PIX Firewall。如果整合產品不能傳送此資訊，而且已安裝了 Websense Network Agent，請針對適當的 NIC 啟動 <b>記錄 HTTP 要求</b> 選項，以啟用頻寬資訊的報告。請參閱 <a href="#">設定網路卡設定</a> ，第 298 頁。
已傳送 [KB]	網際網路要求所傳送的 KB 數。這代表已傳送的資料量，其中可能是簡單要求 URL，也可能是很重要的提交，例如使用者註冊網站。
已接收 [KB]	回應要求所接收的 KB 數。這包括構成網站的所有文字、圖形與指令碼。 對於已封鎖的網站，KB 數會根據建立 Log 記錄的軟體而有所不同。當 Websense Network Agent 記錄記錄時，已封鎖之網站的接收位元組數代表 Websense 封鎖頁面的大小。 如果 Log 記錄是由 Websense Security Gateway 所建立的，由於它是即時掃描的結果，因此已接收的 KB 數代表所掃描的頁面大小。如需有關即時掃描的更多資訊，請參閱 <a href="#">使用即時選項分析內容</a> ，第 127 頁。 如果有其他整合產品建立了 Log 記錄，則已封鎖之網站的已接收 KB 可能為零 (0)，這可能代表封鎖頁面的大小，也可能是從要求的網站獲得的值。
瀏覽時間	檢視網站所花費時間的估計值。請參閱 <a href="#">網際網路瀏覽時間是什麼？</a> ，第 85 頁。

2. 從報告上方的**網際網路使用者**清單中選取選項，可以變更報告的主要群組。選項根據記錄資料庫的內容與特定網路考量而有所不同。例如，如果記錄資料庫中只有一個群組或網域，此清單中就不會顯示「群組」和「網域」。同樣地，如果有太多使用者 (超過 5,000) 或群組 (超過 3,000)，則不會顯示那些選項 (可設定這些限制中的一些，請參閱[顯示與輸出選項](#)，第 289 頁)。



- 按一下左方欄位中的名稱 (或名稱旁的箭頭) 可顯示選項清單, 例如依使用者、依網域或依動作。

所列出選項類似於「網際網路使用者」下所列的選項, 都是自訂為目前顯示之內容的有意義子集合。



### 注意

有時候選項 (例如「使用者」或「群組») 會顯示為紅色字體。在這種情況下, 選取該選項可能產生非常大的報告, 以致於產生速度很緩慢。請考慮在選取該選項之前, 進一步向下查看至詳細資訊。

- 選取這些選項其中之一以產生新的摘要報告, 此報告會顯示相關聯項目的已選取資訊。  
例如, 在「風險等級」摘要報告上, 按一下「法律責任」風險等級下方的「依使用者」會產生「法律責任」風險等級中每個使用者的活動報告。
- 按一下左方欄位的新項目, 然後選取選項以檢視有關該特定項目的更多詳細資訊。
- 使用欄位標題旁的箭頭可變更報告的排序順序。
- 使用下列位於圖表上方的選項控制摘要報告。然後, 按下新報告的元素向下查看相關的詳細資訊。

選項	動作
報告路徑 (「使用者」> 「日期」)	位於 <b>網際網路使用者</b> 清單旁邊的路徑會顯示建立目前報告的選擇。按一下該路徑中的任何連結可返回資料的檢視。
檢視	選取報告的時段: 一天、一週、一月或全部。報告會更新, 以便根據所選時段來顯示資料。 使用相鄰的箭頭按鈕可同時移動到可用資料、單一時段 (天、週或月)。 變更此選擇時, <b>檢視起點</b> 欄位會更新以反映正在檢視的時段。 如果在「檢視起點」欄位或透過「我的最愛」對話方塊選擇了具體日期, 則 <b>檢視</b> 欄位會顯示「自訂」而非時段。
從...到...的檢視	這些欄位中的日期會自動更新以反映您在 <b>檢視</b> 欄位中執行變更時所檢視的時段。 或者, 也可輸入報告的確切開始日期與結束日期, 或按一下行事曆圖示來選取想要的日期。 按一下相鄰的向右箭頭按鈕可在選取日期之後更新報告。
圓形圖/橫條圖	啟動橫條圖時, 按一下 <b>圓形圖</b> 會將目前的摘要報告顯示為圓形圖。按一下片段標籤會顯示與按一下橫條圖左側欄位中的項目所顯示的相同選項。 啟動圓形圖時, 按一下「 <b>橫條圖</b> 」將目前的摘要報告顯示為橫條圖。

選項	動作
全螢幕	選取此選項可在沒有左側與右側瀏覽窗格的單獨視窗中顯示目前的調查報告。
匿名/名稱	<p>按一下<b>匿名</b>可以讓報告在顯示使用者名稱的地方顯示內建指派的使用者識別碼。</p> <p>當名稱隱藏時，按一下<b>名稱</b>會在那些位置顯示使用者名稱。</p> <p>在某些情況下，使用者名稱無法顯示。如需詳細資訊，請參閱<a href="#">設定用於記錄的 Filtering Service</a>，第 265 頁。</p> <p>如果按一下「匿名」然後移至另一個資料檢視 (例如詳細資訊檢視或異常值)，那麼在新報告中，使用者名稱依然是隱藏的。不過，若要以隱藏名稱的方式返回摘要檢視，則必須使用報告頂端的連結，而不是橫幅中的路徑連結列。</p> <p>如果個別管理員不應該擁有存取報告中使用者名稱的權限，請將他們指派到禁止檢視調查報告中使用者名稱之報告權限的角色，並存取簡報報告。</p>
搜尋	<p>從清單選取報告元素，然後在相鄰的文字方塊中輸入要搜尋的全部或部分值。</p> <p>按一下相鄰的箭頭按鈕可開始搜尋並顯示結果。</p> <p>在本範例中，輸入部分 IP 位址 (例如 10.5.)，搜尋所有從 10.5.0.0 到 10.5.255.255 的所有子網路。</p>

8. 建立多層級摘要報告，可以針對左側欄位中所有項目或所選項目，新增資訊的子集合。請參閱[多層級摘要報告](#)，第 106 頁。
9. 按一下相鄰的數字或測量列，可以針對左側欄位中的特定項目，建立表格報告。這個詳細的報告可以加以修改，以符合您的特定需求。請參閱[靈活的細節報告](#)，第 107 頁。

## 多層級摘要報告

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [摘要報告](#)，第 103 頁
- ◆ [靈活的細節報告](#)，第 107 頁
- ◆ [使用者活動細節報告](#)，第 111 頁
- ◆ [標準報告](#)，第 116 頁
- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [排程調查報告](#)，第 120 頁
- ◆ [異常值報告](#)，第 122 頁
- ◆ [輸出至檔案](#)，第 123 頁

多層級摘要報告會顯示次要層級的資訊，以補充顯示的主要資訊。例如，如果主要顯示的是風險等級，您可定義次要層級，以瞭解在每個風險等級中最常要求的類別是哪些。另一個例子是，如果主要報告顯示每個類別的要求，您可以顯示前 5 名類別及最常要求每個類別的 10 個使用者。

使用摘要報告上方緊鄰的設定可建立多層級摘要報告。



1. 在**選擇**清單中，選擇數字以指定要報告的主要項目 (左側欄位) 數。結果報告會包括具有最大值的主要項目 (如果「日期」是主要項目，這樣會顯示最早的日期)。

或者，也可以將左側欄位中想要的個別項目旁的核取方塊標記起來，以僅針對那些項目進行報告。**選擇**欄位會顯示**自訂**。

2. 從**依**清單中選擇要報告的次要資訊。
3. 在**顯示**欄位中，選擇針對每個主要項目要報告的次要結果數。
4. 按一下**列出結果**會產生多層級摘要報告。

摘要報告會更新以只顯示所選數目的主要項目。每個主要項目的列下方會顯示次要項目的清單。

5. 使用欄位標題旁的箭頭可變更報告的排序順序。

若要返回單層級摘要報告，選取**網際網路使用者**下方的不同選項。或者，也可以按一下主要或次要項目其中之一，然後選取選項以產生該資訊的新調查報告。

## 靈活的細節報告

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [摘要報告](#)，第 103 頁
- ◆ [多層級摘要報告](#)，第 106 頁
- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [排程調查報告](#)，第 120 頁
- ◆ [異常值報告](#)，第 122 頁
- ◆ [輸出至檔案](#)，第 123 頁
- ◆ [資料庫連接與報告預設值](#)，第 287 頁
- ◆ [靈活的細節報告欄位](#)，第 109 頁

細節報告可提供有關記錄資料庫中資訊的表格檢視。在檢視了想要獲得更多細節的摘要報告之後，可從主頁存取細節報告檢視。

可從任何列上要求細節檢視。不過，在要求根據點選次數的細節報告時，最好從顯示小於 100,000 次點選次數的列開始。如果特定列的點選次數超過 100,000 次，點選次數值會顯示為紅色，警告您細節報告的產生速度會很慢。

細節報告檢視是 *非常靈活*，因為它可讓您設計自己的報告。可新增或删除資訊欄位以及變更欄位顯示的順序。資訊是根據欄位順序排序的。甚至可將任意欄位的排序順序從升冪反轉為降冪，或反過來。

Websense 調查報告受限於執行 Websense Manager 之電腦的處理器與可用記憶體，以及某些網路資源。要求大型報告可能導致逾時。要求大型報告時，會有選項讓您以不逾時的方式產生報告。



### 重要

在下拉式清單或值清單中，有些選項可能顯示為紅色。紅色字體表示選取該選項可能會導致非常大的報告。在選取該選項之前進一步向下查看至詳細資訊，一般來說會更有效率。

1. 在調查報告主頁上產生摘要報告或多層級報告 (請參閱 [摘要報告](#)，第 103 頁或 [多層級摘要報告](#)，第 106 頁)。
2. 向下查看至結果，以鎖定在最感興趣的資訊上。  
產生有關點選次數的報告時，在開啓細節報告檢視之前，最好向下查看至顯示小於 100,000 次點選次數的項目。
3. 按一下要詳細瀏覽之數字或列上的橫條。若要在一個報告中包括多個列，在按一下數字或一列上的橫條之前，先標記每列的核取方塊。  
載入細節報告時，會有彈出式訊息顯示進度。



### 注意

如果報告的產生時間很長，請考慮按一下正在載入訊息中的連結將其儲存到「我的最愛」報告，然後在稍後將它排程執行。請參閱 [我的最愛調查報告](#)，第 118 頁。

4. 檢閱初始報告中的資訊。  
取決於要報告的是點選次數、頻寬或瀏覽時間，以及在「選項」頁面上所做的選擇，預設欄位會有所不同 (請參閱 [資料庫連接與報告預設值](#)，第 287 頁)。
5. 按一下位於頁面頂端的 **更改報告**。  
「更改報告」對話方塊中的 **目前報告** 清單會顯示目前細節報告中顯示哪些欄位。
6. 在 **可用欄位** 或 **目前報告** 清單中選取欄位名稱，按一下向右箭頭 (>) 或向左箭頭 (<) 按鈕將該欄位移動到其他清單。  
為報告選擇最多 7 個欄位。來自初始摘要報告之顯示測量 (點選次數、頻寬、瀏覽時間) 的欄位始終顯示為最右側欄位。更改報告時，它不會顯示為選擇。  
如需有關可用欄位的清單以及每個欄位的說明，請參閱 [靈活的細節報告欄位](#)，第 109 頁。

7. 在**目前報告**清單中選取欄位名稱，並使用向上與向下箭頭按鈕來變更欄位的順序。  
「目前報告」清單頂端的欄位會變成報告中的左側欄位。
8. 按一下報告上方的**摘要**或**細節**可在兩種顯示之間切換。

選項	說明
摘要	必須移除「時間」欄位才能顯示摘要報告。摘要報告會將共用公共元素的所有記錄分組成一個項目。取決於要報告的資訊，特定的元素會有所不同。一般而言，測量之前的最右側欄位會顯示摘要的元素。
細節	「細節」選項會將每個記錄顯示為單獨的列。「時間」欄位可以顯示出來。

9. 按一下**提交**會產生您所定義的報告。
10. 使用下列選項可以修改顯示的報告。
  - 使用報告上方的**檢視**選項可變更報告的時段。
  - 按一下欄位標題中的向上或向下箭頭可反轉該欄位及相關資料的排序順序。
  - 使用報告上方或下方的**下一頁**與**上一頁**連結，可顯示該報告的其他頁面（如果有的話）。在預設情況下，每個頁面包含 100 列，列可調整以符合您的需求。請參閱[顯示與輸出選項](#)，第 289 頁。
  - 按一下 URL 可在新視窗中開啓要求的網站。
11. 如果想要儲存報告，可以按一下**我的最愛報告**，如此便可快速地再次產生報告或循環地產生報告（請參閱[將報告儲存到我的最愛](#)，第 118 頁）。

## 靈活的細節報告欄位

相關主題：

- ◆ [靈活的細節報告](#)，第 107 頁
- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [排程調查報告](#)，第 120 頁

下表說明細節報告的可用欄位（請參閱[靈活的細節報告](#)，第 107 頁）。

並非所有欄位皆隨時可用。例如，如果顯示了「使用者」欄位，「群組」欄位就無法使用；如果顯示了「類別」欄位，「風險等級」欄位就無法使用。

欄位名稱	說明
使用者	執行要求的使用者名稱。在記錄資料庫中，使用者資訊必須可用，這樣才能將它包括在報告中。以使用者為基礎的報告上，無法使用群組資訊。
日	執行要求的日期。
URL 主機名稱	要求之網站的網域名稱 (又稱為主機名稱)。
網域	執行要求之目錄式用戶端 (使用者或群組、網域，或組織單位) 的目錄服務網域。
群組	要求者所屬的群組名稱。以群組為基礎的報告中，不提供個別使用者的名稱。如果要求網站的使用者屬於目錄服務中一個以上的群組，則報告中的此欄位會列出多個群組。
風險等級	與要求之網站所屬類別相關聯的風險等級。如果類別有多個風險等級，則會列出所有相關的風險等級。請參閱 <a href="#">將類別指派到風險等級</a> ，第 264 頁。
目錄物件	執行報告之使用者的目錄路徑，但不包括使用者名稱。一般而言，這會導致具有相同流量的多個列，因為每個使用者屬於多個路徑。 如果使用的是非 LDAP 目錄服務，則此欄位不可用。
配置	Websense 軟體視為要求結果的動作，例如允許的類別或封鎖的類別。
來源伺服器	傳送要求到 Filtering Service 的電腦的 IP 位址。此即為執行整合產品或 Websense Network Agent 的電腦。
通訊協定	要求的通訊協定。
通訊協定群組	要求之通訊協定所屬的 Master Database 群組。
來源 IP	執行要求之電腦的 IP 位址。
目的 IP	要求之網站的 IP 位址。
完整 URL	要求之網站的網域名稱與路徑 (例如： <a href="http://www.mydomain.com/products/itemone/">http://www.mydomain.com/products/itemone/</a> )。如果沒有記錄完整的 URL，此欄位會空白。請參閱 <a href="#">設定完整 URL 記錄</a> ，第 281 頁。
月	執行要求的行事曆月份。
連接埠	使用者用來與網站通訊的 TCP/IP 連接埠。

欄位名稱	說明
頻寬	資料量 (以 KB 為單位)，包括使用者的初始要求與網站的回應。此為「已傳送」與「已接收」值的加總。 請記住，有些整合產品不會傳送此資訊到 Websense 軟體。例如，Check Point FireWall-1 與 Cisco PIX Firewall。 如果整合產品不能傳送此資訊，而且已安裝了 Websense Network Agent，請針對適當的 NIC 啟動 <b>記錄 HTTP 要求 (加強記錄)</b> 選項，以啟用頻寬資訊的報告。請參閱 <a href="#">設定網路卡設定</a> ，第 298 頁。
已傳送的位元組數	網際網路要求時傳送的位元組數。這代表已傳送的資料量，其中可能是簡單要求 URL，也可能是很重要的提交，例如使用者註冊網站。
已接收的位元組數	為回應要求而從網際網路接收的位元組數。這包括構成網站的所有文字、圖形與指令碼。 對於已封鎖的網站，位元組數會根據建立 Log 記錄的軟體而有所不同。當 Websense Network Agent 記錄記錄時，已封鎖之網站的接收位元組數代表封鎖頁面的大小。 如果 Log 記錄是由 Websense Security Gateway 所建立的，由於它是即時掃描的結果，因此已接收的位元組數代表所掃描的頁面大小。如需有關即時掃描的更多資訊，請參閱 <a href="#">使用即時選項分析內容</a> ，第 127 頁。 如果有其他整合產品建立了 Log 記錄，則已封鎖之網站的已接收位元組數可能為零 (0)，這可能代表封鎖頁面的大小，也可能是從要求的網站獲得的值。
時間	網站被要求時的時間，以 HH:MM:SS 格式顯示，使用 24 小時時鐘。
類別	篩選要求的類別。這可能是來自 Websense Master Database 的類別或自訂類別。

## 使用者活動細節報告

相關主題：

- ◆ [調查報告](#)，第 102 頁

按一下[使用者每日/每月活動細節](#)連結，針對一個使用者產生「使用者活動細節」報告。此報告會針對使用者單日或整月的網際網路活動提供圖解。

首先，針對所選的天，為特定使用者產生報告。從該報告中，您可以產生同一使用者的整月活動報告。如需詳細指示，請參閱：

- ◆ [使用者每日活動細節](#)，第 112 頁
- ◆ [使用者每月活動細節](#)，第 113 頁

## 使用者每日活動細節

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [使用者活動細節報告](#)，第 111 頁
- ◆ [使用者每月活動細節](#)，第 113 頁

「使用者每日活動細節」報告可針對特定使用者在單日的活動提供更深入的檢視。

1. 選取主頁頂端的**使用者每日/每月活動細節**。將出現「使用者每日活動細節」對話方塊。
2. 在**搜尋使用者**欄位中輸入使用者名稱或部分名稱，然後按一下**搜尋**。  
搜尋會顯示記錄資料庫中相符之使用者名稱的捲動清單，最多顯示 100 個。
3. 從**選取使用者**清單進行選擇。
4. 在**選取日期**欄位中，接受預設顯示的最後活動日期，或選擇其他日期。  
可輸入新日期或按一下行事曆圖示以選取日期。行事曆選取方塊會指示作用中記錄資料庫所涵蓋的日期範圍。
5. 按一下**到使用者每日活動細節**以檢視該使用者在要求之日期當天的詳細活動報告。

初始報告會顯示使用者活動的時間表，以 5 分鐘為增量。每個要求都會顯示為對應於 Websense Master Database 類別的圖示。有一個圖示表示所有自訂類別 (圖示的顏色會與「使用者每月活動細節」報告上顯示的風險群組相對應，請參閱[使用者每月活動細節](#)，第 113 頁)。

將滑鼠移到圖示上方會顯示確切時間、類別及與要求相關聯的動作。

可使用下方列出的控制項來修改報告顯示或檢視圖例。

選項	說明
上一日/ 下一日	顯示此使用者在行事曆上一日或下一日的網際網路活動。
表格檢視	顯示每個要求的 URL 清單，提供有關要求、類別及採取之活動 (封鎖、允許或其他) 的日期與時間。
細節檢視	顯示報告的初始圖形檢視。



選項	說明
群組相似點選次數/檢視所有點選次數	將具有相同網域、類別及動作且在 10 秒內互相發生的所有要求，結合在一個列中。這樣可獲得資訊的簡短摘要檢視。 標準時間臨界值是 10 秒。如需變更此值，請參閱 <a href="#">顯示與輸出選項</a> ，第 289 頁。 按下連結之後，它會變成「檢視所有點選次數」，從而還原每個要求的原始清單。
類別檢視控制	顯示目前報告中每個類別的清單，該清單會顯示類別名稱與代表該類別的圖示。 藉由標記要包含之類別的核取方塊，可以控制報告顯示的類別。然後按一下 <a href="#">接受</a> 以便依選擇來更新報告。

- 按一下報告上方的**使用者每月活動細節**，以檢視同一使用者的整月活動。如需詳細資訊，請參閱[使用者每月活動細節](#)，第 113 頁。

## 使用者每月活動細節

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [使用者活動細節報告](#)，第 111 頁
- ◆ [使用者每日活動細節](#)，第 112 頁
- ◆ [類別對應](#)，第 114 頁

當「使用者每日活動細節」報告已開啓時，可進行切換以檢視該使用者的每月活動。

- 開啓「使用者每日活動細節」報告。請參閱[使用者每日活動細節](#)，第 112 頁。
- 按一下頂端的**使用者每月活動細節**。

新報告會顯示行事曆影像，其中每天的區域顯示小小的顏色區塊，代表使用者當天的網際網路活動。對自訂類別中之網站的要求會顯示為灰色區塊。

- 按一下左上方的**資料庫類別圖例**可檢視顏色如何代表要求之網站的潛在風險高低。

類別指派是固定的，而且不可變更。請參閱[類別對應](#)，第 114 頁。

- 按一下上一月或下一月以顯示此使用者上一個月或下一個月的網際網路活動。

## 類別對應

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [使用者活動細節報告](#)，第 111 頁
- ◆ [使用者每月活動細節](#)，第 113 頁

下列清單會指出在「使用者每日活動細節」和「使用者每月活動細節」報告中，每個顏色所代表的是什麼類別。

請記住，Master Database 中的類別名稱可能會有變動。此外，也可以隨時新增或刪除類別。

顏色	類別
灰色	自訂類別 非 HTTP 流量
深藍色	<b>商業與經濟</b> 及其所有下層類別 <b>教育</b> 及其所有下層類別 <b>健康</b> <b>資訊科技</b> ，包括「搜尋引擎與入口網站」和「網站代管」下層類別 <b>其他</b> 下層類別有「內容遞送網路」、「動態內容 (CGI-BIN)」、「影像 (媒體)」、「影像伺服器」及「私有 IP 位址」 <b>生產力/廣告</b>
淺藍色	<b>藥物/處方藥</b> <b>政府</b> 及其「軍事」下層類別 <b>資訊科技/URL 轉換網站</b> <b>其他</b> ，僅上層類別 <b>新聞媒體</b> ，僅上層類別 <b>特殊事件</b>

顏色	類別
黃綠色	<p><b>墮胎</b>及其所有下層類別</p> <p><b>成人資訊/性教育</b></p> <p><b>頻寬</b>，包括下層類別「網際網路廣播與電視」、「個人網路儲存，備份」和「串流媒體」</p> <p><b>娛樂</b>，包括其下層類別 MP3</p> <p><b>遊戲</b></p> <p><b>政府/政治團體</b></p> <p><b>資訊科技/電腦安全</b></p> <p><b>網際網路通訊/網路式電子郵件</b></p> <p><b>其他/檔案下載伺服器</b></p> <p><b>其他/網路錯誤</b></p> <p><b>新聞媒體/可選期刊</b></p> <p><b>生產力</b>，包括其下層類別「即時訊息傳送」、「留言板與俱樂部」和「線上經紀與交易」</p> <p><b>宗教</b>及其下層類別「非傳統宗教、秘術與民間傳說」和「傳統宗教」</p> <p><b>安全性</b>，僅上層類別</p> <p><b>購物</b>及其所有下層類別</p> <p><b>社會組織</b>及其所有下層類別</p> <p><b>社會與生活時尚</b>，包括其下層類別「同性戀，雙性戀」、「嗜好」、「個人網站」及「餐飲」</p> <p><b>體育運動</b>及其所有下層類別</p> <p><b>旅行</b></p> <p><b>使用者定義</b></p> <p><b>交通工具</b></p>

顏色	類別
橙色	<p>成人資訊/裸體</p> <p>倡議團體</p> <p>頻寬/網際網路電話</p> <p>藥物及其下層類別「濫用藥物」、「大麻」及「補充藥物/非規製合成藥物」</p> <p>資訊科技/以 Proxy 規避封鎖</p> <p>網際網路通訊及其下層類別「網上聊天」</p> <p>求職</p> <p>其他/尚未歸類</p> <p>生產力下層類別「免費軟體，軟體下載」及「上網式賺錢」</p> <p>宗教</p> <p>社會與生活時尚下層類別「煙酒」及「個人/約會」</p> <p>惡俗</p> <p>武器</p>
紅色	<p>成人資訊及下列下層類別：「成人內容」、「女仕內衣與泳裝」和「性」</p> <p>頻寬/端對端檔案共用</p> <p>賭博</p> <p>違法或嫌疑行為</p> <p>資訊科技/駭客入侵</p> <p>暴力衝突，極端主義</p> <p>種族歧視</p> <p>安全性下層類別「鍵盤側錄」、「惡意網站」「網路釣魚」及「間諜軟體」</p> <p>暴力</p>

## 標準報告

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [排程調查報告](#)，第 120 頁

標準報告用於快速顯示特定資訊集，而無需使用向下查看程序。

1. 按一下主要「調查報告」頁面上的**標準報告**連結。

2. 選擇含有所需資訊的報告。提供以下報告。

---

**最高活動等級**

---

- 點選次數最多的使用者？
- 前 10 大造訪次數的 URL 的前 10 名使用者
- 在購物、娛樂與體育運動的前 5 大使用者活動
- 前 5 大造訪類別的前 5 大 URL

---

**最高頻寬使用量**

---

- 耗費最多頻寬的群組
- 耗費最多串流媒體頻寬的群組
- 網路頻寬損失使用者的 URL 細節報告
- 前 10 大頻寬類別群組

---

**上網瀏覽時間最多**

---

- 哪些使用者上網瀏覽時間最多
- 哪些使用者上網瀏覽生產力類別網站的時間最多

---

**封鎖次數最多**

---

- 最常被封鎖的使用者？
- 最常被封鎖的網站？
- 被封鎖使用者的 URL 細節報告
- 前 10 大被封鎖類別

---

**最高安全風險**

---

- 構成最多安全風險的類別
- P2P 通訊協定的使用者排名
- 安全性類別的網站使用者排名
- 前 10 大有間諜軟體活動的電腦 URL

---

**法律責任**

---

- 法律責任風險類別
  - 成人類別的使用者排名
- 

3. 檢視所顯示的報告。
4. 如果想要循環執行報告，可將報告儲存到「我的最愛」。請參閱[我的最愛調查報告](#)，第 118 頁。

## 我的最愛調查報告

相關主題：

- ◆ [調查報告，第 102 頁](#)
- ◆ [排程調查報告，第 120 頁](#)

可將最常用的調查報告儲存到「我的最愛」。這包括藉由向下查看至特定資訊所產生的報告、標準報告以及經修改符合特定需求的詳細報告。然後，可以隨時執行「我的最愛」報告，或將它排程在特定日期或時間執行。

在使用委派管理的組織中，儲存與排程「我的最愛」的權限是由超級管理員設定的。獲得此權限的管理員僅能執行與排程自己儲存的「我的最愛」，而不能存取其他管理員儲存的「我的最愛」。

如需有關使用「我的最愛」報告的詳細指示，請參閱：

- ◆ [將報告儲存到我的最愛，第 118 頁](#)
- ◆ [產生或刪除我的最愛報告，第 119 頁](#)
- ◆ [修改我的最愛報告，第 119 頁](#)

## 將報告儲存到我的最愛

相關主題：

- ◆ [我的最愛調查報告，第 118 頁](#)
- ◆ [修改我的最愛報告，第 119 頁](#)

使用下列程序可將報告儲存到「我的最愛」。

1. 產生具有所需格式與資訊的調查報告。
2. 按一下**我的最愛報告**。
3. 接受或修改 Websense Manager 顯示的名稱。  
名稱可以包含字母、數字及底線字元 ( \_ )。不能使用空格或其他特殊字元。
4. 按一下**新增**。  
報告名稱即新增到「我的最愛」清單。
5. 在此清單上選取報告，然後選取選項以便管理報告。取決於您所選取的選項，請參閱：
  - [產生或刪除我的最愛報告，第 119 頁](#)
  - [排程調查報告，第 120 頁](#)

## 產生或刪除我的最愛報告

相關主題：

- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [修改我的最愛報告](#)，第 119 頁

可隨時產生「我的最愛」報告，或刪除已過時的報告。

1. 按一下**我的最愛報告**以顯示儲存到我的最愛的報告清單。



### 注意

如果貴組織使用委派管理，此清單不會包括其他管理員儲存的我的最愛報告。

2. 從清單中選取所需報告。

如果所需報告尚未儲存到「我的最愛」，請參閱[將報告儲存到我的最愛](#)，第 118 頁。

3. 視需求執行以下操作：

- 按一下**立即執行**以立即產生和顯示所選報告。
- 按一下**排程**以將報告排程在稍後執行或循環執行。如需詳細資訊，請參閱[排程調查報告](#)，第 120 頁。
- 按一下**刪除**從「我的最愛」清單中移除報告。

## 修改我的最愛報告

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [我的最愛調查報告](#)，第 118 頁

可按如下方式輕鬆建立與現有「我的最愛」報告類似的新的「我的最愛」報告。

1. 按一下**我的最愛報告**以顯示儲存到我的最愛的報告清單。



### 注意

如果貴組織使用委派管理，此清單不會包括其他管理員儲存的我的最愛報告。

2. 選取並執行與想要建立之新報告最相近的現有「我的最愛」報告。(請參閱[產生或刪除我的最愛報告](#)，第 119 頁。)
3. 依需要修改所顯示的報告。

4. 按一下**我的最愛報告**以新名稱將修訂後的顯示儲存到「我的最愛」報告。  
(請參閱[將報告儲存到我的最愛](#)，第 118 頁。)

## 排程調查報告

相關主題：

- ◆ [我的最愛調查報告](#)，第 118 頁
- ◆ [將報告儲存到我的最愛](#)，第 118 頁
- ◆ [管理排程的調查報告工作](#)，第 122 頁

必須先將調查報告儲存到「我的最愛」，然後才能將它排程為稍後執行或以重複週期方式執行。執行排程報告工作時，結果報告會透過電子郵件傳送到指定的收件人。建立排程工作時，請考量電子郵件伺服器是否可以處理報告檔案附件的大小與數量。

排程報告檔案會儲存在以下目錄中：

< 安裝路徑 > \webroot \Explorer \< 名稱 > \

預設安裝路徑為 C:\Program Files\WebSense。如果排程工作只有一個收件者，<名稱> 就是電子郵件位址的第一部份 (在 @ 之前)。在有多個收件者的情況下，報告會儲存在名為 Other 的目錄中。



### 注意

重複工作所儲存的報告每次都會使用相同的檔案名稱。如果想要針對比單一週期更長的時間儲存檔案，務必要變更檔案名稱或將檔案複製到其他位置。

取決於所排程報告的大小與數目，此目錄可能會變得很大。務必定期清除目錄，刪除不需要的報告檔案。

1. 將一或多個報告儲存到我的最愛 (請參閱[將報告儲存到我的最愛](#)，第 118 頁)。
2. 按一下**我的最愛報告**以顯示儲存到我的最愛報告清單。



### 注意

如果貴組織使用委派管理角色，此清單不會包括其他管理員儲存的我的最愛報告。

3. 反白顯示最多 5 個報告，作為工作的一部分來執行。
4. 按一下**排程**以建立排程報告工作，然後提供「排程報告」頁面上要求的資訊。



建議將報告工作排程在不同日期或不同時間，以避免記錄資料庫超載及降低記錄與互動式報告的效能。

欄位	說明
重複執行	選取執行報告工作的頻率 (一次、每天、每週、每月)。
開始日期	選取一週內的哪一天或行事曆日期，以便首次執行工作 (或僅執行一次)。
執行時間	設定執行工作的時間。
傳送電子郵件至	使用 <b>其他電子郵件位址</b> 欄位，將適當的位址新增到此清單。 反白顯示工作中要接收報告的一或多個電子郵件位址 (務必取消選取不應該接收報告的位址)。
其他電子郵件位址	輸入電子郵件位址，然後按一下 <b>新增</b> 將它放到 <b>傳送電子郵件至</b> 清單。 新的電子郵件位址會自動與其他已選取的電子郵件位址一起反白顯示。
自訂電子郵件的主旨與內文	標記這個核取方塊，以便自訂您的電子郵件通知主旨行與內文。 如果沒有勾選此方塊，會使用預設的主旨與內文。
電子郵件主旨	輸入發佈排程報告時做為電子郵件主旨行的文字。 預設的電子郵件主旨為： 調查報告排程工作
電子郵件內文	輸入發佈排程報告時要新增到電子郵件訊息的文字。 電子郵件內文顯示如下，其中，您的文字會放在 <CUSTOM TEXT> 位置。 報告排程器會在 <date time> 產生一或多個附加檔案。 <CUSTOM TEXT> 若要檢視所產生的報告，按一下後面的連結。 注意：如果收件人沒有權限存取送出工作的網路伺服器，連結將不會起作用。
排程工作名稱	為排程工作指派唯一的名稱。名稱會在「工作佇列」中識別此工作。請參閱 <a href="#">管理排程的調查報告工作</a> ，第 122 頁。
輸出格式	選取排程報告的檔案格式： <b>PDF</b> ：「可攜式文件格式」需使用 Adobe Reader 檢視。 <b>Excel</b> ：Excel 試算表檔案需使用 Microsoft Excel 檢視。
日期範圍	設定此工作報告所涵蓋的日期範圍。 <b>所有日期</b> ：記錄資料庫中所有可用的日期。 <b>相對</b> ：選取要包括的時段 (天、週或月) 和特定區段 (本、最後、最後 2 等等)。 <b>特定</b> ：設定此工作報告的特定日期或日期範圍。

- 按下一步顯示「排程確認」頁面。
- 按一下**儲存**以儲存您的選擇並前往「工作佇列」頁面 (請參閱[管理排程的調查報告工作](#)，第 122 頁)。

## 管理排程的調查報告工作

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [排程簡報報告](#)，第 96 頁

為調查報告建立排程的工作時，會出現**工作佇列**頁面，其中顯示新工作與現有排程工作的清單。也可按一下主要調查報告頁面上的**工作佇列**連結來存取頁面。



### 注意

如果貴組織使用委派管理，此頁面不會顯示其他管理員所排程的工作。

**排程報告細節**區段會以建立順序列出每個排程工作，並顯示已定義排程和工作狀態的概覽。此外，還有下列選項可供使用。

選項	說明
編輯	顯示針對此工作所定義的排程，並可視需要加以修改。
刪除	刪除工作及在「狀態記錄」區段中新增項目，將該工作顯示為「已刪除」。

**狀態記錄**區段會列出以各種方式變更過的每個工作，顯示工作的排程開始時間、實際結束時間和狀態。

按一下**清除狀態記錄**可移除「狀態記錄」區段中的所有項目。

## 異常值報告

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [摘要報告](#)，第 103 頁

異常值報告會顯示資料庫中具有最無用之網際網路活動的使用者。Websense 軟體會計算所有使用者每個類別、每天、每個活動 (有時稱為配置) 及每個通訊協定的平均活動。然後顯示統計上與平均值差異最大的使用者活動。差異的計算是以平均值為基準的標準差。

1. 在主要調查報告頁面上，會產生顯示您要檢視異常值之資訊的報告。在「網際網路使用者」欄位旁邊，以藍色強調並顯示的報告區段會反映在異常值報告中。

例如，若要檢視特定類別依點選次數的異常值，在**網際網路使用者**清單中選取**類別**，並選取**點選次數**做為**測量**。



### 注意

無法產生瀏覽時間的異常值報告。如果從顯示瀏覽時間的摘要報告開始，異常值報告會以點選次數為基礎。

## 2. 按一下**異常值**。

列會以降冪順序排序，第一個顯示的是最大差異。每個列會顯示：

- 使用者、類別、通訊協定、日期及動作的總數 (點選次數或頻寬)。
- 針對該類別、通訊協定、日期及動作的所有使用者平均值 (點選次數或頻寬)。
- 與使用者平均值的差異。

## 3. 若要檢視此類別在不同時間的個別使用者活動，按一下使用者名稱。

例如，如果某個使用者在特定日期的活動異常多，按一下該使用者名稱可檢視報告，以便對有關該使用者整體活動有更深入的了解。

## 輸出至檔案

相關主題：

- ◆ [調查報告，第 102 頁](#)
- ◆ [列印調查報告，第 124 頁](#)

產生調查報告之後，可使用報告上方的按鈕將它儲存至檔案。您所按下的按鈕會決定檔案格式。

選項	說明
	將報告儲存為 XLS 格式。 如果存取 Websense Manager 的電腦上已安裝 Microsoft Excel 2003 或更新版本，系統會提示您檢視或儲存報告。如果沒有安裝，系統會提示您為儲存的報告選取目錄與檔案名稱。 使用 Microsoft Excel 中的選項列印、儲存或以電子郵件傳送報告。
	將報告儲存為 PDF 格式。 如果存取 Websense Manager 的電腦上已安裝 Adobe Reader v7.0 或更新版本，系統會提示您檢視或儲存報告。如果沒有安裝，系統會提示您為儲存的報告選取目錄與檔案名稱。 使用 Adobe Reader 中的選項列印、儲存或以電子郵件傳送報告。

## 列印調查報告

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [輸出至檔案](#)，第 123 頁

可使用下列方式列印調查報告：

- ◆ 在報告顯示時，使用網頁瀏覽器的列印功能。
- ◆ 建立 PDF 或 XLS 檔案，然後使用 Adobe Reader 或 Microsoft Excel 中的列印功能 (請參閱 [輸出至檔案](#)，第 123 頁)。

雖然報告已經設定好可以從瀏覽器成功列印，但您仍可能想要測試列印以檢查結果。

「使用者每月活動細節」報告被設定為以橫向模式列印。其他所有報告都被設定為直向模式。

設計您自己的報告時 (請參閱 [靈活的細節報告](#)，第 107 頁)，欄位寬度會根據其中所包含的資訊而改變。如果報告寬度大於 8 1/2 英吋，頁面方向會變成橫向。

頁面內容的寬度為 7 1/2 英吋或 10 英吋。若使用 A4，邊界會稍微窄一點，但依然在列印範圍內。(預設的紙張大小是 Letter 或 8.5 x 11 英吋。如果使用 A4 紙，務必 wse.ini 檔案中變更此設定。請參閱 [顯示與輸出選項](#)，第 289 頁。)

## 存取自行報告

---

相關主題：

- ◆ [調查報告](#)，第 102 頁
- ◆ [設定報告偏好設定](#)，第 265 頁
- ◆ [自行報告](#)，第 291 頁

Websense 自行報告用於評估您自己的網際網路瀏覽活動，而且可視需要調整它們以符合組織的方針。報告也符合要求組織讓使用者檢視所收集之資訊類別的政府規範。

如果貴組織啟用自行報告，可從瀏覽器進行存取：

1. 輸入 Websense 管理員提供的 URL，或按一下主要 Websense Manager 登入頁面上的「自行報告」連結，以存取自行報告登入頁面。
2. 如果 **Policy Server** 顯示下拉式清單，請選取記錄您網際網路活動資訊之 Policy Server 的 IP 位址。

請聯絡 Websense 管理員以獲得協助。

3. 輸入用來登入網路的**使用者名稱**和**密碼**。
4. 按一下**登入**。

Websense Manager 會開啓調查報告，其中會依照風險等級顯示您的網際網路活動。按一下頁面上的各種連結和元素可存取其他選項，以各種方式檢視有關您活動的儲存資訊。使用報告時，可透過**說明**系統獲得協助。



# 7

## 使用即時選項分析內容

相關主題：

- ◆ [掃描選項](#)，第 129 頁
- ◆ [分類內容與掃描威脅](#)，第 129 頁
- ◆ [檔案掃描](#)，第 130 頁
- ◆ [抽除內容](#)，第 132 頁
- ◆ [即時掃描活動的報告](#)，第 134 頁

Websense 篩選軟體會根據您啓用的政策與儲存在 Master Database 中的資訊來篩選網際網路活動。如果您訂閱 Websense Content Gateway 或 Websense Web Security Gateway，也可以即時方式分析網站與檔案內容。

視您的訂閱而定，有 2 個即時分析選項可供使用：內容分類與安全性即時掃描。

- ◆ 使用**內容分類**來檢閱尚未封鎖的 URL 內容 (根據您啓用的政策和該 URL 的 Websense Master Database 分類)，並傳回類別供篩選使用。
- ◆ 如果您訂閱 Websense Web Security Gateway，有 3 個**安全性即時掃描**選項可以使用。
  - **內容掃描**會查看網頁內容以尋找安全威脅，例如網路釣魚、URL 重新導向、Web 入侵和以 Proxy 規避封鎖。
  - **檔案掃描**會檢查檔案內容以判斷威脅類別，例如病毒、特洛伊木馬程式或蠕蟲。
  - **內容抽除**會從要求的網頁移除主動式內容。

當啓動這些選項皆的任一項時，只會對根據您啓用之政策及其 Websense Master Database 分類而尚未封鎖的網站進行分析。如需詳細資訊，請參閱[掃描選項](#)，第 129 頁。



### 重要

限制存取篩選器與未篩選的 URL 會取代即時分類。

如果使用者要求的網站是在啓用的限制存取篩選器中 (請參閱[將使用者限制於定義的網際網路網站清單](#)，第 145 頁) 或在「未篩選的 URL」清單中 (請參閱[重新定義特定網站的篩選](#)，第 158 頁)，則會允許該要求，即使執行了即時掃描且發現威脅也一樣。

若要利用這些即時安全性功能，請在下列 2 個位置輸入包含 Websense Content Gateway 或 Websense Web Security Gateway 支援的訂閱密碼：

- ◆ 在 Websense Manager 中 (前往設定 > 帳戶)。
- ◆ 在 Websense Content Gateway 管理介面中 (前往設定 > 我的代理 > 訂閱 > 訂閱管理標籤)。

這 2 個產品會花數分鐘下載必要的資料庫、進行同步，並在兩個管理工具中顯示所有即時功能。

## Websense 即時選項

Websense 即時選項可協助確保網路安全。使用這些選項以掃描網際網路內容並將它指派到篩選類別。即時結果會傳送到 Filtering Service，Filtering Service 會根據啓用之政策中指派到該網站的即時分類的動作，來篩選網站。

## 資料庫下載

即時選項有賴於與 Websense Web Security Gateway 一起安裝的小型資料庫，它會定期檢查資料庫更新。這些資料庫的更新，是獨立於 Master Database 更新 (包括即時資料庫更新與即時安全性更新) 以外執行的。

每一次您使用 `./WCGAdmin start` 指令來啓動 Websense Security Gateway 時，就會開始資料庫下載。如果下載失敗，則每 15 分鐘會嘗試重新下載，直到成功下載為止。

資料庫更新檢查的預設間隔是 15 分鐘。您可以透過編輯 Websense Content Gateway 電腦上 `/opt/bin/downloadservice.ini` 檔案中的 `PollInterval` 值，來變更此間隔。

編輯 `downloadservice.ini` 檔案之後，您必須從指令行停止並重新啓動 Websense Content Gateway。

- ◆ 若要停止，輸入：`/opt/WCG/WCGAdmin stop`
- ◆ 若要重新啓動，輸入：`/opt/WCG/WCGAdmin start`



## 掃描選項

使用 **設定 > 即時掃描** 頁面來啓用與設定即時選項。下列各節會詳細說明各個掃描選項。

- ◆ [分類內容與掃描威脅](#)，第 129 頁
- ◆ [檔案掃描](#)，第 130 頁
- ◆ [抽除內容](#)，第 132 頁

針對每個選項，您至少有 2 個選擇：

- ◆ **關閉**。不執行即時掃描或封鎖。此選項不提供額外的安全性。
- ◆ **建議或開啓**。如果您的網站已設定進行即時掃描，此設定可提供您最佳的效能。系統會根據 2 個因素來執行掃描：
  - **設定 > 即時掃描 > 例外標籤**上的「永遠掃描」與「永不掃描」清單（請參閱 [優化掃描](#)，第 133 頁）。
  - Websense 軟體是否已將網站識別為包含動態內容。標幟為包含動態內容的網站都會掃描。將網站識別為包含動態內容的標記是使用者無法設定的。「永不掃描」清單上顯示之具有動態內容的網站則不會掃描。
- ◆ **全部**。掃描所有要求的網頁。唯一的例外是列在「永不掃描」清單上的網站。此選項提供最高的安全性，但是可能會嚴重減慢系統效能。



### 警告

在任何情況下，都不會分析「永不掃描」清單中所列的網站。如果「永不掃描」清單上的網站遭到入侵，即時選項也不會分析與偵測惡意程式碼。

## 分類內容與掃描威脅

相關主題：

- ◆ [掃描選項](#)，第 129 頁
- ◆ [檔案掃描](#)，第 130 頁
- ◆ [抽除內容](#)，第 132 頁
- ◆ [優化掃描](#)，第 133 頁
- ◆ [即時掃描活動的報告](#)，第 134 頁

網頁內容的變更非常快速。統計資料顯示，絕大部分的網頁內容是動態的。此外，網際網路托管了更多使用者產生的內容，例如社群網路網站上的內容。管理企業網站的內容與樣式方針，並無法管理這類內容。

當啓用了內容分類時，所選取的網站會即時分類，而所劃分的類別會轉送到 Websense 篩選軟體，以便根據啓用的政策來封鎖或允許。



### 重要

如果您計畫產生即時掃描活動的報告，請啓用完整 URL 記錄 (請參閱 [設定完整 URL 記錄](#)，第 281 頁)。否則，Log 記錄會僅包含已分類網站的網域 (www.domain.com)，以及可能符合不同類別的網站中的個別頁面。

如果您的網站使用 WebCatcher 以將爲已分類 URL 報告至 Websense, Inc. (請參閱 [設定 WebCatcher](#)，第 274 頁)，那麼透過內容分類進行分類的 URL 便會轉送，以便包含在 Master Database 中。

如果您的訂閱包含 Websense Security Gateway，那麼您也可以指定掃描該網站的安全威脅。

使用 [設定 > 即時掃描 > 常用選項](#) 頁面可以指定何時要使用內容分類與內容掃描。

1. 在「內容分類」區域中，選取 **關閉** 或 **開啓** (預設) 來決定是否執行掃描。請參閱 [掃描選項](#)，第 129 頁。

當類別已決定之後，就會套用您已設定的任何其他即時選項，以便提供額外的安全性。

2. (*Websense Security Gateway*) 在「內容掃描」區域中，選取 **關閉** (預設)、**建議** 或 **全部** 以決定掃描等級。
3. 執行下列其中之一：
  - 若要新增網站到「永不掃描」或「永遠掃描」清單，選取 **例外標籤**。請參閱 [優化掃描](#)，第 133 頁。
  - 若要變更其他即時掃描選項的設定，繼續使用 [常用選項](#) 頁面。請參閱 [檔案掃描](#)，第 130 頁和 [抽除內容](#)，第 132 頁。
4. 完成之後，按一下 **確定** 來快取您的變更。按一下 **全部儲存** 才能使變更生效。

簡報報告可以提供有關嘗試存取含有威脅之網站的詳細資料。如需有關執行 Websense 報告的詳細資料，請參閱 [簡報報告](#)，第 86 頁。

## 檔案掃描

相關主題：

- ◆ [掃描選項](#)，第 129 頁
- ◆ [分類內容與掃描威脅](#)，第 129 頁
- ◆ [抽除內容](#)，第 132 頁
- ◆ [優化掃描](#)，第 133 頁
- ◆ [即時掃描活動的報告](#)，第 134 頁

檔案掃描會查看使用者嘗試下載或遠端開啓之內送應用程式檔案中的內容。該即時選項會將類別傳回至 Websense 篩選軟體，以便適當地允許或封鎖該檔案。

最佳作法是掃描所有的可執行檔 (例如，.exe 與 .dll 檔案)。您也可以識別其他檔案類型以便掃描，並設定掃描的大小上限。



#### 注意

只掃描 Windows 32 位元可攜式應用程式檔案。

使用 **設定 > 即時掃描 > 常用選項** 標籤來指定何時要使用檔案掃描。

1. 在「檔案掃描」區域中，選取**關閉**、**建議** (預設) 或**全部**以決定掃描等級。請參閱 [掃描選項](#)，第 129 頁。
2. 按一下**進階設定**。
3. 預設會選取**掃描所有含可執行內容的檔案類型**。如果您希望列出要掃描的個別副檔名，清除此核取方塊。
4. 若要指定掃描其他檔案類型，請輸入副檔名 (例如 ppt 或 wmv)，然後按一下**新增**。副檔名僅能包含英數字元、底線 ( \_ ) 或橫線 ( - )。不包含副檔名之前的點。  
若要從「已選擇副檔名」清單中移除副檔名，選取該副檔名，然後按一下**移除**。
5. 在「選項」之下，輸入要掃描的檔案的大小上限 (預設為 10 MB)。選擇**自訂**以輸入大小，最大可達 4096 MB (4 GB)。大於指定大小的檔案將不會掃描。
6. 執行下列其中之一：
  - 如果您要新增網站到「永不掃描」或「永遠掃描」清單，請選取**例外**標籤。請參閱 [優化掃描](#)，第 133 頁。
  - 如果您要變更其他即時掃描選項的設定，繼續使用**常用選項**標籤。請參閱 [分類內容與掃描威脅](#)，第 129 頁和 [抽除內容](#)，第 132 頁。
7. 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

有數個簡報報告可以提供有關嘗試下載具有安全風險之檔案的詳細資料。如需有關執行 Websense 報告的指示，請參閱 [簡報報告](#)，第 86 頁。

如需有關根據類型與 URL 類別來封鎖檔案的資訊，請參閱 [根據檔案類型管理流量](#)，第 168 頁。

## 抽除內容

相關主題：

- ◆ [掃描選項](#)，第 129 頁
- ◆ [分類內容與掃描威脅](#)，第 129 頁
- ◆ [檔案掃描](#)，第 130 頁
- ◆ [優化掃描](#)，第 133 頁
- ◆ [即時掃描活動的報告](#)，第 134 頁

對您系統的威脅有可能隱藏在透過網頁傳送的主動式內容中。保持您系統完整性的其中一個方式是確保永遠不會收到這種內容。

Websense 即時選項可以指定從內送網頁中，將特定指令碼語言 (ActiveX、JavaScript 或 VB Script) 的內容抽除。如果啓用內容抽取，將從標幟為含有動態內容或顯示在「永遠掃描」清單中的網站內移除特定指令碼語言的所有內容 (請參閱[掃描選項](#)，第 129 頁)。

只有當即時選項已分類該網站，且 Websense 篩選軟體已決定要套用哪個政策之後，才會移除內容。



### 重要

依賴於已抽除之主動式內容的網站將無法如預期地運作。若要允許完整存取需要主動式內容的網站，請停用內容抽除或將該網站新增到「永不掃描」清單。

要求具有主動式內容之網頁的使用者不會收到任何有關該內容已被移除的通知。

使用[設定](#) > [即時掃描](#) > [常用選項](#)標籤可以指定何時要從具有動態內容的網站抽除內容。

1. 在「內容抽除」區域中，選取應該從內送網頁移除的主動式內容類型。
2. 若要變更其他即時選項的設定，請參閱：
  - [分類內容與掃描威脅](#)，第 129 頁
  - [檔案掃描](#)，第 130 頁
3. 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

若要針對任何已選擇的語言停用內容抽除，清除相關聯的核取方塊。

## 優化掃描

相關主題：

- ◆ [掃描選項](#)，第 129 頁
- ◆ [分類內容與掃描威脅](#)，第 129 頁
- ◆ [檔案掃描](#)，第 130 頁
- ◆ [抽除內容](#)，第 132 頁

使用「永遠掃描」與「永不掃描」清單來自訂「建議」與「全部」掃描選項的行為。

- ◆ 當即時選項設為「建議」或「開啓」時，則會掃描具有動態內容的網站和「永遠掃描」清單上的網站（請參閱[掃描選項](#)，第 129 頁）。「永不掃描」清單上的網站則會忽略。
- ◆ 當即時選項設為「全部」時，「永不掃描」清單上的網站也會忽略。這可以改善效能。

請小心使用「永不掃描」清單。如果此清單上的網站遭到入侵，Websense Security Gateway 仍不會掃描該網站，無法察覺安全問題。

使用**設定 > 即時掃描 > 例外**頁面以填寫及編輯「永遠掃描」與「永不掃描」清單。

若要新增網站至「永遠掃描」或「永不掃描」清單：

1. 在 **URL** 方塊中輸入網站名稱。  
僅輸入主機名稱（例如，**thissite.com**）。不需要輸入完整的 URL。請務必輸入網域和副檔名；**thissite.com** 和 **thissite.net** 是不同的項目。  
您一次可以輸入一個以上的主機名稱。
2. 在**選項**欄位中，選取要對您輸入的所有網站套用哪些即時選項。您可以選取一或多個選項。請注意，**安全威脅**只涉及內容掃描，不涉及檔案掃描。「永遠掃描」與「永不掃描」清單不會影響檔案掃描。  
若要對不同網站套用不同選項，請分別輸入網站。
3. 選取**新增至永遠掃描**或**新增至永不掃描**。  
同一個網站只能出現在這 2 個清單其中之一。例如，您不能指定同一個網站應該永遠掃描威脅但永不執行內容抽取。
  - 若要變更某網站應該出現在哪個清單，請先選取網站，然後使用向右箭頭 (>) 與向左箭頭 (<) 按鈕，將網站移至新清單。
  - 若要從這兩個清單中刪除網站，選取網站，然後按一下**移除**。
4. 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

若要變更與網站相關聯的掃描選項：

1. 在「永遠掃描」或「永不掃描」清單中選取網站，然後按一下**編輯**。
2. 在「編輯規則」方塊中，選取該主機名稱的新選項：
  - **不變更**會維持現有設定。
  - **開啓**表示會針對指定選項來掃描內容，例如內容分類。
  - **關閉**表示不會執行指定選項的掃描。如果關閉某個選項，則會改善效能，但可能會危及安全性。
3. 完成變更之後，按一下「編輯規則」方塊中的**確定**返回「例外」標籤。
4. 再按一次**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## 即時掃描活動的報告

相關主題：

- ◆ [掃描選項](#)，第 129 頁
- ◆ [分類內容與掃描威脅](#)，第 129 頁
- ◆ [檔案掃描](#)，第 130 頁
- ◆ [抽除內容](#)，第 132 頁

如果您的訂閱包括即時掃描功能，可以使用簡報報告與調查報告來分析這些功能的影響。

在「簡報報告」頁面上，有一個名為「即時安全威脅」的報告群組可以使用。這些報告特別鎖定與威脅有關的活動。就如同所有簡報報告一樣，您可以複製安全威脅報告，並在以該複本為基礎產生報告時，編輯複本的報告篩選器，以便修訂其中所包含的資訊。

有些安全威脅報告會包括「威脅 ID」欄位。您可以按一下個別的威脅 ID，開啓 Websense Security Labs 頁面，其中會說明辨識到的威脅類型。

此外，其他的簡報報告包含有關即時掃描活動以及標準篩選活動的資訊。複製預先定義的報告並編輯其篩選器，以建立專門針對即時掃描活動的報告。



### 重要

啓用完整 URL 記錄 (請參閱[設定完整 URL 記錄](#)，第 281 頁) 以確保即時掃描活動的報告是有意義的。否則，報告只能顯示已分類網站的網域 (www.domain.com)，即使該網站中的個別頁面屬於不同類別或包含不同威脅也一樣。

例如，在「報告目錄」的「網際網路活動」群組中的「依類別的完整 URL 細節」報告會提供每個類別中所存取的每個 URL 詳細清單。若要製作專屬於即時掃描的報告，複製「依類別的完整 URL 細節」報告並編輯其報告篩選器。在「動作」標籤上，僅選取與即時掃描有關的允許與封鎖動作。在「選項」標籤上，變更報告目錄標題與報告名稱，以便將它識別為即時掃描報告。例如，您可以將名稱與標題變更為「即時掃描：依類別的完整 URL 細節」。

調查報告可以用來深入瞭解即時掃描活動。

1. 在**網際網路使用者**下拉式清單中，選取「動作」。
2. 在結果報告中，按一下即時動作 (例如「即時封鎖類別」) 以顯示向下展開式選項的清單。
3. 按一下需要的向下展開式選項，例如「類別」或「使用者」。
4. 按一下「點選次數」值或任何列上的橫條，以檢視相關詳細資料。
5. 按一下位於頁面頂端的**更改報告**以便將「完整 URL」欄位來為新增至報告。  
如需有關使用所有調查報告功能的詳細資料，請參閱[調查報告](#)，第 102 頁。

## 即時掃描如何記錄

當您使用即時掃描選項時，請注意，標準網路篩選活動與即時掃描活動的記錄方式有所不同。

對於標準網路篩選，您有數個選項可以降低記錄資料庫的大小。

- ◆ 啟用**造訪次數**可以針對每個要求的網站僅記錄一個記錄。請參閱[設定記錄快取檔案](#)，第 271 頁。
- ◆ 啟用**合併**可以將具有特定共同元素的多個要求合併成單一 Log 記錄。請參閱[設定合併選項](#)，第 272 頁。
- ◆ 停用**完整 URL 記錄**可以僅記錄每個要求的網域名稱 (www.domain.com)，而不會記錄網域中特定網頁的路徑 (/products/productA)。請參閱[設定完整 URL 記錄](#)，第 281 頁。
- ◆ 啟用**選擇性類別記錄**可以將記錄限制在對貴組織很重要的已選擇類別。請參閱[設定用於記錄的 Filtering Service](#)，第 265 頁。

不過，即時掃描功能並不完全受這些設定的限制。當即時掃描在分析網站時，它會建立 2 個不同的 Log 記錄。

- ◆ **網路篩選器記錄**會使用已實施的所有減少大小的設定，而且可供所有網路篩選器報告使用。
- ◆ **即時記錄**會忽略大多數的減少大小設定。每次單獨的點選都會記錄，對所有類別的要求都會記錄，而且不會合併任何記錄。不論是否根據即時掃描結果而封鎖或允許網站，都會產生即時報告。針對即時記錄，只有完整 URL 記錄的設定會執行。

如果您已啟用任何記錄資料庫減少大小選項，那麼即時報告中顯示的數字可能會與標準篩選報告中顯示的數字不相符，即使那些報告都是針對相同使用者、時段與類別所設定，也是如此。例如，如果您選擇記錄造訪次數，而某個使用者要求了由即時掃描功能所分析的網站，那麼該使用者的要求會在標準篩選報告中顯示為一次造訪，但可能在即時報告中顯示多次點選。

若要檢視標準與即時篩選的可比較資料，**停用**記錄資料庫減少大小設定。由於這可能導致資料庫相當龐大且增長快速，因此請確定記錄資料庫電腦擁有足夠的硬碟、處理速度及記憶體容量。

如需有關設定減少大小設定的詳細資訊，請參閱[報告管理](#)，第 261 頁。如需有關產生報告的資訊，請參閱[簡報報告](#)，第 86 頁和[調查報告](#)，第 102 頁。



# 8

## 篩選遠端用戶端

相關主題：

- ◆ [Remote Filtering 的運作方式](#)，第 138 頁
- ◆ [設定 Remote Filtering 設定](#)，第 143 頁

對許多組織的使用者來說，他們有時候可能需要帶著筆記型電腦離開網路。對執行 Microsoft Windows 作業系統的遠端使用者來說，可實施 Websense Remote Filtering (Websense Web Security 和 Websense Web Filter 中的一項選用功能) 來篩選網際網路要求。

Remote Filtering 可監控 HTTP、SSL 和 FTP 流量，根據使用者登入遠端電腦的方式，套用指派給個別使用者或群組的政策或預設政策。Remote Filtering 不是根據指派給電腦或網路範圍的政策進行篩選。如需詳細資訊，請參閱 [識別遠端使用者](#)，第 141 頁。

遠端用戶端不支援以頻寬為基礎的篩選 (請參閱 [使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁)。頻寬量測和報告中並未包括遠端流量產生的頻寬。

只能封鎖或允許 FTP 和 SSL 要求 (例如 HTTPS) 的 Remote Filtering。例如，如果遠端使用者要求存取屬於某個被指派了配額或確認動作之類別的 FTP 網站或 HTTPS 網站，該網站便會對 Remote Filtering 用戶端封鎖。當這些電腦從網路內部瀏覽時，一般會套用配額和確認篩選動作。

若要實施 Remote Filtering，您必須安裝下列元件：

- ◆ Remote Filtering Server 必須安裝於最外邊的防火牆之內，而且遠端電腦必須能夠與它通訊。一般來說，它安裝於網路的 *非軍事區域* 或 DMZ，在保護網路其餘部份的防火牆之外。最多可安裝 3 個 Remote Filtering Server 來提供容錯移轉功能。

- ◆ Remote Filtering Client 必須安裝於執行 Windows 作業系統且在網路外部使用的每台電腦上。



#### 注意

請仔細遵照 *部署手冊* 中的建議部署這些元件。如需安裝指示，請參閱 *安裝手冊*。

如果在單機模式（沒有整合產品）下使用 Websense 軟體，請將 Network Agent 設定成不監控 Remote Filtering Server 機器（請參閱 [設定全域設定](#)，第 296 頁）。

Remote Filtering Client 和 Remote Filtering Server 之間的所有通訊都經過驗證並加密。

## Remote Filtering 的運作方式

---

相關主題：

- ◆ [網路內部](#)，第 139 頁
- ◆ [網路外部](#)，第 140 頁
- ◆ [識別遠端使用者](#)，第 141 頁
- ◆ [伺服器通訊若失敗](#)，第 141 頁
- ◆ [虛擬私人網路 \(VPN\)](#)，第 142 頁
- ◆ [設定 Remote Filtering 設定](#)，第 143 頁

每當遠端電腦提出 HTTP、SSL 或 FTP 要求時，其 Remote Filtering Client 便會與 Remote Filtering Server 通訊。Remote Filtering Server 再與 Websense Filtering Service 通訊，決定採取什麼動作。接下來 Remote Filtering Server 會回應 Remote Filtering Client，或者允許存取該網站，或者傳送適當的封鎖訊息。

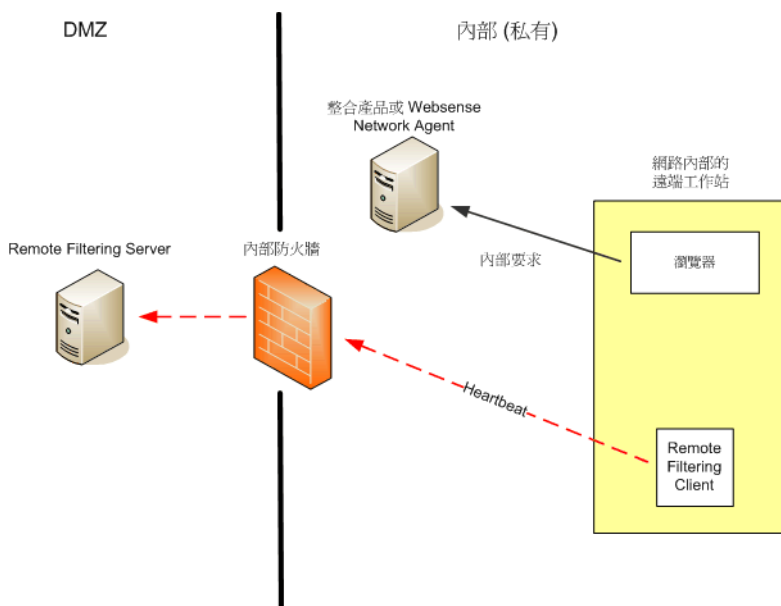
當執行 Remote Filtering Client 之電腦上的瀏覽器透過 HTTP、SSL 或 FTP 提出要求時，Remote Filtering Client 必須決定是否向 Remote Filtering Server 查詢要求。這項決定由與網路相關之電腦的位置控制。

## 網路內部

相關主題：

- ◆ [Remote Filtering 的運作方式](#)，第 138 頁
- ◆ [網路外部](#)，第 140 頁
- ◆ [識別遠端使用者](#)，第 141 頁
- ◆ [伺服器通訊若失敗](#)，第 141 頁
- ◆ [虛擬私人網路 \(VPN\)](#)，第 142 頁
- ◆ [設定 Remote Filtering 設定](#)，第 143 頁

當電腦在網路內部啟動時，Remote Filtering Client 會嘗試傳送活動訊號 (heartbeat) 到 DMZ 中的 Remote Filtering Server。由於 heartbeat 連接埠在內部防火牆上開啓，因此 heartbeat 會成功。



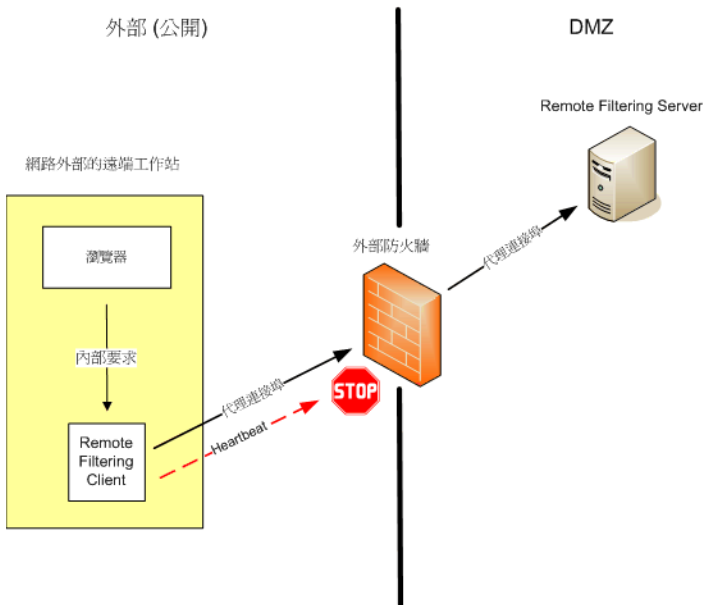
在此情況下，Remote Filtering Client 會變成被動而且不會向 Remote Filtering Server 查詢網際網路要求。而是將這些要求直接傳送到整合產品 (例如 Cisco Pix、Microsoft ISA Server) 或 Websense Network Agent。系統會使用與篩選其他內部要求相同的方法來篩選此要求。

## 網路外部

相關主題：

- ◆ [Remote Filtering 的運作方式](#)，第 138 頁
- ◆ [網路內部](#)，第 139 頁
- ◆ [識別遠端使用者](#)，第 141 頁
- ◆ [伺服器通訊若失敗](#)，第 141 頁
- ◆ [虛擬私人網路 \(VPN\)](#)，第 142 頁
- ◆ [設定 Remote Filtering 設定](#)，第 143 頁

當電腦在網路外部啟動時，Remote Filtering Client 會嘗試傳送 heartbeat 到 Remote Filtering Server。由於 heartbeat 連接埠被內部防火牆封鎖，因此 heartbeat 會失敗。



此 heartbeat 失敗會提示 Remote Filtering Client 透過設定的連接埠 (預設為 80)，將關於每個 HTTP、SSL 或 FTP 要求的查詢傳送到 DMZ 中的 Remote Filtering Server。接下來 Remote Filtering Server 會將篩選要求轉送到網路內部的 Websense Filtering Service。Filtering Service 會評估要求並傳送回應給 Remote Filtering Server。然後，將回應傳送給遠端電腦。如果網站被封鎖，Remote Filtering Client 會要求並收到適當的封鎖頁面，然後將其顯示給使用者。

Remote Filtering Client 會延遲每個已篩選的要求，直到它收到 Remote Filtering Server 的回應為止。Remote Filtering Client 再根據收到的回應，決定是允許存取網站或顯示封鎖頁面。

系統使用記錄檔追蹤 Remote Filtering 活動，例如進入和離開網路、無法開啓或關閉，以及重新啓動用戶端。Remote Filtering Client 會在第一次啓動時建立此記錄檔。可控制此記錄檔的存在情況和大小。請參閱 [設定 Remote Filtering 設定](#)，第 143 頁。

## 識別遠端使用者

相關主題：

- ◆ [Remote Filtering 的運作方式](#)，第 138 頁
- ◆ [網路內部](#)，第 139 頁
- ◆ [網路外部](#)，第 140 頁
- ◆ [伺服器通訊若失敗](#)，第 141 頁
- ◆ [虛擬私人網路 \(VPN\)](#)，第 142 頁
- ◆ [設定 Remote Filtering 設定](#)，第 143 頁

使用者登入遠端電腦的方式決定了應強制執行的政策。

如果使用者使用快取的網域認證 (網路目錄登入資訊) 登入，Websense Filtering Service 能夠解析使用者名稱，並將適當的使用者和群組政策套用至遠端電腦。同時，將網際網路活動記錄在網路使用者名稱下。

如果使用者使用本機電腦的使用者帳戶登入，Filtering Service 將無法解析使用者名稱，而是套用預設政策。網際網路活動將記錄在本機使用者名稱下。Remote Filtering 不是根據指派給電腦或網路範圍的政策進行篩選。



### 注意

系統一律根據遠端使用者的登入認證來篩選遠端使用者，如此處所述。選擇性驗證設定不適用於這些使用者。

## 伺服器通訊若失敗

相關主題：

- ◆ [Remote Filtering 的運作方式](#)，第 138 頁
- ◆ [網路內部](#)，第 139 頁
- ◆ [網路外部](#)，第 140 頁
- ◆ [識別遠端使用者](#)，第 141 頁
- ◆ [虛擬私人網路 \(VPN\)](#)，第 142 頁
- ◆ [設定 Remote Filtering 設定](#)，第 143 頁

當網路外部的 Remote Filtering Client 與網路 DMZ 中的 Remote Filtering Server 成功進行通訊時，便會開始篩選。不過，通訊有時候也可能會失敗。

當 Remote Filtering Client 無法與 Remote Filtering Server 通訊時可以設定其所採取的動作。在預設情況下，Remote Filtering Client 會使用**無法開啓**設定，此設定允許在無法在這些元件之間建立通訊時，接受所有 HTTP、SSL 和 FTP 要求。

Remote Filtering Client 會繼續嘗試與 Remote Filtering Server 通訊。成功建立通訊時，便會強制行適當的篩選政策。

當 Remote Filtering Client 設定成**失敗則關閉**時，會套用一個逾時值 (預設為 15 分鐘)。當遠端電腦啟動時，就會開始計時。Remote Filtering Client 會立即嘗試連線至 Remote Filtering Server，並且持續循環可用的 Remote Filtering Server，直到成功為止。

如果使用者一啟動就可以存取網路，那麼在 Remote Filtering Client 連線至 Remote Filtering Server 之前，將不會進行任何篩選 (允許所有要求)。開始篩選時，會強制行適當的篩選政策。

若 Remote Filtering Client 無法在設定的逾時期間內連線，所有網際網路存取均會被封鎖 (失敗則關閉)，直到可以建立 Remote Filtering Server 連線為止。



#### 注意

如果 Remote Filtering Server 因任何原因而無法連線至 Websense Filtering Service，則會傳回錯誤給 Remote Filtering Client，而且一律不會開啓篩選。

這個逾時期間讓旅行中且需要付費存取網際網路的使用者能夠在不會登出的情況下啟動電腦和安排連線。如果使用者未在 15 分鐘的逾時期間內建立網路存取，就無法在該工作階段建立網路存取。發生此情況時，使用者必須重新啟動電腦，以重新開始逾時間隔。

若要變更無法開啓/失敗則關閉設定以及逾時值，請參閱[設定 Remote Filtering 設定](#)，第 143 頁。

## 虛擬私人網路 (VPN)

相關主題：

- ◆ [Remote Filtering 的運作方式](#)，第 138 頁
- ◆ [網路內部](#)，第 139 頁
- ◆ [網路外部](#)，第 140 頁
- ◆ [識別遠端使用者](#)，第 141 頁
- ◆ [伺服器通訊若失敗](#)，第 141 頁
- ◆ [設定 Remote Filtering 設定](#)，第 143 頁

Websense Remote Filtering 支援 VPN 連線，包括分割通道 VPN。當遠端電腦透過 VPN (非分割通道) 連線至內部網路時，Remote Filtering Client 可以傳送 heartbeat 到 Remote Filtering Server。因此，Remote Filtering Client 會變成被動，並且所有遠端電腦發出的 HTTP、SSL、和 FTP 要求均會由內部整合產品或 Network Agent 篩選，就像其他網路內的電腦一樣。

如果遠端電腦透過分割通道 VPN 用戶端連線至內部網路，Remote Filtering Client 會偵測此連線但不會傳送 heartbeat 到 Remote Filtering Server。Remote Filtering Client 會假設這是外部作業，然後提交要求到 Remote Filtering Server 以進行篩選。

Websense 軟體支援下列 VPN 用戶端的分割通道：

- ◆ Checkpoint SecureClient
- ◆ Cisco
- ◆ Juniper/Netscreen
- ◆ Microsoft PPTP
- ◆ Nokia
- ◆ Nortel
- ◆ SonicWALL

## 設定 Remote Filtering 設定

相關主題：

- ◆ [Remote Filtering 的運作方式](#)，第 138 頁
- ◆ [網路內部](#)，第 139 頁
- ◆ [網路外部](#)，第 140 頁
- ◆ [識別遠端使用者](#)，第 141 頁
- ◆ [伺服器通訊若失敗](#)，第 141 頁
- ◆ [虛擬私人網路 \(VPN\)](#)，第 142 頁

無條件的「超級管理員」可使用**設定 > 一般 > Remote Filtering** 頁面，設定會影響與此安裝有關之所有 Remote Filtering Client 的選項。

如需 Remote Filtering 運作方式的詳細資訊，請參閱 [Remote Filtering 的運作方式](#)，第 138 頁。

1. 核取**失敗則關閉**方塊，即可在 Remote Filtering Client 與 Remote Filtering Server 進行通訊之前，封鎖它們所有的網際網路存取。  
在預設情況下，不會核取此方塊，表示當遠端使用者的電腦無法與 Remote Filtering Server 進行通訊時，他們可以在不經過篩選的情況下存取網際網路。
2. 如果核取了「失敗則關閉」選項，在**失敗則關閉逾時**欄位選擇時間（最長為 60 分鐘，預設為 15 分鐘），或者選擇**無逾時**。  
在逾時期間內，所有 HTTP、SSL 和 FTP 要求均會被允許。  
如果 Remote Filtering Client 無法在逾時間隔內與 Remote Filtering Server 進行通訊，所有網際網路存取都將被封鎖（失敗則關閉）。

若選取**無逾時**，遠端電腦可能會在使用者從酒店或其他付費提供者建立網際網路連線之前被鎖定。除此以外，Remote Filtering Client 會持續嘗試與 Remote Filtering Server 進行通訊。



**警告**

Websense, Inc. 不建議選取**無逾時**，或者將逾時期間設成很小的值。

---

3. 選取**本機記錄快取的大小上限** (MB)，最大為 10 MB。如果選取**無記錄**，則會停用記錄。

這樣可控制遠端電腦初次中斷與 Remote Filtering Server 連線時建立的記錄檔大小和存在情況。此記錄檔可追蹤下列事件：

- 電腦離開網路
- 電腦重新加入網路
- Remote Filtering Client 重新啓動
- 發生無法開啓的情況
- 發生無法關閉的情況
- Remote Filtering Client 收到政策更新

電腦會保留 2 個最新的記錄。這些記錄可用於排除連線故障或其他 Remote Filtering 問題。



# 9

## 優化篩選政策

網際網路使用篩選的最簡單形式只需要單個政策，此政策套用一個類別篩選器以及一個通訊協定篩選器，一天 24 小時，一週 7 天。然而，Websense 軟體提供的工具遠超過這項基本的篩選功能，讓您能夠精確的達到管理網際網路使用所需的資料層次。您可以：

- ◆ 建立**限制存取篩選器**，只允許特定的使用者存取指定的網站，其他的則一律封鎖存取 (請參閱[將使用者限制於定義的網際網路網站清單](#)，第 145 頁)。
- ◆ 建立**自訂類別**，重新定義篩選所選網站的方式 (請參閱[使用類別](#)，第 152 頁)。
- ◆ **重新分類 URL**，將特定網站從預設的 Master Database 類別移到另一個 Websense 定義或自訂的類別 (請參閱[重新分類 URL](#)，第 160 頁)。
- ◆ 定義**未篩選的 URL**，讓使用者能夠存取特定的網站，即使已指派該網站給已啟用類別篩選器之某個封鎖類別 (請參閱[定義未篩選的 URL](#)，第 159 頁)。
- ◆ 實行**頻寬限制**，即在頻寬使用達到指定的臨界值之後，不讓使用者存取以其他方式允許的類別和通訊協定。
- ◆ 定義**關鍵字**，在啟用並啟動關鍵字封鎖功能時，用以封鎖以其他方式允許之類別的網站 (請參閱[根據關鍵字篩選](#)，第 156 頁)。
- ◆ 定義**檔案類型**，在啟動檔案類型封鎖功能時，用以禁止下載以其他方式允許之類別的所選檔案類型 (請參閱[根據檔案類型管理流量](#)，第 168 頁)。

### 將使用者限制於定義的網際網路網站清單

---

相關主題：

- ◆ [限制存取篩選器與篩選優先權](#)，第 146 頁
- ◆ [建立限制存取篩選器](#)，第 147 頁
- ◆ [編輯限制存取篩選器](#)，第 148 頁

限制存取篩選器提供了一個非常精確的網際網路存取篩選方法。每個限制存取篩選器都是一份個別的網站清單。就像類別篩選器，限制存取篩選器也會加到政策中，並且在指定的期間內強制實行。當政策中的限制存取篩選器為作用中狀態時，被指派該政策的使用者將只能夠瀏覽清單中的網站。其他所有網站均被封鎖。

例如，若「第一級」政策實行只包含特定教育與參考網站的限制存取篩選器，那麼由「第一級」政策管理的學生就只能瀏覽這些網站，除此以外的網站均無法存取。



### 重要

套用限制存取篩選器時，Websense 軟體只會檢查要求的網站是否出現在篩選器中。不會執行其他額外檢查。

這表示若某個篩選器允許存取的網站感染了惡意程式碼，不管網站之 Master Database 或「即時掃描」的分類為何，還是會允許存取該網站的使用者要求。

當限制存取篩選器為作用中狀態時，若要求存取該篩選器未包含的 URL，均會傳回封鎖頁面。

Websense 軟體最多可支援 2,500 個限制存取篩選器，可包含的 URL 總數為 25,000 個。

## 限制存取篩選器與篩選優先權

在某些情況下，可對一位使用者套用一個以上的篩選政策。例如，若某位使用者隸屬於一個以上的群組，且這些群組由不同的政策管理時，就可能發生此情況。另一種情況是，某個 URL 除了是限制存取篩選器中的一個項目外，同時也定義為未篩選的 URL。

在多個群組政策套用至一位使用者時，將由**使用更為嚴格的封鎖**設定（請參閱[篩選順序](#)，第 71 頁）決定篩選使用者的方式。這項設定預設為關閉的狀態。

Websense 軟體會決定篩選器層次之哪個篩選設定的限制性較低。例如，使用多個政策篩選一位使用者，且其中一個政策實行限制存取篩選器，「限制性較低」有時可能會讓人直覺上覺得有點矛盾。

當**使用更為嚴格的封鎖**為關閉時：

- ◆ 如果可同時套用**全部封鎖**類別篩選器和限制存取篩選器，則限制存取篩選器的限制性一律比較低。
- ◆ 如果可同時套用其他類別篩選器和限制存取篩選器，類別篩選器的限制性會比較低。

這代表即使限制存取篩選器允許存取網站，如果類別篩選器封鎖網站，網站還是會被封鎖。

當**使用更為嚴格的封鎖**為開啓時，限制存取篩選器的限制性會高於除「全部封鎖」外的其他類別篩選器。

下表摘要說明了在能夠套用多個政策的情況下，**使用更為嚴格的封鎖**設定對篩選的影響：

	<i>使用更為嚴格的封鎖關閉</i>	<i>使用更為嚴格的封鎖開啓</i>
限制存取篩選器 + <b>全部封鎖</b> 類別篩選器	限制存取篩選器 (允許要求)	<b>全部封鎖</b> (封鎖要求)
限制存取篩選器 + 允許的類別	類別篩選器 (允許要求)	限制存取篩選器 (允許要求)
限制存取篩選器 + 封鎖的類別	類別篩選器 (封鎖要求)	限制存取篩選器 (允許要求)
限制存取篩選器 + 配額/確認類別	類別篩選器 (配額/確認限制的要求)	限制存取篩選器 (允許要求)
限制存取篩選器 + 未篩選的 URL	未篩選的 URL (允許要求)	限制存取篩選器 (允許要求)

## 建立限制存取篩選器

相關主題：

- ◆ [使用篩選器](#)，第 42 頁
- ◆ [將使用者限制於定義的網際網路網站清單](#)，第 145 頁
- ◆ [編輯限制存取篩選器](#)，第 148 頁

在**新增限制存取篩選器**頁面 (從**篩選器**或**編輯政策**頁面存取) 中輸入新篩選器的唯一名稱和說明。建立篩選器之後，請輸入一份允許的 URL 清單，指派篩選器給某個政策，然後將政策套用至用戶端。

- 輸入唯一的**篩選器名稱**。名稱長度必須介於 1 到 50 個字元之間，且不能包含下列任何字元：

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

篩選器名稱可包含空格、橫線和單引號。

- 輸入篩選器的簡短**說明**。此說明會顯示在「篩選器」頁面之「限制存取篩選器」區段中的篩選器名稱旁邊，且應說明篩選器的目的，以協助管理員以後管理政策。

適用於篩選器名稱的字元限制也適用於說明，但有 2 個例外：說明可包含句點 (.) 和逗號 (,)。

- 若要查看及編輯新篩選器，請按一下**確定**。若要放棄變更並返回「篩選器」頁面，按一下**取消**。

您建立的新限制存取篩選器會增加到**政策管理 > 篩選器 > 限制存取篩選器**清單中。按一下篩選器名稱，編輯該篩選器。

要完成自訂新篩選器，請繼續[編輯限制存取篩選器](#)。

## 編輯限制存取篩選器

相關主題：

- ◆ [將使用者限制於定義的網際網路網站清單](#)，第 145 頁
- ◆ [限制存取篩選器與篩選優先權](#)，第 146 頁
- ◆ [建立限制存取篩選器](#)，第 147 頁
- ◆ [編輯政策](#)，第 68 頁

限制存取篩選器是一份網站 (URL 或 IP 位址) 和正規表示式清單，用以識別使用者可以存取的特定網站。將此篩選器套用至用戶端時，用戶端即無法瀏覽任何清單中未包含的網站。



### 重要

套用限制存取篩選器時，Websense 軟體只會檢查要求的網站是否出現在篩選器中。不會執行其他額外檢查。

這表示若某個篩選器允許存取的網站感染了惡意程式碼，不管網站之 Master Database 或「即時掃描」的分類為何，還是會允許存取該網站的使用者要求。

可使用 [政策管理](#) > [篩選器](#) > [編輯限制存取篩選器](#) 頁面變更現有限制存取篩選器。您可以變更篩選器名稱和說明、檢視強制執行篩選器的政策的清單，以及管理篩選器中應該包含的網站。

編輯限制存取篩選器時，所做的變更會影響強制執行篩選器的每個政策。

1. 確認篩選器名稱與說明。要變更篩選器名稱，按一下 **重新命名**，然後輸入新名稱。系統會將新的名稱更新到強制執行所選限制存取篩選器的所有政策中。
2. 可使用 **使用此篩選器的政策** 欄位來查看目前有多少政策強制執行此篩選器。若有一個或多個政策強制執行此篩選器，按一下 **檢視政策** 可列示它們。
3. 在「新增或移除網站」底下，輸入要新增至限制存取篩選器的 URL 和 IP 位址。每一行只能輸入一個 URL 或 IP 位址。

不需要包含 HTTP:// 前置碼。

若根據網站的 Master Database 類別篩選網站，Websense 軟體會將 URL 與其對等的 IP 位址進行比對。但對於限制存取篩選器情況就不是這樣。若要允許網站的 URL 和 IP 位址，請將這兩者新增至篩選器。

4. 按一下向右箭頭 (>)，將 URL 和 IP 位址移至允許的網站清單中。
5. 除了新增個別網站至限制存取篩選器之外，也可以新增比對多個網站的正規表示式。若要建立正規表示式，按一下 **進階**。
  - 一行輸入一個正規表示式，然後按向右箭頭，將表示式移到允許的網站清單中。
  - 若要驗證正規表示式是否能夠比對想要的網站，按一下 **測試**。

- 如需有關使用正規表示式進行篩選的詳細資訊，請參閱 [使用正規表示式](#)，第 170 頁。
6. 檢閱**允許的網站**清單中的 URL、IP 位址和正規表示式。
    - 若要變更某個網站或正規表示式，選取它並按一下**編輯**。
    - 若要移除清單中的網站或正規表示式，選取它並按一下**刪除**。
  7. 在編輯篩選器後，請按一下**確定**以快取所做的變更，並返回「篩選器」頁面。按一下**全部儲存**後，才會執行變更。

## 從「編輯政策」頁面新增網站

相關主題：

- ◆ [將使用者限制於定義的網際網路網站清單](#)，第 145 頁
- ◆ [限制存取篩選器與篩選優先權](#)，第 146 頁
- ◆ [建立限制存取篩選器](#)，第 147 頁
- ◆ [編輯政策](#)，第 68 頁

可使用**政策 > 編輯政策 > 新增網站**頁面，將網站新增到限制存取篩選器。

每一行只能輸入一個 URL 或 IP 位址。如果您未指定通訊協定，Websense 軟體會自動加上 **HTTP://** 前置碼。

完成變更之後，按一下**確定**以返回「編輯政策」頁面。還必須按一下「編輯政策」頁面中的**確定**來快取變更。按一下**全部儲存**後，才會執行變更。

對限制存取篩選器所做的變更會影響強制執行該篩選器的所有政策。

## 將篩選器和政策複製到角色

相關主題：

- ◆ [建立類別篩選器](#)，第 43 頁
- ◆ [建立通訊協定篩選器](#)，第 45 頁
- ◆ [建立限制存取篩選器](#)，第 147 頁
- ◆ [建立政策](#)，第 68 頁

「超級管理員」可以使用**篩選器 > 將篩選器複製到角色**和**政策 > 將政策複製到角色**頁面，將一或多個篩選器或政策複製到委派的管理角色。複製篩選器或政策之後，委派的管理員就可以使用篩選器或政策來篩選他們管理的用戶端。

- ◆ 在目標角色中，系統會在篩選器或政策名稱的結尾加上「(已複製)」標記。若相同的篩選器或政策複製了多次，就會加上數字。
- ◆ 委派的管理員可以重新命名或編輯複製到其角色的篩選器或政策。
- ◆ 複製到委派管理角色的類別篩選器會設定允許在角色中建立自訂類別的篩選動作。委派的管理員應該更新複製的類別篩選器，以為其角色專用的自訂類別設定想要執行的動作。
- ◆ 委派的管理員對「超級管理員」複製到其角色的篩選器或政策所做的變更，並不會影響「超級管理員」的原始篩選器或政策，或者接收到該篩選器或政策複本的其他角色。
- ◆ 「篩選器鎖定」限制不會影響「超級管理員」的原始篩選器或政策，但是會影響委派之管理員的篩選器或政策複本。
- ◆ 由於委派的管理員會受「篩選器鎖定」限制影響，因此無法將「全部允許」類別和通訊協定篩選器複製到委派的管理角色。

複製篩選器或政策：

1. 在「將篩選器複製到角色」或「將政策複製到角色」頁面，檢查頁面頂端的清單中顯示的政策或篩選器是否正確。
2. 從**選取角色**下拉式清單中選取一個目的角色。
3. 按一下**確定**。

此時會顯示一個彈出式對話方塊，指示正在複製選取的篩選器或政策。複製作業可能需要一些時間才會完成。

按一下**全部儲存**後，才會執行變更。

複製作業完成之後，下次委派的管理員登入 **Websense Manager** 時，就可以在選取的角色中使用複製的篩選器或政策。如果委派的管理員在複製篩選器或政策時已登入具政策存取權的角色，那麼他們要先登出並再登入之後，才會見到新的篩選器或政策。

## 建立篩選器元件

可以從**政策管理 > 篩選器元件**頁面，存取用來優化及自訂 Websense 軟體如何強制執行您組織之網際網路存取政策的工具。此畫面中包含與下列工作相關的 4 個按鈕：

<b>編輯類別</b>	<ul style="list-style-type: none"> <li>• 重新分類 URL (請參閱<a href="#">重新定義特定網站的篩選</a>, 第 158 頁)。例如, 若您的網際網路篩選政策封鎖了「購物」類別, 但您想允許存取特定提供者或夥伴網站, 您就可以將這些網站移至允許的類別, 例如「商業與經濟」。</li> <li>• 定義或編輯自訂類別 (請參閱<a href="#">建立自訂類別</a>, 第 154 頁)。在 Websense 定義的上層類別或使用者定義的上層類別內建立其他下層類別, 然後將 URL 指派給新的類別。</li> <li>• 將關鍵字指派給類別 (請參閱<a href="#">根據關鍵字篩選</a>, 第 156 頁)。若要重新分類並封鎖對 URL 包含特定字串之網站的存取, 請先定義關鍵字, 然後在類別篩選器中啟用關鍵字封鎖功能。</li> <li>• 建立可用以比對多個 URL 的正規表示式 (請參閱<a href="#">使用正規表示式</a>, 第 170 頁)、樣式或範本, 然後將它們指派給類別。</li> </ul>
<b>編輯通訊協定</b>	<p>定義或編輯自訂通訊協定定義 (請參閱<a href="#">建立自訂通訊協定</a>, 第 164 頁和<a href="#">編輯自訂通訊協定</a>, 第 162 頁)。例如, 如果您組織的成員使用自訂訊息工具, 那麼您可以建立一個自訂通訊協定定義, 以允許使用該工具且同時封鎖其他即時訊息傳送通訊協定。</p>
<b>檔案類型</b>	<p>建立或編輯檔案類型定義, 用以封鎖其他允許類別內之特定類型的檔案 (請參閱<a href="#">根據檔案類型管理流量</a>, 第 168 頁)。</p>
<b>未篩選的 URL</b>	<p>定義允許所有用戶端存取特定網站, 即使其屬於封鎖類別 (請參閱<a href="#">定義未篩選的 URL</a>, 第 159 頁)。請注意, 新增 URL 至這份清單並不會覆寫「全部封鎖」類別篩選器或限制存取篩選器。</p>

## 使用類別

相關主題：

- ◆ [編輯類別及其屬性](#)，第 152 頁
- ◆ [建立自訂類別](#)，第 154 頁
- ◆ [根據關鍵字篩選](#)，第 156 頁
- ◆ [重新定義特定網站的篩選](#)，第 158 頁

Websense 軟體提供多種供用於篩選不在 Master Database 中的網站，以及變更篩選 Master Database 中個別網站之方式的方法。

- ◆ 建立可更精確篩選與報告的**自訂類別**。
- ◆ 使用已**重新分類的 URL**來定義未分類之網站的類別，或者變更出現在 Master Database 中的網站類別。
- ◆ 定義**關鍵字**，將 URL 包含特定字串的所有網站重新分類。

## 編輯類別及其屬性

相關主題：

- ◆ [建立自訂類別](#)，第 154 頁
- ◆ [檢閱所有自訂的類別屬性](#)，第 153 頁
- ◆ [進行全域類別篩選變更](#)，第 153 頁
- ◆ [根據關鍵字篩選](#)，第 156 頁
- ◆ [重新定義特定網站的篩選](#)，第 158 頁

可使用**政策管理 > 篩選器元件 > 編輯類別**頁面建立及修改自訂類別、已重新分類的 URL 和關鍵字。

現有類別 (包含 Websense 定義和自訂類別) 會列在內容窗格的左邊。若要檢視某個類別相關的現有自訂設定，或者建立新的自訂定義，請先從清單中選取一個類別。

若要檢視與所有類別相關的全部自訂 URL、關鍵字和正規表示式清單，按一下頁面最上方之工具列中的**檢視所有的自訂 URL / 關鍵字**。如需詳細資訊，請參閱[檢閱所有自訂的類別屬性](#)，第 153 頁。

- ◆ 若要建立新的類別，按一下**新增**，然後前往[建立自訂類別](#)，第 154 頁瞭解進一步的指示。

若要移除現有的自訂類別，請選取類別，然後按一下**刪除**。您無法刪除 Websense 定義的類別。



- ◆ 若要變更自訂類別的名稱或說明，請選取類別，然後按一下**重新命名**（請參閱[重新命名自訂類別](#)，第 154 頁）。
- ◆ 若要變更所有類別篩選器中與類別有關的篩選動作，按一下**覆寫動作**（請參閱[進行全域類別篩選變更](#)，第 153 頁）。
- ◆ **已重新分類的 URL** 清單中顯示的是指派給此類別的已重新分類網站 (URL 和 IP 位址)。
  - 若要新增網站至清單，按一下**新增 URL**。如需進一步的指示，請參閱[重新分類 URL](#)，第 160 頁。
  - 若要變更現有的重新分類網站，請選取 URL 或 IP 位址，然後按一下**編輯**。
- ◆ **關鍵字**清單中顯示的是與此類別相關的關鍵字。
  - 若要定義與所選類別有關的關鍵字，按一下**新增關鍵字**。如需進一步的指示，請參閱[根據關鍵字篩選](#)，第 156 頁。
  - 若要變更現有的關鍵字定義，請選取關鍵字，然後按一下**編輯**。
- ◆ 除了 URL 和關鍵字之外，您也可以替類別定義**正規表示式**。每個正規表示式均是用以讓多個網站與類別關聯的樣式或範本。
 

若要檢視或建立類別的正規表示式，按一下**進階**。

  - 若要定義正規表示式，按一下「新增表示式」（請參閱[使用正規表示式](#)，第 170 頁）。
  - 若要變更現有的正規表示式，請選取表示式，然後按一下**編輯**。
- ◆ 若要刪除已重新分類的 URL、關鍵字或正規表示式，請選取要移除的項目，然後按一下**刪除**。

完成變更「編輯類別」頁面後，按一下**確定**來快取變更並返回「篩選器元件」頁面。按一下**全部儲存**才能使變更生效。

## 檢閱所有自訂的類別屬性

使用**篩選器元件 > 編輯類別 > 檢視所有的自訂 URL 和關鍵字**頁面，檢閱自訂 URL、關鍵字和正規表示式的定義。您也可以刪除已經不需要的定義。

此頁面有 3 個類似的表格，每個類別屬性一個表格：自訂 URL、關鍵字或正規表示式。在每個表格中，屬性列在它相關之類別的名稱旁邊。

若要刪除類別屬性，請標記適當的核取方塊，然後按一下**刪除**。

若要返回「編輯類別」頁面，按一下**關閉**。如果刪除了「檢視所有的自訂 URL 和關鍵字」頁面中的任何項目，按一下「編輯類別」頁面中的**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## 進行全域類別篩選變更

使用**篩選器元件 > 編輯類別 > 覆寫動作**頁面變更套用至所有現有類別篩選器中之某個類別的動作。這同時決定了套用至新篩選器中類別的預設動作。

雖然此變更會覆寫套用至所有現有篩選器中之類別的動作，管理員稍後還是可以編輯這些篩選器，以套用不同的動作。

變更套用至類別的篩選設定之前，請先驗證已選擇類別旁邊顯示的類別名稱是否正確。接下來，您可以：

1. 選擇新的**動作**（「允許」、「封鎖」、「確認」或「配額」）。如需詳細資訊，請參閱[篩選動作](#)，第 39 頁。  
根據預設，頁面中的所有選項均設為**請勿變更目前的設定**。
2. 指定是否要**封鎖關鍵字**。如需詳細資訊，請參閱[根據關鍵字篩選](#)，第 156 頁。
3. 指定是否要**封鎖檔案類型**，然後自訂封鎖設定。如需詳細資訊，請參閱[根據檔案類型管理流量](#)，第 168 頁。
4. 在**進階篩選**底下，指定是否使用 Bandwidth Optimizer 來管理 HTTP 網站的存取，以及自訂封鎖設定。如需詳細資訊，請參閱[使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁。



#### 重要

在此處所做的變更會影響**全部封鎖**和**全部允許**以外的每個現有類別篩選器。

5. 按一下**確定**以返回「編輯類別」頁面（請參閱[編輯類別及其屬性](#)，第 152 頁）。系統要等到您按一下「編輯類別」頁面中的**確定**之後才會快取變更。

## 重新命名自訂類別

使用[篩選器元件](#) > [編輯類別](#) > [重新命名類別](#)頁面變更自訂類別的名稱或說明。

- ◆ 使用**篩選器名稱**欄位編輯類別名稱。新的名稱必須為唯一，而且不可超過 50 個字元。  
名稱不可包含下列任一字元：  
\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,
- ◆ 使用**說明**欄位編輯類別說明。說明不可超過 255 個字元。  
適用於篩選器名稱的字元限制也適用於說明，但有 2 個例外：說明可包含句點 (.) 和逗號 (,)。

完成變更之後，按一下**確定**以返回「編輯類別」頁面。系統要等到您按一下「編輯類別」頁面中的**確定**之後才會快取變更。

## 建立自訂類別

相關主題：

- ◆ [編輯類別及其屬性](#)，第 152 頁
- ◆ [根據關鍵字篩選](#)，第 156 頁
- ◆ [重新定義特定網站的篩選](#)，第 158 頁

除了使用 Master Database 中超過 90 個以上 Websense 定義的類別之外，您也可以定義自己的**自訂類別**以提供更精確的篩選與報告。例如，建立自訂類別，像是：

- ◆ **出差**：將核准之廠商的網站群組在一起，供員工用來購買機票以及預定租賃車輛和飯店。
- ◆ **參考材料**：將適合國小學生的線上字典和百科全書網站群組在一起。
- ◆ **專業開發**：將可提昇員工技能的訓練網站和其他資源群組在一起。

使用**政策管理 > 篩選器元件 > 編輯類別 > 新增類別**頁面將自訂類別新增到任何上層類別。最多可以建立 100 個自訂類別。

1. 輸入唯一的描述性**類別名稱**。名稱不可包含下列任一字元：

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

2. 輸入新類別的**說明**。

適用於篩選器名稱的字元限制也適用於說明，但有 2 個例外：說明可包含句點 (.) 和逗號 (,)。

3. 從**新增到**清單中選取一個上層類別。根據預設，會選取**所有類別**。

4. 輸入要新增至此類別的網站 (URL 或 IP 位址)。如需詳細資訊，請參閱[重新分類 URL](#)，第 160 頁。

您也可以在建立類別之後編輯這份清單。

5. 輸入要使其與此類別相關聯的關鍵字。如需詳細資訊，請參閱[根據關鍵字篩選](#)，第 156 頁。

您也可以在建立類別之後編輯這份清單。

6. 定義要套用至所有現有類別篩選器中此類別的預設篩選**動作**。您可於稍後編輯個別篩選器中的這個動作。



#### 注意

複製到委派管理角色的類別篩選器會設定允許在角色中建立自訂類別的篩選動作。委派的管理員應該更新複製的類別篩選器，以為其角色專用的自訂類別設定想要執行的動作。

7. 啓用應該要套用至所有現有類別篩選器中此類別的**進階篩選**動作 (關鍵字封鎖、檔案類型封鎖或頻寬封鎖)。

8. 完成定義新類別之後，按一下**確定**來快取變更並返回「編輯類別」頁面。按一下**全部儲存**才能使變更生效。

新類別會新增至「類別」清單中，並且顯示類別的自訂 URL 和關鍵字資訊。

## 根據關鍵字篩選

相關主題：

- ◆ [重新分類 URL](#)，第 160 頁
- ◆ [設定 Websense 篩選設定](#)，第 49 頁
- ◆ [建立類別篩選器](#)，第 43 頁
- ◆ [編輯類別篩選器](#)，第 44 頁
- ◆ [使用類別](#)，第 152 頁

關鍵字與類別相關，主要用以保護尚未明確加到 Master Database 或定義為自訂 URL 的網站。啟用關鍵字封鎖有 3 個必要的步驟：

1. 在全域層次啟用關鍵字封鎖 (請參閱 [設定 Websense 篩選設定](#)，第 49 頁)。
2. 定義與類別有關的關鍵字 (請參閱 [定義關鍵字](#)，第 157 頁)。
3. 啓用作用中類別篩選器中類別的關鍵字封鎖功能 (請參閱 [編輯類別篩選器](#)，第 44 頁)。

為特定類別定義關鍵字並啟用關鍵字封鎖之後，Websense 軟體就會封鎖 URL 包含關鍵字的所有網站，並將網站記錄為屬於指定的類別。即使類別中有其他允許的 URL，還是會封鎖網站。

例如，若「體育運動」類別是作用中類別篩選器的允許項目，但是您想封鎖對籃球網站的存取，您可以設定關鍵字“nba”與「體育運動」的關聯，然後啟用關鍵字封鎖功能。也就是說，下列 URL 會被封鎖，並將它們記錄為屬於「體育運動」類別：

- ◆ sports.espn.go.com/nba/
- ◆ modernbakery.com
- ◆ modernbabiesandchildren.com
- ◆ fashionbar.com

定義關鍵字時，請務必注意避免非計畫封鎖。



### 重要

如果您使用 Websense Web Security，請避免讓關鍵字與任何「延伸的防護」下層類別產生關聯。這些類別未強制執行關鍵字封鎖。

根據關鍵字封鎖要求時，使用者會在收到的 Websense 封鎖頁面看見指示。

## 定義關鍵字

相關主題：

- ◆ [編輯類別篩選器](#)，第 44 頁
- ◆ [使用類別](#)，第 152 頁
- ◆ [根據關鍵字篩選](#)，第 156 頁
- ◆ [使用正規表示式](#)，第 170 頁

關鍵字是一個可能在 URL 中找到的字元字串 (例如單字、詞句或縮寫)。將關鍵字指派給類別，然後在類別篩選器啓用關鍵字封鎖功能。

使用 [政策管理](#) > [篩選器元件](#) > [編輯類別](#) > [新增關鍵字](#) 頁面設定關鍵字與類別的關聯。如果您需要變更關鍵字定義，請使用 [編輯關鍵字](#) 頁面。

定義關鍵字時，請務必注意避免非計畫封鎖。例如，使用關鍵字“sex”封鎖對成人網站的存取，但導致搜尋引擎無法提供像 sextuplets 或 City of Essex，以及像 [msexchange.org](#) (資訊科技)、[vegasexperience.com](#) (旅行) 和 [sci.esa.int/marsexpress](#) (教育協會) 等網站的資訊。

每一行輸入一個關鍵字。

- ◆ 請勿在關鍵字中包含空格。URL 和 CGI 字串的字與字之間不含任何空格。
- ◆ 在特殊字元之前加上反斜線 (\)，例如：

. , # ? \* +

如果您未加上反斜線，Websense 軟體將會忽略該特殊字元。

- ◆ 如果您使用 Websense Web Security，請避免讓關鍵字與任何「延伸的防護」下層類別產生關聯。這些類別未強制執行關鍵字封鎖。

完成新增或編輯關鍵字之後，按一下 **確定** 來快取變更並返回「[編輯類別](#)」頁面。按一下 **全部儲存** 才能使變更生效。

爲了強制執行關鍵字封鎖功能，您還必須：

1. 透過 [設定](#) > [篩選器](#) 頁面啓用關鍵字封鎖功能 (請參閱 [設定 Websense 篩選設定](#)，第 49 頁)。
2. 在一或多個作用中類別篩選器啓用關鍵字封鎖功能 (請參閱 [編輯類別篩選器](#)，第 44 頁)。

## 重新定義特定網站的篩選

相關主題：

- ◆ [建立自訂類別](#)，第 154 頁
- ◆ [根據關鍵字篩選](#)，第 156 頁
- ◆ [定義未篩選的 URL](#)，第 159 頁
- ◆ [重新分類 URL](#)，第 160 頁

您可以利用自訂 URL 達成下列目的：

- ◆ 套用更精確的篩選到 Websense Master Database 中所沒有的網站。根據預設，會使用套用至其他尚未歸類類別的動作來篩選這些網站。
- ◆ 以不同於 Master Database 類別的方式篩選網站。

Websense 軟體會先尋找網站的自訂 URL 定義，再查詢 Master Database，因此是根據指派給自訂 URL 的類別篩選網站。

自訂 URL 有 2 種類型：未篩選與已重新分類。

- ◆ 未篩選的 URL 指的是允許不是由「全部封鎖」類別或限制存取篩選器管理之全部使用者存取的 URL (請參閱[定義未篩選的 URL](#)，第 159 頁)。
- ◆ 已重新分類的 URL 指的是從 Master Database 類別移到另一個 Websense 定義或自訂類別的 URL (請參閱[重新分類 URL](#)，第 160 頁)。

根據預設，系統不會封鎖對已重新分類 URL 的存取。此類 URL 會根據套用至其在每個作用中類別篩選器之新類別的動作篩選。

若根據網站的 Master Database 類別篩選網站，Websense 軟體會比對 URL 與其對等的 IP 位址。但對於自訂 URL 情況就不是這樣。若要變更篩選網站的方式，請同時將它的 URL 和它的 IP 位址定義為自訂 URL。

如果某個網站可以透過多個 URL 存取，將每個可用來存取網站的 URL 定義為自訂 URL，以確保按預期允許或封鎖存取網站。

如果將網站移至新的網域，並且使用 HTTP 重新導向將使用者重導至新的 URL，並不會自動使用與重新導向網站相同的方法篩選新的 URL。為了確保可正確篩位於選新位址的網站，請建立新的自訂 URL。

## 定義未篩選的 URL

相關主題：

- ◆ [使用類別](#)，第 152 頁
- ◆ [重新定義特定網站的篩選](#)，第 158 頁
- ◆ [重新分類 URL](#)，第 160 頁

使用 [政策管理](#) > [篩選器元件](#) > [未篩選的 URL](#) 頁面定義可由「全部封鎖」類別或限制存取篩選器管理之外的所有使用者存取的網站。

內容窗格右邊的 [允許的網站](#) 清單中所列的是您所定義的未篩選的網站 (URL 和 IP 位址) 和正規表示式 (請參閱 [使用正規表示式](#)，第 170 頁)。每個網站均有一個相關的類別。

- ◆ URL 可與其 Master Database 類別關聯或重新分類。
- ◆ 當使用者要求存取未篩選的 URL 時，系統會在它所屬的類別中將要求記錄為允許的自訂 URL。

新增未篩選的 URL：

1. 在 [定義未篩選的 URL](#) 底下，一行輸入一個 URL 或 IP 位址，然後按一下向右箭頭 (>)。

Websense 軟體不會比對自訂 URL 與其相等的 IP 位址。若要允許存取某個網站的 URL 和 IP 位址，將這兩者都加到「未篩選的 URL」清單中。

2. 若要新增比對多個網站的正規表示式，按一下 [進階](#)。一行輸入一個正規表示式，然後按向右箭頭，將表示式移到「未篩選的 URL」清單中。若要驗證樣式是否能夠比對想要的網站，按一下 [測試](#)。

如需詳細資訊，請參閱 [使用正規表示式](#)，第 170 頁。

3. 完成之後，按一下 [確定](#) 來快取變更並返回「編輯類別」頁面。按一下 [全部儲存](#) 才能使變更生效。

若要移除「未篩選的 URL」清單中的網站，選取 URL、IP 位址或正規表示式，然後按一下 [刪除](#)。

## 重新分類 URL

相關主題：

- ◆ [使用類別](#)，第 152 頁
- ◆ [重新定義特定網站的篩選](#)，第 158 頁
- ◆ [定義未篩選的 URL](#)，第 159 頁

使用 [政策管理](#) > [篩選器元件](#) > [編輯類別](#) > [重新分類 URL](#) 頁面新增個別網站到任一類別。若要變更現有的已重新分類網站，使用 [編輯 URL](#) 頁面。

重新分類 URL 以變更篩選及記錄個別網站的方式。新增已重新分類的網站時：

- ◆ 在單獨的行中輸入每個 URL 或 IP 位址。
- ◆ 為非 HTTP 網站，加上通訊協定。如果省略通訊協定，Websense 軟體會將網站當作 HTTP 網站篩選。

若為 HTTPS 網站，同時包括連接埠號碼 (<https://63.212.171.196:443/> 或 <https://www.onlinebanking.com:443/>)。

- ◆ Websense 軟體會完全根據輸入的 URL 樣式辨識自訂 URL。如果「搜尋引擎與入口網站」類別被封鎖，而您重新將 **www.yahoo.com** 分類到允許的類別，則只有當使用者鍵入完整位址時，才允許存取該網站。如果使用者鍵入 [images.search.yahoo.com](https://images.search.yahoo.com) 或 [yahoo.com](https://yahoo.com)，將仍然無法存取該網站。但是，如果您重新分類 **yahoo.com**，那麼將可存取位址中含有 **yahoo.com** 的全部網站。

完成新增或編輯已重新分類的網站之後，按一下 **確定** 來快取變更並返回「編輯類別」頁面。按一下 **全部儲存** 才能使變更生效。

儲存已重新分類的 URL 之後，請使用右方之捷徑窗格中的 **URL 類別** 工具來驗證是否將網站指派給正確的類別。請參閱 [使用「工具箱」來驗證篩選行為](#)，第 171 頁。

## 使用通訊協定

Websense Master 資料庫包括可用來篩選 HTTP、HTTPS 和 FTP 以外之網際網路通訊協定的通訊協定定義。這些定義包括網際網路應用程式和資料傳輸方法，例如像用於即時訊息傳送、串流媒體、檔案共享、檔案傳輸、網際網路郵件，以及其他網路和資料庫作業的方法。

您甚至可以使用這些通訊協定定義來篩選經過一般由 HTTP 流量使用之連接埠而越過防火牆的通訊協定或應用程式。例如，即時訊息傳送資料即可透過 HTTP 連接埠進入使用防火牆封鎖即時訊息傳送通訊協定的網路。Websense 軟體可準確地識別這些通訊協定，並且根據您設定的政策篩選它們。



### 注意

若要啓用以通訊協定為基礎的篩選，必須要安裝 Network Agent。



除了使用 Websense 定義的通訊協定定義之外，您也可以定義用於篩選的自訂通訊協定。自訂的通訊協定定義可以根據 IP 位址或連接埠號碼，而且可以編輯。

若要封鎖特定連接埠的流量，設定讓該連接埠號碼與某個自訂通訊協定關聯，然後為該通訊協定指派一個預設的封鎖動作。

若要使用自訂通訊協定定義，請前往**政策管理 > 篩選器元件**，然後按一下**通訊協定**。如需詳細資訊，請參閱[編輯自訂通訊協定](#)，第 162 頁和[建立自訂通訊協定](#)，第 164 頁。

## 篩選通訊協定

相關主題：

- ◆ [使用通訊協定](#)，第 160 頁
- ◆ [編輯自訂通訊協定](#)，第 162 頁
- ◆ [建立自訂通訊協定](#)，第 164 頁
- ◆ [新增或編輯通訊協定識別碼](#)，第 162 頁
- ◆ [新增到 Websense 定義的通訊協定](#)，第 166 頁

安裝 Network Agent 之後，Websense 軟體即可封鎖使用特定連接埠、使用特定 IP 位址傳輸或標記特定簽章的網際網路內容 (不論資料的本質是什麼)。根據預設，封鎖連接埠會攔截透過該連接埠進入您網路的所有網際網路內容 (不論來源為何)。



### 注意

有時候，使用特定連接埠傳送的內部網路流量可能不會被封鎖，即使使用該連接埠的通訊協定被封鎖也是如此。通訊協定透過內部伺服器傳送資料的速度可能會比 Network Agent 能夠擷取並處理資料的速度還要快。但是，這不會發生在從網路外部傳送進來的資料。

提出通訊協定要求時，Websense 軟體會使用下列步驟來決定是應該封鎖還是允許要求：

1. 判斷通訊協定 (或網際網路應用程式) 名稱。
2. 根據要求目的地位址識別通訊協定。
3. 搜尋自訂通訊協定定義中的相關連接埠號碼或 IP 位址。
4. 搜尋 Websense 定義之通訊協定定義中的相關連接埠號碼、IP 位址或簽章。

若 Websense 軟體無法決定此資訊的任一項，則允許存取與此通訊協定有關的所有內容。

## 編輯自訂通訊協定

相關主題：

- ◆ [使用通訊協定，第 160 頁](#)
- ◆ [建立自訂通訊協定，第 164 頁](#)
- ◆ [建立通訊協定篩選器](#)
- ◆ [編輯通訊協定篩選器](#)
- ◆ [使用類別](#)

使用 [政策管理](#) > [篩選器元件](#) > [編輯通訊協定](#) 頁面建立及編輯自訂通訊協定定義，以及檢閱 Websense 定義的通訊協定定義。無法編輯 Websense 定義的通訊協定。

「通訊協定」清單中包含所有自訂以及 Websense 定義的通訊協定。按一下通訊協定或通訊協定群組，內容窗格的右邊即會顯示與所選項目有關的資訊。

若要新增自訂通訊協定，按一下 [新增通訊協定](#)，然後繼續 [建立自訂通訊協定，第 164 頁](#)。

編輯通訊協定定義：

1. 從「通訊協定」清單中選取通訊協定。清單右邊就會顯示通訊協定定義。
2. 按一下 [覆寫動作](#) 即可變更套用至所有通訊協定篩選器中此通訊協定的篩選動作 (請參閱 [進行全域通訊協定篩選變更，第 163 頁](#))。
3. 按一下 [新增識別碼](#) 即可為此通訊協定定義其他通訊協定識別碼 (請參閱 [新增或編輯通訊協定識別碼，第 162 頁](#))。
4. 從清單中選取一個識別碼，然後按一下 [編輯](#)，變更該識別碼所定義的 [連接埠](#)、[IP 位址範圍](#) 或 [傳輸方法](#)。
5. 完成之後，按一下 [確定](#) 來快取您的變更。按一下 [全部儲存](#) 才能使變更生效。

若要刪除通訊協定定義，由「通訊協定」清單中選取一個項目，然後按一下 [刪除](#)。

### 新增或編輯通訊協定識別碼

使用 [篩選器元件](#) > [編輯通訊協定](#) > [新增通訊協定識別碼](#) 頁面為現有的自訂通訊協定定義其他通訊協定識別碼。使用 [編輯通訊協定識別碼](#) 頁面變更先前定義的識別碼。

建立或變更識別碼之前，檢查 [選擇的通訊協定](#) 旁邊顯示的通訊協定名稱是否正確。

使用通訊協定識別碼時，請記住每個通訊協定至少要有一個唯一的條件 (連接埠、IP 位址或傳輸類型)。

1. 指定此識別碼中包含哪些 [連接埠](#)。
  - 如果您選取 [所有連接埠](#)，該條件將會與其他通訊協定定義中輸入的其他連接埠或 IP 位址重疊。

- 如果連接埠範圍重疊，就不會視為是唯一的。例如，80-6000 的連接埠範圍與 4000-9000 範圍重疊。
  - 定義連接埠 80 或 8080 的通訊協定時請務必特別小心。因為 Network Agent 使用這兩個連接埠監聽網際網路要求。  
由於自訂通訊協定的優先權高於 Websense 通訊協定，若您自訂了使用連接埠 80 的通訊協定，所有其他使用連接埠 80 的通訊協定都會被當作自訂通訊協定而篩選並記錄。
2. 指定此識別碼中包含哪些 IP 位址。
    - 如果您選取**所有的外部 IP 位址**，該條件會與其他通訊協定定義中輸入的其他 IP 位址重疊。
    - 如果 IP 位址範圍重疊，就不會視為是唯一的。
  3. 指定此識別碼中包含哪一個**通訊協定傳輸**方法。
  4. 按一下**確定**來快取變更並返回「編輯通訊協定」頁面。按一下**全部儲存**才能使變更生效。

## 重新命名自訂通訊協定

使用**篩選器元件 > 編輯通訊協定 > 重新命名通訊協定**頁面變更自訂通訊協定的名稱，或者將它移到其他通訊協定群組。

- ◆ 使用**名稱**欄位編輯通訊協定名稱。新的名稱不可超過 50 個字元。  
名稱不可包含下列任一字元：  
\* < > { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,
- ◆ 若要將通訊協定移到其他通訊協定群組，由**屬於群組**欄位中選取新群組。

完成變更之後，按一下**確定**以返回「編輯通訊協定」頁面。還必須按一下「編輯通訊協定」中的**確定**來快取變更。

## 進行全域通訊協定篩選變更

使用**篩選器元件 > 編輯通訊協定 > 覆寫動作**頁面變更所有現有通訊協定篩選器中篩選通訊協定的方式。這同時決定了套用至新篩選器中通訊協定的預設動作。

雖然此變更會覆寫套用至所有現有通訊協定篩選器中的篩選動作，管理員稍後還是可以編輯這些篩選器，以套用不同的動作。

1. 檢查**選擇的通訊協定**旁邊顯示的通訊協定名稱是否正確。
2. 選取要套用至此通訊協定的**新動作**（「允許」或「封鎖」）。根據預設，會選取**不變更**。如需詳細資訊，請參閱**篩選動作**，第 39 頁。
3. 指定新的**記錄**選項。通訊協定流量必須要記錄，才會顯示在報告中並且啟用通訊協定使用警示。

- 指定是否使用 **Bandwidth Optimizer** 來管理對此通訊協定的存取。如需詳細資訊，請參閱 [使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁。



#### 重要

在此處所做的變更會影響**全部封鎖**和**全部允許**以外的每個現有通訊協定篩選器。

- 完成之後，按一下**確定**以返回「編輯通訊協定」頁面 (請參閱 [編輯自訂通訊協定](#)，第 162 頁)。還必須按一下「編輯通訊協定」頁面中的**確定**來快取變更。

## 建立自訂通訊協定

相關主題：

- ◆ [使用通訊協定](#)，第 160 頁
- ◆ [篩選通訊協定](#)，第 161 頁
- ◆ [編輯自訂通訊協定](#)，第 162 頁
- ◆ [新增到 Websense 定義的通訊協定](#)，第 166 頁

使用 [篩選器元件](#) > [通訊協定](#) > [新增通訊協定](#) 頁面定義新的自訂通訊協定。

- 輸入通訊協定的名稱。

名稱不可包含下列任一字元：

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

為自訂通訊協定指派的名稱可以與 Websense 定義的通訊協定名稱相同，以擴充與原始通訊協定相關的 IP 位址或連接埠數目。如需詳細資訊，請參閱 [新增到 Websense 定義的通訊協定](#)，第 166 頁。

- 展開 [新增通訊協定到此群組](#) 下拉式清單，然後選取一個通訊協定群組。新的通訊協定將顯示在所有通訊協定清單和篩選器的這個群組中。
- 為此群組定義一個唯一的 [通訊協定識別碼](#) (一組 [連接埠](#)、[IP 位址](#) 和 [傳輸方法](#))。您稍後可以從「編輯通訊協定」頁面新增其他識別碼。

遵照下列準則建立通訊協定識別碼：

- 每個通訊協定定義至少要有一個唯一的條件 (連接埠、IP 位址或傳輸類型)。
- 如果您選取 [所有連接埠](#) 或 [所有的外部 IP 位址](#)，該條件將會與其他通訊協定定義中輸入的其他連接埠或 IP 位址重疊。

- 如果連接埠範圍或 IP 位址範圍重疊，就不會視為是唯一的。例如，80-6000 的連接埠範圍與 4000-9000 範圍重疊。



### 注意

定義連接埠 80 或 8080 的通訊協定時請務必特別小心。因為 Network Agent 使用這兩個連接埠監聽網際網路要求。

由於自訂通訊協定的優先權高於 Websense 通訊協定，若您自訂了使用連接埠 80 的通訊協定，所有其他使用連接埠 80 的通訊協定都會被當作自訂通訊協定而篩選並記錄。

下表提供有效與無效通訊協定定義的範例：

連接埠	IP 位址	傳輸方法	是不是接受的組合？
70	ANY	TCP	是 – 連接埠號碼讓每個通訊協定識別碼成為唯一的。
90	ANY	TCP	

連接埠	IP 位址	傳輸方法	是不是接受的組合？
70	ANY	TCP	否 – IP 位址不是唯一的。10.2.1.201 含括在“ANY”設定中。
70	10.2.1.201	TCP	

連接埠	IP 位址	傳輸方法	是不是接受的組合？
70	10.2.3.212	TCP	是 – IP 位址是唯一的。
70	10.2.1.201	TCP	

4. 在「預設篩選動作」底下，指定應該要套用到所有作用中通訊協定篩選器中此通訊協定的預設動作（允許或封鎖）：
  - 指定是否應該要記錄使用此通訊協定的流量。通訊協定流量必須要記錄，才會顯示在報告中並且啓用通訊協定使用警示。
  - 指定是否應該要由 **Bandwidth Optimizer** 管理此通訊協定的存取（請參閱 [使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁）。
5. 完成之後，按一下**確定**以返回「編輯通訊協定」頁面。新的通訊協定定義就會顯示在「通訊協定」清單中。
6. 再按一次**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## 新增到 Websense 定義的通訊協定

您無法直接新增連接埠號碼或 IP 位址到 Websense 定義的通訊協定。不過，您可以使用與 Websense 定義的通訊協定相同的名稱建立自訂通訊協定，然後將連接埠或 IP 位址新增到其定義。

當自訂通訊協定名稱與 Websense 定義的通訊協定名稱相同時，Websense 軟體會查詢這兩個定義中指定之連接埠和 IP 位址的通訊協定流量。

在報告中，自訂通訊協定名稱會有一個“C\_”前置碼。例如，如果您為 SQL\_NET 建立自訂通訊協定並且指定其他的連接埠號碼，當通訊協定使用自訂通訊協定中的連接埠號碼時，報告會顯示 C\_SQL\_NET。

## 使用 Bandwidth Optimizer 管理頻寬

相關主題：

- ◆ [使用類別](#)，第 152 頁
- ◆ [使用通訊協定](#)，第 160 頁
- ◆ [設定預設的 Bandwidth Optimizer 限制](#)，第 167 頁

當您建立類別或通訊協定篩選器時，您可以根據頻寬使用量，選擇將限制對某個類別或通訊協定的存取。

- ◆ 根據網路頻寬使用量總計封鎖類別或通訊協定存取。
- ◆ 根據 HTTP 流量的頻寬使用量總計封鎖類別存取。
- ◆ 根據特定通訊協定的頻寬使用量封鎖該通訊協定存取。

例如：

- ◆ 如果網路頻寬使用量總計超過可用頻寬的 50%，或者 AIM 目前的頻寬使用量超過網路頻寬總計的 10%，即封鎖 AOL Instant Messaging 通訊協定。
- ◆ 如果網路頻寬使用量總計達到 75%，或者所有 HTTP 流量的頻寬使用量達到可用網路頻寬的 60%，即封鎖「體育運動」類別。

通訊協定頻寬使用量包括為通訊協定定義之所有連接埠、IP 位址或簽章的流量。這表示若某個通訊協定或網際網路應用程式使用多個連接埠傳輸資料，則會將通訊協定定義中含括之所有連接埠的流量計入該通訊協定的頻寬使用量總計。但是，如果某個網際網路應用程式使用通訊協定定義中未包括的連接埠，該連接埠的流量將不會計入使用的頻寬。

Websense 軟體會記錄已篩選的以 TCP 和 UDP 為根據之通訊協定所使用的頻寬。

Websense, Inc. 會定期更新 Websense 通訊協定定義，確保量測之頻寬的正確性。

Network Agent 會按照預先定義的時間間隔，將網路頻寬資料傳送給 Filtering Service。這可確保 Websense 軟體能夠正確監控頻寬使用，並且收到最接近平均值的量測值。

啓用以頻寬為基礎的篩選選項時，Websense 軟體會在初始設定 10 分鐘之後，以及每次 Websense Policy Server 重新啓動後 10 分鐘，開始以頻寬為基礎的篩選。這段延遲時間主要在確保量測之頻寬資料的正確性，以及正確將這項資料用於篩選。

根據頻寬限制而將某個要求封鎖時，會在 Websense 封鎖頁面的原因欄位中顯示這項資訊。如需詳細資訊，請參閱[封鎖頁面](#)，第 75 頁。

## 設定預設的 Bandwidth Optimizer 限制

相關主題：

- ◆ [編輯類別篩選器](#)，第 44 頁
- ◆ [編輯通訊協定篩選器](#)，第 46 頁
- ◆ [使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁

在政策中指定頻寬設定之前，請先驗證觸發以頻寬為基礎之篩選設定的預設頻寬臨界值。Websense 定義的值包括：

- ◆ 網路的預設頻寬：**50%**
- ◆ 每一通訊協定的預設頻寬：**20%**

預設的頻寬值儲存在 Policy Server，並由 Network Agent 的所有相關實例強制執行。如果您有多個 Policy Server，變更其中一個 Policy Server 的預設頻寬值並不會影響其他 Policy Server。

變更預設頻寬值：

1. 在 Websense Manager 中，前往**設定值>篩選**。
2. 輸入啓用頻寬篩選功能時，觸發以頻寬為基礎之篩選的頻寬使用量臨界值。
  - 根據整個網路的流量而將類別或通訊協定封鎖時，由**網路的預設頻寬**定義預設篩選臨界值。
  - 根據通訊協定的流量而將某個類別或通訊協定封鎖時，由**每一通訊協定的預設頻寬**定義預設篩選臨界值。

您可以覆寫任何類別或通訊協定篩選器中之每個類別或通訊協定的預設臨界值。

3. 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

若您變更預設值，有可能會影響強制執行 Bandwidth Optimizer 限制的任何類別和通訊協定篩選器。

- ◆ 若要管理與特定通訊協定相關的頻寬使用量，編輯作用中通訊協定篩選器。

- ◆ 若要管理與特定 URL 類別相關的頻寬使用量，編輯適當的類別篩選器。  
當您根據 HTTP 頻寬使用量篩選類別時，Websense 軟體會量測針對 Websense 軟體指定為 HTTP 連接埠之所有連接埠上的 HTTP 頻寬使用量總計。

## 根據檔案類型管理流量

在建立類別篩選器時，可以根據副檔名定義篩選，將存取限制在某些類別之網站中的特定檔案類型。例如，允許存取「體育運動」類別，但是封鎖「體育運動」類別之網站的視訊檔案。

Websense 軟體提供許多預先定義的檔案類型，或用於類似用途的副檔名群組。這些檔案類型定義均儲存在 Master Database 中，而且可以在更新 Master Database 時變更。

您可以使用預先定義的檔案類型執行篩選、修改現有的檔案類型定義，或者建立新的檔案類型。不過請注意，您無法刪除 Websense 定義的檔案類型，或者刪除與其相關聯的副檔名。

當使用者要求某個網站時，Websense 軟體會先判斷網站類別，然後檢查已篩選的副檔名。



### 注意

若要執行完全篩選視訊和音訊網際網路媒體，請結合以通訊協定為基礎的篩選功能和檔案類型篩選功能。在此情況下，由通訊協定篩選功能負責處理串流媒體，由檔案類型篩選功能負責處理可以下載並播放的檔案。

當使用者嘗試存取副檔名被封鎖的檔案時，會在 Websense 封鎖頁面的原因欄位中指示檔案類型被封鎖。如需詳細資訊，請參閱[封鎖頁面](#)，第 75 頁。



### 注意

若封鎖的 GIF 或 JPEG 影像只包含允許之頁面的一部份，就不會顯示標準的封鎖頁面。而是在影像區域顯示空白。這樣可以避免可能在允許之頁面的多個位置顯示封鎖頁面的一小部份。

檔案類型定義可根據篩選用途，包含不限數目的副檔名。例如，Websense 定義的檔案類型包括下列副檔名：

音訊	壓縮檔		可執行檔	視訊	
.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		.mlv	.ram



音訊	壓縮檔		可執行檔	視訊	
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp
.ogg	.gzip	.uue		.mp2v	.wmv
.rmi	.hqx	.xxe		.mpa	.wmx
.snd	.iso	.z		.mpe	.wxv
.wav	.jar	.zip			
.wax	.lzh				
.wma					

可以將與 Websense 定義之檔案類型相關的副檔名新增到自訂檔案類型。之後，即可根據與自訂檔案類型相關的設定篩選並記錄副檔名。

若要檢視現有的檔案類型定義、編輯檔案類型或者建立自訂檔案類型，請前往 **政策管理 > 篩選器元件**，然後按一下 **檔案類型**。如需詳細資訊，請參閱 [使用檔案類型](#)，第 169 頁。

## 使用檔案類型

相關主題：

- ◆ [根據檔案類型管理流量](#)，第 168 頁
- ◆ [編輯類別篩選器](#)，第 44 頁
- ◆ [篩選網站](#)，第 72 頁

可使用 **政策管理 > 篩選器元件 > 編輯檔案類型** 頁面建立並管理最多達 32 個的 **檔案類型**。檔案類型指的是可明確在類別篩選器中封鎖的副檔名群組（請參閱 [根據檔案類型管理流量](#)，第 168 頁）。

- ◆ 按一下某個檔案類型以查看與該類型相關的副檔名。
- ◆ 若要新增副檔名至所選取的檔案類型，按一下 **新增副檔名**，然後參閱 [新增副檔名到檔案類型](#)，第 170 頁，瞭解進一步的指示。
- ◆ 若要建立新的檔案類型，按一下 **新增檔案類型**，然後參閱 [新增自訂檔案類型](#)，第 170 頁，瞭解進一步的指示。
- ◆ 若要刪除自訂檔案類型或副檔名，選取項目，然後按一下 **刪除**。

您無法刪除 Websense 定義的檔案類型，或刪除與其相關聯的副檔名。

但是，您可以將與 Websense 定義之檔案類型相關的副檔名新增到自訂檔案類型。之後，即可根據與自訂檔案類型相關的設定篩選並記錄副檔名。無法將相同的副檔名新增到多個自訂檔案類型。

完成變更檔案類型定義之後，按一下 **確定**。按一下 **全部儲存** 才能使變更生效。

## 新增自訂檔案類型

使用**篩選器元件** > **編輯檔案類型** > **新增檔案類型**頁面定義自訂檔案類型。

1. 輸入唯一的**檔案類型名稱**。  
您可以使用與 Websense 定義的檔案類型相同的名稱建立自訂檔案類型，以將其他副檔名新增到現有的檔案類型。
2. 在**檔案副檔名**清單中，以一行一個的方式輸入副檔名。您不需要在每個副檔名之前加上點 (“.”)。
3. 按一下**確定**，返回「編輯檔案類型」畫面。新的檔案類型就會顯示在「檔案類型」清單中。
4. 完成檔案類型定義後，按一下「編輯檔案類型」頁面中的**確定**。按一下**全部儲存**才能使變更生效。

## 新增副檔名到檔案類型

使用**篩選器元件** > **編輯檔案類型** > **新增副檔名**頁面新增副檔名到選取的檔案類型。

1. 確認預期的檔案類型名稱出現在**已選擇檔案類型**旁邊。
2. 在**副檔名**清單中，以一行一個的方式輸入副檔名。您不需要在每個副檔名之前加上點 (“.”)。
3. 按一下**確定**，返回「編輯檔案類型」畫面。新的副檔名就會顯示在「自訂副檔名」清單中。
4. 完成檔案類型定義後，按一下「編輯檔案類型」頁面中的**確定**。按一下**全部儲存**才能使變更生效。

## 使用正規表示式

---

**正規表示式**指的是用以比對多個字串或一組字元的範本或樣式。您可以在限制存取篩選器中使用正規表示式，或者使用正規表示式定義自訂 URL 或關鍵字。然後 Websense 篩選會嘗試比對一般樣式，而非特定的單一 URL 或關鍵字。

以下為簡單的正規表示式範例：

```
domain.(com|org|net)
```

此表示式樣式比對 URL：

- ◆ domain.com
- ◆ domain.org
- ◆ domain.net

請小心使用正規表示式。雖然表示式是一種強大的篩選工具，但是也很容易導致封鎖或允許存取非預期的網站。此外，不良的正規表示式可造成額外的篩選負荷。



### 重要

使用正規表示式做為篩選條件可能會增加 CPU 使用量。測試顯示使用 100 個正規表示式時，Filtering Service 電腦的平均 CPU 使用量會增加 20%。

Websense 軟體支援大部份的 Perl 正規表示式語法，但有一些例外。部份不支援的語法對於比對可能在 URL 中找到的字串沒有用處。

不支援的正規表示式語法包括：

(?<=pattern) string	(?!pattern) string
\N{name}	(?imsx-imsx)
(?(condition)pat1)	\pP
(?(condition)pat1 pat2)	\PP
(?(code))	??{code}}

如需正規表示式的進一步說明，請參閱：

[en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression)

[www.regular-expressions.info/](http://www.regular-expressions.info/)

## 使用「工具箱」來驗證篩選行為

Websense Manager 右方的捷徑窗格中包含了**工具箱**，可讓您快速檢查篩選設定。

按一下工具名稱即可存取該工具。再按一次名稱即可檢視工具清單。如需有關使用工具的詳細資訊，請參閱：

- ◆ [URL 類別](#)，第 172 頁
- ◆ [檢查政策](#)，第 172 頁
- ◆ [測試篩選](#)，第 172 頁
- ◆ [URL 存取](#)，第 173 頁
- ◆ [調查使用者](#)，第 173 頁

您也可以按一下**支援入口網站**，在新的瀏覽器標籤或視窗中，存取 Websense 技術支援網站。在「支援入口網站」，您可以使用「知識庫」來存取教學課程、秘訣、文章和文件。

## URL 類別

查看網站目前的分類方式：

1. 按一下「工具箱」中的 **URL 類別**。
2. 輸入 URL 或 IP 位址。
3. 按一下**執行**。

網站目前的類別會顯示在快顯視窗中。如果您的組織已重新分類 URL，就會顯示新類別。

網站的分類會根據您所使用之 Master Database (包括即時更新) 版本的不同而有所不同。

## 檢查政策

您可以使用此工具來判斷套用至特定用戶端的政策。顯示的結果為當時的結果。

1. 按一下「工具箱」中的**檢查政策**。
2. 若要識別某個目錄或電腦用戶端，輸入下述其中一個項目：
  - 完整的使用者名稱  
若要瀏覽或搜尋目錄以識別使用者，按一下**尋找使用者** (請參閱[識別要檢查政策或測試篩選的使用者](#)，第 173 頁)。
  - IP 位址
3. 按一下**執行**。

一或多個政策的名稱會顯示在快顯視窗中。尚未指派政策給使用者，但是已指派政策給使用者所屬的多個群組、網域或組織單位時，才會顯示多個政策。

即使顯示多個政策，任何時候都只能為使用者強制執行一個政策 (請參閱[篩選順序](#)，第 71 頁)。

## 測試篩選

查看當特定用戶端要求特定網站時會產生的結果：

1. 按一下「工具箱」中的**測試篩選**。
2. 若要識別某個目錄或電腦用戶端，輸入下述其中一個項目：
  - 完整的使用者名稱  
若要瀏覽或搜尋目錄以識別使用者，按一下**尋找使用者** (請參閱[識別要檢查政策或測試篩選的使用者](#)，第 173 頁)。
  - IP 位址
3. 輸入您要檢查之網站的 URL 或 IP 位址。
4. 按一下**執行**。

網站類別、套用至類別的動作，以及動作的原因均會顯示在快顯視窗中。

## URL 存取

檢視使用者在過去 2 週內 (包括今天) 是否嘗試存取網站：

1. 按一下「工具箱」中的 **URL 存取**。
2. 輸入想要檢查之網站的全部或部份 URL 或 IP 位址。
3. 按一下**執行**。

系統就會顯示一份調查報告，指示網站是否被存取過以及存取的時間 (如果曾經存取)。

如果您收到安全警示，可以使用此工具來檢查您的組織是否暴露於網路釣魚或受病毒感染的網站。

## 調查使用者

檢閱用戶端過去 2 週 (不含今天) 的網際網路使用歷史：

1. 按一下「工具箱」中的**調查使用者**。
2. 輸入全部或部份的使用者名稱或電腦 IP 位址。
3. 按一下**執行**。

系統就會顯示一份有關用戶端之使用歷史的調查報告。

## 識別要檢查政策或測試篩選的使用者

使用**尋找使用者**頁面指定「檢查政策」或「測試篩選」工具的使用者 (目錄) 用戶端。

當此頁面開啓時，預設會選取**使用者**選項。展開**目錄項目**資料夾來瀏覽目錄，或者按一下**搜尋**。此搜尋功能只有在您使用以 LDAP 為基礎的目錄服務時才可使用。

搜尋目錄以尋找使用者：

1. 輸入全部或部份的使用者**名稱**。
2. 展開**目錄項目**樹狀結構並瀏覽以識別搜尋內容。  
您必須按一下樹狀結構中的一個資料夾 (DC、OU 或 CN) 來指定內容。此內容會填入樹狀結構下方的欄位中。
3. 按一下**搜尋**。符合您搜尋詞的項目會列在**搜尋結果**底下。
4. 按一下某個使用者名稱來選取使用者，或者按一下**再次搜尋**，輸入新的搜尋詞或內容。  
若返回瀏覽目錄，按一下**取消搜尋**。
5. 當**使用者**欄位中顯示正確的完整使用者名稱時，按一下**執行**。

如果您使用「測試篩選」工具，請確認等到 **URL** 欄位中顯示 URL 或 IP 位址之後，再按一下**執行**。

若要識別電腦用戶端而非使用者，按一下 **IP 位址**。



# 10

## 使用者識別

爲了將政策套用至使用者和群組，Websense 軟體必須能夠從來源 IP 位址識別提出要求的使用者。可用的識別方法如下：

- ◆ 由整合裝置或應用程式識別並驗證使用者，然後將使用者資訊傳送給 Websense 軟體。如需詳細資訊，請參閱 [安裝手冊](#)。
- ◆ 由在背景作業的 Websense 無障礙識別代理程式與目錄服務通訊並識別使用者 (請參閱 [無障礙識別](#))。
- ◆ 當使用者開啓網頁瀏覽器並登入時，由 Websense 軟體提示他們輸入自己的網路認證 (請參閱 [手動驗證](#)，第 177 頁)。

### 無障礙識別

---

相關主題：

- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定使用者識別方法](#)，第 177 頁

一般來說，**無障礙識別**是一種方法，Websense 軟體用它來識別目錄服務中的使用者，而且不需要提示使用者輸入登入資訊。這包括將 Websense 軟體與提供篩選所需之使用者資訊的裝置或應用程式整合，或使用選用的 Websense 無障礙識別代理程式。

- ◆ Websense [DC Agent](#)，第 185 頁會與以 Windows 爲基礎的目錄服務搭配使用。此代理程式會定期查詢網域控制站的使用者登入工作階段，並輪詢用戶端電腦來驗證登入狀態。它在 Windows 伺服器上執行，而且可安裝於網路中的任何網域。
- ◆ Websense [Logon Agent](#)，第 187 頁會在使用者登入 Windows 網域時識別使用者。此代理程式在 Linux 或 Windows 伺服器上執行，但是它的相關 Logon Application 只能在 Windows 電腦上執行。
- ◆ Websense [RADIUS Agent](#)，第 190 頁可與以 Windows 爲基礎或以 LDAP 爲基礎的目錄服務搭配使用。此代理程式還可搭配 RADIUS 伺服器和用戶端，以識別從遠端位置登入的使用者。

- ◆ Websense *eDirectory Agent*，第 194 頁會搭配 Novell eDirectory 使用。此代理程式使用 Novell eDirectory 驗證將使用者對應到 IP 位址。

如需安裝每個代理程式的指示，請參閱 *安裝手冊*。代理程式可單獨使用，也可組合在一起使用 (請參閱 *設定多個代理程式*，第 199 頁)。



#### 注意

如果使用整合的 NetCache 設備，NetCache 必須使用 WinNT、LDAP 或 RADIUS 格式將使用者名稱傳送給 Websense 軟體，然後才能進行無障礙識別。

如果擁有代理伺服器，且同時使用無障礙識別代理程式，那麼最好在代理伺服器使用匿名驗證。

Websense Manager 中同時設定有一般使用者識別設定和特定的無障礙識別代理程式。按一下左側瀏覽窗格中的 **設定** 標籤，然後按一下 **使用者識別**。

如需詳細配置指示，請參閱 *設定使用者識別方法*，第 177 頁。

在某些情況下，Websense 軟體可能無法從無障礙識別代理程式取得使用者資訊。如果將多個使用者指派給相同的電腦，或者如果使用者是匿名使用者或來賓，或有其他原因時，都可能發生此情況。若發生這些情況，可提示使用者透過瀏覽器登入 (請參閱 *手動驗證*，第 177 頁)。

## 遠端使用者的無障礙識別

在特定配置中，Websense 軟體可無障礙地識別從遠端位置登入您網路的使用者：

- ◆ 如果已部署 Websense Remote Filtering Server 和 Remote Filtering Client，Websense 軟體即可識別使用網域帳戶登入快取之網域的遠端使用者。如需詳細資訊，請參閱 *篩選遠端用戶端*，第 137 頁。
- ◆ 如果已部署 DC Agent，且遠端使用者直接登入您網路中的已命名 Windows 網域，DC Agent 即可識別這些使用者 (請參閱 *DC Agent*，第 185 頁)。
- ◆ 如果使用 RADIUS 伺服器驗證從遠端位置登入的使用者，RADIUS Agent 將可無障礙地識別這些使用者，而您可以根據使用者或群組套用篩選政策 (請參閱 *RADIUS Agent*，第 190 頁)。



## 手動驗證

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [設定特定電腦的驗證規則](#)，第 179 頁
- ◆ [安全手動驗證](#)，第 181 頁
- ◆ [設定使用者識別方法](#)，第 177 頁

無障礙識別不一定適用於所有環境。若組織未使用無障礙識別，或者由於某些原因無法使用無障礙識別，仍然可以使用**手動驗證**來根據以使用者和群組為基礎的政策進行篩選。

如果進行手動驗證，則系統會在使用者第一次透過瀏覽器存取網際網路時，提示使用者輸入使用者名稱和密碼。Websense 軟體會確認密碼與支援的目錄服務，然後擷取該使用者的政策資訊。

您可以設定 Websense 軟體，讓它在無法使用無障礙識別時啓用手動驗證 (請參閱[設定使用者識別方法](#)，第 177 頁)，或者建立一份自訂驗證設定的特定電腦的清單，以在使用者開啓瀏覽器時提示使用者登入 (請參閱[設定特定電腦的驗證規則](#)，第 179 頁)。

啓用手動驗證時，使用者會在發生下列情況時收到 HTTP 錯誤，而且無法存取網際網路：

- ◆ 3 次輸入密碼嘗試均失敗。使用者名稱或密碼無效時便會發生此情況。
- ◆ 按一下**取消**略過驗證提示。

啓用手動驗證時，無法識別的使用者不能瀏覽網際網路。

## 設定使用者識別方法

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [手動驗證](#)，第 177 頁
- ◆ [使用使用者與群組](#)，第 56 頁

使用**設定 > 使用者識別**頁面管理 Websense 軟體嘗試識別網路中的使用者，從而套用以使用者和群組為基礎的政策的時候和方式。

- ◆ 設定 Policy Server 與無障礙識別代理程式通訊。
- ◆ 檢閱及更新無障礙識別代理程式設定。
- ◆ 設定當無障礙識別代理程式或整合裝置無法識別使用者時，決定 Websense 軟體應該如何回應的全域規則。
- ◆ 識別您網路中未套用全域使用者識別規則的電腦，並且指定是否應該以及如何驗證這些電腦的使用者。

如果使用 Websense 無障礙識別代理程式，這些代理程式會列在**無障礙識別代理程式**下：

- ◆ **伺服器**顯示無障礙識別代理程式所在之電腦的 IP 位址或名稱。
- ◆ **連接埠**列示 Websense 軟體用來與代理程式通訊的連接埠。
- ◆ **類型**指示指定的實例是 DC Agent、Logon Agent、RADIUS Agent 還是 eDirectory Agent (如需每個代理程式類型的指示，請參閱**無障礙識別**，第 175 頁)。

若要將代理程式新增到此清單，可從**新增代理程式**下拉式清單中選擇代理程式類型。按下列某個連結以瞭解配置指示：

- ◆ [設定 DC Agent](#)，第 186 頁
- ◆ [設定 Logon Agent](#)，第 188 頁
- ◆ [設定 RADIUS Agent](#)，第 192 頁
- ◆ [設定 eDirectory Agent](#)，第 196 頁

若要移除清單中的代理程式實例，則標記清單中代理程式資訊旁邊的核取方塊，然後按一下**刪除**。

在**其他驗證選項**下指定無法由代理程式或整合裝置無障礙識別使用者時，Websense 軟體的預設回應：

- ◆ 按一下**套用電腦或網路政策**即可忽略以使用者和群組為基礎政策，並且套用以電腦和網路為基礎的政策或「預設」政策。
- ◆ 按一下**提示使用者輸入登入資訊**，即可要求使用者在開啓瀏覽器時提供登入認證。然後就可以套用以使用者和群組為基礎的政策 ( 請參閱**手動驗證**，第 177 頁)。
- ◆ 指定每次提示使用者輸入登入認證時，Websense 軟體應該使用的預設網域**內容**。此為使用者的認證有效的網域。  
如果使用「例外」清單指定提示使用者輸入登入資訊的電腦，那麼必須提供預設網域內容，即使全域規則指定套用以電腦或網路為基礎的政策也是如此。

建立決定 Websense 軟體識別使用者之時機與方式的一般規則之後，就可以建立規則的例外情況。

例如，如果使用無障礙識別代理程式或整合產品以識別使用者，並且啓用手動驗證以在無法進行無障礙識別時提示使用者輸入他們的認證，您就可以識別特定電腦，這些電腦具有以下特點：

- ◆ 從不提示無法識別的使用者輸入他們的認證。換句話說，若無障礙識別失敗，也不會嘗試手動驗證，但會套用電腦或網路政策，或者「預設」政策。

- ◆ 始終忽略使用者資訊 (即使這些資訊可用) , 且始終提示使用者輸入他們的認證。
- ◆ 始終忽略使用者資訊 (即使這些資訊可用) , 且從不提示使用者輸入他們的認證 (始終套用電腦或網路政策, 或者「預設」政策)。

若要建立例外, 按一下**例外**, 然後參閱[設定特定電腦的驗證規則](#), 第 179 頁。

在此頁面中完成變更之後, 按一下**確定**來儲存所做的變更。若要放棄變更, 按一下**取消**。

## 設定特定電腦的驗證規則

相關主題：

- ◆ [設定使用者識別方法](#), 第 177 頁
- ◆ [手動驗證](#), 第 177 頁
- ◆ [安全手動驗證](#), 第 181 頁

可利用選擇性驗證, 以決定是否提示從特定用戶端電腦 (由 IP 位址識別) 要求網際網路存取的使用者透過瀏覽器提供他們的登入認證。這可用於：

- ◆ 為公共 Kiosk 中的電腦建立與提供 Kiosk 的組織員工不同的驗證規則。
- ◆ 確保醫學辦公室中檢驗室電腦的使用者在存取網際網路之前一律要經過識別。

套用特別使用者識別設定的電腦會列在**設定 > 使用者識別**頁面中。按一下**例外**即可為您網路中的某些電腦建立特定的使用者識別設定, 或者查看是否已經為特定電腦定義特殊設定。

若要新增電腦到清單中, 按一下**新增**, 然後參閱[定義使用者識別設定的例外](#), 第 179 頁, 瞭解進一步的指示。

完成將電腦或網路範圍新增到清單之後, 按一下**確定**。按一下**全部儲存**才能使變更生效。

## 定義使用者識別設定的例外

相關主題：

- ◆ [無障礙識別](#), 第 175 頁
- ◆ [手動驗證](#), 第 177 頁
- ◆ [設定使用者識別方法](#), 第 177 頁

可在**設定 > 使用者識別 > 新增 IP 位址**頁面指定應該套用特定使用者識別規則的電腦。

1. 輸入 **IP 位址**或 **IP 位址範圍**來指定要套用特定驗證方法的電腦，然後按向右箭號按鈕將它們加入**已選擇**清單。  
若要將相同的規則套用到多台電腦，則將它們全部加入清單。
2. 從**使用者識別**下拉式清單中選取一個項目，指示 Websense 軟體是否應該嘗試無障礙地識別這些電腦的使用者。
  - 選擇**嘗試無障礙地識別使用者**，即可向無障礙識別代理程式或整合裝置要求使用者資訊。
  - 選擇**忽略使用者資訊**，即可避免使用任何無障礙的方法識別使用者。
3. 指示是否應該提示使用者透過瀏覽器提供登入認證。若因其他識別失敗或因使用者資訊被忽略而無法取得使用者資訊，就會套用這項設定。
  - 選擇**提示使用者輸入登入資訊**，即可要求使用者提供登入認證。  
若同時選擇**嘗試無障礙地識別使用者**，則使用者只有在不是無障礙識別時，才會看到瀏覽器提示。
  - 選擇**套用電腦或網路政策**，即可確保從不要求使用者提供登入認證。  
如果同時選擇**嘗試無障礙地識別使用者**，則會由適當的使用者政策來篩選其認證可被無障礙驗證的使用者。
4. 按一下**確定**返回「使用者識別」頁面。
5. 完成更新「例外」清單後，按一下**確定**來快取所做的變更。按一下**全部儲存**才能使變更生效。

## 修訂使用者識別設定的例外

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定使用者識別方法](#)，第 177 頁

可在**設定 > 使用者識別 > 編輯 IP 位址**頁面變更「例外」清單中的項目。在此頁面中所做的變更會影響「已選擇」清單中的所有電腦(由 IP 位址或範圍識別)。

1. 從**使用者識別**下拉式清單中選取一個項目，指示 Websense 軟體是否應該嘗試無障礙地識別這些電腦的使用者。
  - 選擇**嘗試無障礙地識別使用者**，即可向無障礙識別代理程式或整合裝置要求使用者資訊。
  - 選擇**忽略使用者資訊**，即可避免使用任何無障礙的方法識別使用者。
2. 指示是否應該提示使用者透過瀏覽器提供登入認證。若因無障礙識別失敗或因無障礙識別被忽略而無法取得使用者資訊，就會套用這項設定。
  - 選擇**提示使用者輸入登入資訊**，即可要求使用者提供登入認證。  
若同時選擇**嘗試識別使用者**，則使用者只有在不是無障礙識別時，才會看到瀏覽器提示。

- 選擇**套用電腦或網路政策**，即可確保從不提示使用者提供登入認證。  
若同時選擇**嘗試識別使用者**，則會由適當的使用者政策來篩選其認證可被無障礙驗證的使用者。
- 3. 按一下**確定**返回「使用者識別」頁面。
- 4. 完成更新「例外」清單後，按一下**確定**來快取所做的變更。按一下**全部儲存**才能使變更生效。

## 安全手動驗證

相關主題：

- ◆ [設定使用者識別方法](#)，第 177 頁
- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定特定電腦的驗證規則](#)，第 179 頁
- ◆ [啟動安全手動驗證](#)，第 183 頁

Websense 安全手動驗證使用 Secure Sockets Layer (SSL) 加密來保護在用戶端電腦與 Websense 軟體之間傳輸的驗證資料。內建於 Filtering Service 的 SSL 伺服器能夠加密在用戶端電腦與 Filtering Service 之間傳輸的使用者名稱和密碼。預設會停用安全手動驗證。



### 注意

安全手動驗證不能搭配 Remote Filtering 使用。如果 Remote Filtering Server 與啓用安全手動驗證的 Filtering Service 實例關聯，它就無法為用戶端提供封鎖頁面。

若要啓動這項功能，您必須執行下列步驟：

1. 產生 SSL 憑證和密碼，並將它們置於 Websense 軟體可以存取且 Filtering Service 可以讀取的位置 (請參閱[產生密碼和憑證](#)，第 182 頁)。
2. 啓用與目錄服務的安全手動驗證 (請參閱[啟動安全手動驗證](#)，第 183 頁) 和安全通訊。
3. 將憑證匯入瀏覽器 (請參閱[接受用戶端瀏覽器內的憑證](#)，第 184 頁)。

## 產生密碼和憑證

相關主題：

- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定特定電腦的驗證規則](#)，第 179 頁
- ◆ [安全手動驗證](#)，第 181 頁
- ◆ [啟動安全手動驗證](#)，第 183 頁
- ◆ [接受用戶端瀏覽器內的憑證](#)，第 184 頁

憑證包含用來加密資料的公鑰，以及用來解密資料的私鑰。憑證由「憑證授權單位 (CA)」核發。您可以從內部憑證伺服器產生憑證，或者從協力廠商 CA (例如 VeriSign) 取得用戶端憑證。

核發用戶端憑證的 CA 必須是受 Websense 軟體信任的。這通常由瀏覽器設定決定。

- ◆ 如需私鑰、CSR 和憑證等常見問題的解答，請參閱 [http://docs.apache.org/docs/2.2/ssl/ssl\\_faq.html#aboutcerts](http://docs.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts)。
- ◆ 如需自行產生私鑰、CSR 和憑證的詳細資訊，請參閱 [www.akadia.com/services/ssh\\_test\\_certificate.html](http://www.akadia.com/services/ssh_test_certificate.html)。

可使用很多工具來產生自行簽署的憑證，包括 OpenSSL 工具組 (可從 [www.openssl.org](http://www.openssl.org) 取得)。

不論選用哪種方法來產生憑證，請使用下列一般步驟。

1. 產生私鑰 (**server.key**)。
2. 使用私鑰產生「憑證簽署要求 (CSR)」。



### 重要

系統提示輸入 CommonName 時，輸入 Filtering Server 電腦的 IP 位址。如果略過此步驟，用戶端瀏覽器將會顯示安全性憑證錯誤。

3. 使用 CSR 來建立自行簽署的憑證 (**server.crt**)。
4. 將 **server.crt** 和 **server.key** 檔案儲存到 Websense 軟體可以存取且 Filtering Service 可以讀取的位置。

## 啓動安全手動驗證

相關主題：

- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定特定電腦的驗證規則](#)，第 179 頁
- ◆ [安全手動驗證](#)，第 181 頁
- ◆ [產生密碼和憑證](#)，第 182 頁
- ◆ [接受用戶端瀏覽器內的憑證](#)，第 184 頁

1. 停止 Websense Filtering Service (請參閱[停止和啓動 Websense 服務](#)，第 245 頁)。
2. 瀏覽至 Filtering Service 電腦上的 Websense 安裝目錄 (預設為 **C:\Program Files\Websense\bin** 或 **/opt/Websense/bin/**)。
3. 找到 **eimserver.ini**，然後在其他目錄中建立它的備份複本。
4. 在文字編輯器中開啓原始的 INI 檔案。
5. 找到 **[WebsenseServer]** 區段，然後加上下列命令行：

```
SSLManualAuth=on
```

6. 在前一行下方，加上下列命令行：

```
SSLCertFileLoc=[ 路徑 ]
```

將 **[路徑]** 換成 SSL 憑證的完整路徑，包括憑證檔案名稱 (例如 **C:\secmanauth\server.crt**)。

7. 同時加上：

```
SSLKeyFileLoc=[ 路徑 ]
```

將 **[路徑]** 換成 SSL 密碼的完整路徑，包括密碼檔案名稱 (例如 **C:\secmanauth\server.key**)。

8. 儲存並關閉 **eimserver.ini**。
9. 啓動 Websense Filtering Service。

啓動之後，Filtering Service 將在預設的安全 HTTP 連接埠 (**15872**) 監聽要求。

前面的步驟可保護用戶端電腦與 Websense 軟體之間的通訊。若要同時保護 Websense 軟體與目錄服務之間的通訊，確定在**設定 > 目錄服務**頁面中選擇**使用 SSL**。如需詳細資訊，請參閱[進階目錄設定](#)，第 59 頁。

## 接受用戶端瀏覽器內的憑證

相關主題：

- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定特定電腦的驗證規則](#)，第 179 頁
- ◆ [安全手動驗證](#)，第 181 頁
- ◆ [產生密碼和憑證](#)，第 182 頁
- ◆ [啟動安全手動驗證](#)，第 183 頁

第一次嘗試瀏覽網站時，瀏覽器會顯示安全性憑證警告。若不想再看到此訊息，請在憑證存放區中安裝憑證。

### Microsoft Internet Explorer (7.0 版)

1. 開啓瀏覽器並前往某個網站。  
此時會出現網站的安全性憑證有問題的警告。
2. 按一下[繼續瀏覽此網站 \(不建議\)](#)。  
如果看到驗證提示，則按一下[取消](#)。
3. 按一下位址列 (在瀏覽器視窗的最上方) 右側的[憑證錯誤](#)方塊，然後按一下[檢視憑證](#)。
4. 在「憑證」對話方塊的「一般」標籤中，按一下[安裝憑證](#)。
5. 選擇[自動根據憑證類型來選取憑證存放區](#)，然後按下一步。
6. 按一下[完成](#)。
7. 詢問是否要安裝憑證時，按一下[是](#)。

今後使用者就不會在此電腦上看到與 Filtering Service 相關的憑證安全警告。

### Mozilla Firefox (2.x 版)

1. 開啓瀏覽器並前往某個網站。  
您會看到一個警告訊息。
2. 按一下[永久接受該憑證](#)。
3. 如果出現提示，則輸入您的認證。
4. 移至工具 > [選項](#)，然後按一下[進階](#)。
5. 選擇[加密](#)標籤，然後按一下[檢視憑證](#)。
6. 選擇[網站](#)標籤，然後檢查憑證是否列示。

今後使用者就不會在此電腦上看到與 Filtering Service 相關的憑證安全警告。



## Mozilla Firefox (3.x 版)

1. 開啓瀏覽器並前往某個網站。  
您會看到一個警告訊息。
2. 按一下[或者可以新增例外](#)。
3. 按一下[新增例外](#)。
4. 確定已選擇永久儲存此例外，然後按一下[確認安全性例外](#)。

今後使用者就不會在此電腦上看到與 Filtering Service 相關的憑證安全警告。

## DC Agent

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [設定 DC Agent](#)，第 186 頁
- ◆ [為每個代理程式實例配置不同的設定](#)，第 201 頁

Websense DC Agent 會在 Windows 上執行，並且偵測執行 NetBIOS、WINS 或 DNS 網路服務的 Windows 網路中的使用者。

DC Agent 和 User Service 會收集網路使用者資料並將它傳送到 Websense Filtering Service。多個變數決定了資料傳輸的速度，包括網路大小以及現有網路流量。

若要使用 DC Agent 啓用無障礙識別：

1. 安裝 DC Agent。如需詳細資訊，請參閱[安裝手冊](#)中的[分別安裝 Websense 元件](#)。



### 注意

使用網域管理員權限執行 DC Agent。此網域管理員帳戶必須也是 DC Agent 電腦上之「管理員」群組的成員。

只有這樣，DC Agent 才可從網域控制站擷取使用者登入資訊。如果無法使用此類權限安裝 DC Agent，請在安裝後為這些服務設定管理員權限。如需詳細資訊，請參閱[Websense 軟體未套用使用者或群組政策](#)，第 313 頁。

2. 設定 DC Agent 與其他 Websense 元件以及您網路中的網域控制站通訊 (請參閱[設定 DC Agent](#))。
3. 使用 Websense Manager 將使用者和群組新增到篩選器 (請參閱[新增用戶端](#)，第 61 頁)。

若 DC Agent 無法無障礙地識別使用者，Websense 軟體會提示使用者輸入識別。如需詳細資訊，請參閱[手動驗證](#)，第 177 頁。

## 設定 DC Agent

相關主題：

- ◆ [無障礙識別](#)
- ◆ [手動驗證](#)
- ◆ [設定使用者識別方法](#)
- ◆ [DC Agent](#)
- ◆ [設定多個代理程式](#)

可使用**設定 > 使用者識別 > DC Agent** 頁面設定新的 DC Agent 實例，以及設定套用至所有 DC Agent 實例的全域設定。

若要新增 DC Agent 實例，請先提供安裝代理程式的位置的基本資訊，以及與 Filtering Service 通訊的方式。每個代理程式實例的這些設定可以是唯一的。

1. 在「基本代理程式配置」下輸入安裝代理程式之**伺服器**的 IP 位址或名稱。



### 注意

電腦名稱必須以字母字元 (a-z) 開頭，而不能以數字或特殊字元開頭。

系統可能無法正確解析包含特定的延伸 ASCII 字元的電腦名稱。如果使用非英文版的 Websense 軟體，請輸入 IP 位址而非電腦名稱。

2. 輸入 DC Agent 用來與其他 Websense 元件通訊的**連接埠**。預設值是 30600。
3. 若要在 Filtering Service 與 DC Agent 之間建立已驗證連線，核取**啓動驗證**，然後輸入連線的**密碼**。

接下來自訂全域 DC Agent 通訊和疑難排解、網域控制站輪詢以及電腦輪詢設定。依照預設，您在此處所做變更會影響所有 DC Agent 實例。不過可以覆寫代理程式配置檔案中標記星號 (\*) 的設定，以自訂該代理程式實例的行為 (請參閱 [為每個代理程式實例配置不同的設定](#)，第 201 頁)。

1. 在「DC Agent 通訊」下輸入 DC Agent 與其他 Websense 元件通訊時所用的**通訊連接埠**。預設值是 30600。

除非「Websense 技術支援部」指示這麼做，否則請勿變更**診斷連接埠**設定。預設值是 30601。

2. 在「網域控制站輪詢」下核取**啓動網域控制站輪詢**，讓 DC Agent 查詢網域控制站的使用者登入工作階段。

您可以在代理程式的配置檔案中指定每個 DC Agent 實例輪詢的網域控制站。如需詳細資訊，請參閱 [設定多個代理程式](#)，第 199 頁。

3. 在**查詢時間間隔**欄位中指定 DC Agent 查詢網域控制站的頻率 (秒)。
 

降低查詢時間間隔可提升擷取登入工作階段的準確性，但是會增加整體網路流量。增加查詢時間間隔可減少網路流量，但是可能會延遲或無法擷取某些登入工作階段。預設值是 10 秒。
4. 在**使用者項目逾時**欄位中指定 DC Agent 重新整理其地圖中使用者項目的頻率 (小時)。預設值是 24 小時。
5. 在「電腦輪詢」下核取**啓動電腦輪詢**，讓 DC Agent 查詢電腦的使用者登入工作階段。這可以包括網域外部代理程式已經查詢的電腦。
 

DC Agent 使用 WMI (Windows Management Instruction) 來輪詢電腦。如果啓動電腦輪詢，則需要在用戶端電腦上設定 Windows Firewall 以允許使用連接埠 135 通訊。
6. 輸入**使用者地圖驗證時間間隔**，指定 DC Agent 聯繫用戶端電腦來驗證登入之使用者的頻率。預設值是 15 分鐘。
 

DC Agent 會將查詢結果與它傳送到 Filtering Service 之使用者地圖中的使用者名稱/IP 位址組做比較。降低此時間間隔可提升使用者地圖的準確性，但是會增加網路流量。增加此時間間隔可減少網路流量，但是會降低準確性。
7. 輸入**使用者項目逾時**期間，指定 DC Agent 重新整理其使用者地圖中透過電腦輪詢取得的項目。預設值是 1 小時。
 

DC Agent 會移除超過此逾時時段，因此 DC Agent 無法驗證為目前登入的使用者名稱 /IP 位址項目。增加此時間間隔會降低使用者地圖的準確性，因為地圖會將舊的使用者名稱保留較長的時間。



#### 注意

請勿將使用者項目逾時時間間隔設定的比使用者地圖驗證時間間隔短。因為這會造成在進行驗證之前就將使用者名稱從使用者地圖移除。

8. 按一下**確定**以立即儲存並實行所做的變更。

## Logon Agent

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [設定 Logon Agent](#)，第 188 頁
- ◆ [為每個代理程式實例配置不同的設定](#)，第 201 頁

在使用者登入網域的同時，Websense Logon Agent 會即時識別使用者。這可避免因查詢時間問題而遺漏使用者登入。

可以將 Logon Agent (也稱為 Authentication Server) 安裝於 Windows 或 Linux 電腦上。此代理程式會與 Windows 用戶端電腦上的 Websense Logon Application (LogonApp.exe) 共同作業，以在使用者登入 Windows 網域時識別使用者。

在大多數情況下，使用 DC Agent 與 Logon Agent 中的一個就已足夠，不過還是可以將這兩個代理程式一起使用。在此情況下，Logon Agent 的優先權高於 DC Agent。DC Agent 只有在 Logon Agent 發生罕見的遺漏情形時，才讓登入工作階段與 Filtering Service 通訊。

安裝 Logon Agent，然後將 Logon Application 從中央位置部署到用戶端電腦。如需詳細資訊，請參閱 [安裝手冊](#)。

安裝之後，設定代理程式與用戶端電腦和 Websense Filtering Service 通訊 (請參閱 [設定 Logon Agent](#))。



#### 注意

如果使用 Windows Active Directory (原生模式) 且 User Service 安裝在 Linux 電腦上，請參閱 [在 Linux 上執行 User Service](#)，第 319 頁以瞭解額外的配置步驟。

## 設定 Logon Agent

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定使用者識別方法](#)，第 177 頁
- ◆ [Logon Agent](#)，第 187 頁
- ◆ [設定多個代理程式](#)，第 199 頁

可使用 [設定 > 使用者識別 > Logon Agent](#) 頁面設定新的 Logon Agent 實例，以及設定套用至所有 Logon Agent 實例的全域設定。

新增 Logon Agent 實例的方法如下：

1. 在「基本代理程式配置」下輸入安裝代理程式之**伺服器**的 IP 位址或名稱。



#### 注意

電腦名稱必須以字母字元 (a-z) 開頭，而不能以數字或特殊字元開頭。

系統可能無法正確解析包含特定的延伸 ASCII 字元的電腦名稱。如果使用非英文版的 Websense 軟體，請輸入 IP 位址而非電腦名稱。

2. 輸入 Logon Agent 用來與其他 Websense 元件通訊的**連接埠**。預設值是 30602。

3. 若要在 Filtering Service 與 Logon Agent 之間建立已驗證連線，核取**啓動驗證**，然後輸入連線的**密碼**。
4. 按一下**確定**儲存所做的變更，或者繼續在畫面的下一個區段輸入其他配置資訊。

接下來自訂全域 Logon Agent 通訊設定。依照預設，您在此處所做變更會影響所有 Logon Agent 實例。

1. 在「Logon Agent 通訊」下輸入 Logon Agent 與其他 Websense 元件通訊時所用的**通訊連接埠**。預設值是 30602。
2. 除非「Websense 技術支援部」指示這麼做，否則請勿變更**診斷連接埠**設定。預設值是 30603。
3. 在「Logon Application 通訊」下指定登入應用程式用來與 Logon Agent 通訊的**連線埠**。預設值是 15880。
4. 輸入每個 Logon Agent 實例允許的**連線數目上限**。預設值是 200。  
如果網路很大，則可能需要增加這個數目。增加數目並不會增加網路流量。
5. 按一下**確定**儲存所做的變更，或者繼續在畫面的下一個區段輸入其他配置資訊。

若要設定決定使用者項目有效性的預設設定，您必須先決定在**持續模式**還是**非持續模式** (預設) 中運作 Logon Agent 和用戶端登入應用程式。

非持續模式的啓動方式是在啓動 **LogonApp.exe** 時加上 /NOPERSIST 參數。(如需詳細資訊，請參閱 Logon Agent 安裝所含的 **LogonApp\_ReadMe.txt** 檔案。)

- ◆ 若為持續模式，登入應用程式會定期聯繫 Logon Agent 來交換使用者登入資訊。  
如果使用持續模式，則指定**查詢時間間隔**以決定登入應用程式交換登入資訊的頻率。



#### 注意

如果變更這個值，所做的變更要等到上一個間隔期間過了之後才會生效。例如，如果將時間間隔從 15 分鐘變更成 5 分鐘，那麼必須等目前的 15 分鐘時間間隔結束後，才會開始每 5 分鐘查詢一次。

- ◆ 若為非持續模式，登入應用程式只會針對每個登入傳送一次使用者登入資訊給 Logon Agent。

如果使用非持續模式，則指定**使用者項目效期時段**。到達此逾時時段時，就會從使用者地圖移除使用者項目。

完成配置變更後，按一下**確定**來儲存設定。

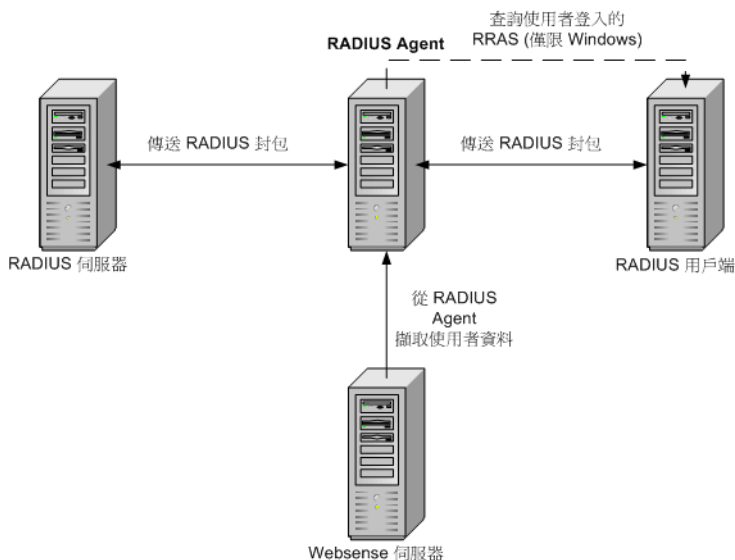
## RADIUS Agent

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [處理 RADIUS 流量](#)，第 191 頁
- ◆ [設定 RADIUS 環境](#)，第 191 頁
- ◆ [設定 RADIUS Agent](#)，第 192 頁
- ◆ [設定 RADIUS 用戶端](#)，第 193 頁
- ◆ [設定 RADIUS 伺服器](#)，第 194 頁
- ◆ [為每個代理程式實例配置不同的設定](#)，第 201 頁

Websense RADIUS Agent 可讓您使用 RADIUS 伺服器提供的驗證來套用以使用者和群組為基礎的政策。RADIUS Agent 使用撥接、Virtual Private Network (VPN)、Digital Subscriber Line (DSL) 或者其他遠端連線 (根據您的配置而定) 來無障礙識別存取您網路的使用者。

RADIUS Agent 與您網路中的 RADIUS 伺服器和 RADIUS 用戶端一起作業，處理並追蹤 Remote Access Dial-In User Service (RADIUS) 通訊協定流量。這讓您可以指派特定篩選政策給從遠端存取您網路的使用者或群組，以及本機使用者。



安裝 RADIUS Agent 時，此 Agent 會與現有的 Websense 元件整合。但是，還是必須適當的設定 RADIUS Agent、您的 RADIUS 伺服器以及您的 RADIUS 用戶端 (請參閱[設定 RADIUS Agent](#)，第 192 頁)。

## 處理 RADIUS 流量

Websense RADIUS Agent 就像是在 RADIUS 用戶端與 RADIUS 伺服器之間 (或多個用戶端和伺服器之間) 轉送 RADIUS 訊息的代理。

RADIUS Agent 不會直接驗證使用者。相反，代理程式會識別遠端使用者並將他們與 IP 位址關聯，讓 RADIUS 伺服器能夠驗證這些使用者。在正常情況下，RADIUS 伺服器會將驗證要求傳送給以 LDAP 為基礎的目錄服務。

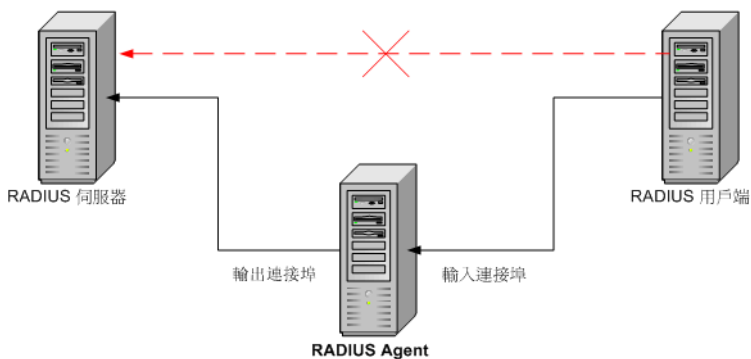
RADIUS Agent 會將使用者名稱與 IP 位址組儲存在使用者地圖中。如果您的 RADIUS 用戶端支援帳戶處理 (或使用者登入追蹤)，而且啟動帳戶處理時，RADIUS Agent 會從它收到的 RADIUS 訊息收集更多有關使用者登入工作階段的詳細資訊。

如果設定正確，Websense RADIUS Agent 可擷取並處理下列類型的所有 RADIUS 通訊協定封包：

- ◆ **要求存取**：由 RADIUS 用戶端傳送，要求授權網路存取連線嘗試。
- ◆ **接受存取**：由 RADIUS 伺服器傳送，回應「要求存取」訊息；通知 RADIUS 用戶端已授權並驗證嘗試的連線。
- ◆ **拒絕存取**：由 RADIUS 伺服器傳送，回應「要求存取」訊息；通知 RADIUS 用戶端嘗試的連線被拒絕。
- ◆ **要求停止帳戶處理**：由 RADIUS 用戶端傳送，通知 RADIUS 伺服器停止追蹤使用者活動。

## 設定 RADIUS 環境

Websense RADIUS Agent 可作為 RADIUS 用戶端與 RADIUS 伺服器之間的代理。此圖顯示 RADIUS Agent 與標準 RADIUS 設定在用法上的不同之處。



RADIUS Agent 和 RADIUS 伺服器應該安裝在不同的電腦上。代理程式和伺服器不能使用相同的 IP 位址，而且必須使用不同的連接埠。

安裝 RADIUS Agent 之後，在 Websense Manager 設定 RADIUS Agent (請參閱[設定 RADIUS Agent](#)，第 192 頁)。此外，您必須：

- ◆ 設定 RADIUS 用戶端 (一般是 Network Access Server [NAS]) 與 RADIUS Agent 通訊，而不是直接與 RADIUS 伺服器通訊。

- ◆ 設定 RADIUS 伺服器將 RADIUS Agent 用作代理 (請參閱 RADIUS 伺服器文件)。如果您有多個 RADIUS 伺服器，請分別設定每個伺服器。



#### 注意

如果您使用 Lucent RADIUS Server 和 RRAS，您必須設定 RADIUS 伺服器使用「密碼驗證通訊協定 (PAP)」，而且 RRAS 伺服器只接受 PAP 要求。如需詳細資訊，請參閱相關的產品文件。

## 設定 RADIUS Agent

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定使用者識別方法](#)，第 177 頁
- ◆ [RADIUS Agent](#)，第 190 頁
- ◆ [設定多個代理程式](#)，第 199 頁

可使用 **設定 > 使用者識別 > RADIUS Agent** 頁面設定新的 RADIUS Agent 實例，以及設定套用至所有 RADIUS Agent 實例的全域設定。

新增 RADIUS Agent 實例的方法如下：

1. 在「基本代理程式配置」下輸入安裝代理程式之**伺服器**的 IP 位址或名稱。



#### 注意

電腦名稱必須以字母字元 (a-z) 開頭，而不能以數字或特殊字元開頭。

系統可能無法正確解析包含特定的延伸 ASCII 字元的電腦名稱。如果使用非英文版的 Websense 軟體，請輸入 IP 位址而非電腦名稱。

2. 輸入 RADIUS Agent 用來與其他 Websense 元件通訊的**連接埠**。預設值是 30800。
3. 若要在 Filtering Service 與 RADIUS Agent 之間建立已驗證連線，核取**啓動驗證**，然後輸入連線的**密碼**。
4. 按一下**確定**儲存所做的變更，或者繼續在畫面的下一個區段輸入其他配置資訊。

接下來自訂全域 RADIUS Agent 設定。依照預設，您在此處所做變更會影響所有 RADIUS Agent 實例。不過可以覆寫代理程式配置檔案中標記星號 (\*) 的設定，以自訂該代理程式實例的行為 (請參閱 [為每個代理程式實例配置不同的設定](#)，第 201 頁)。



1. 輸入 RADIUS Agent 與其他 Websense 元件通訊時所用的**通訊連接埠**。預設值是 30800。
2. 除非「Websense 技術支援部」指示這麼做，否則請勿變更**診斷連接埠**設定。預設值是 30801。
3. 在「RADIUS 伺服器」下輸入 **RADIUS 伺服器 IP 或名稱**。RADIUS Agent 會將驗證要求轉送給 RADIUS 伺服器，而且必須知道此電腦的身份。
4. 如果使用 Microsoft RRAS，則輸入 **RRAS 電腦**的 IP 位址。Websense 軟體會查詢此電腦的使用者登入工作階段。
5. 輸入**使用者項目逾時**時間間隔，決定 RADIUS Agent 重新整理其使用者地圖的頻率。一般來說，預設的查詢值 (24 小時) 最佳。
6. 使用**驗證連接埠**和**帳戶處理連接埠**設定，指定 RADIUS Agent 用來傳送及接收驗證和帳戶處理要求的連接埠。對每種類型的通訊，您可以指定與下列組件通訊的連接埠：
  - RADIUS Agent 和 RADIUS 伺服器
  - RADIUS Agent 和 RADIUS 用戶端
7. 完成之後，按一下**確定**立即儲存設定。

## 設定 RADIUS 用戶端

您必須設定 RADIUS 用戶端，從而透過 RADIUS Agent 將驗證和帳戶處理要求傳輸至 RADIUS 伺服器。

修改您的 RADIUS 用戶端配置，從而實現以下操作：

- ◆ RADIUS 用戶端將驗證要求傳送至 RADIUS Agent 監聽驗證要求的電腦和連接埠。這就是在 RADIUS Agent 配置期間指定的**驗證連接埠**。
- ◆ RADIUS 用戶端將帳戶處理要求傳送至 RADIUS Agent 監聽帳戶處理要求的電腦和連接埠。這就是在 RADIUS Agent 配置期間指定的**帳戶處理連接埠**。

設定 RADIUS 用戶端的程序會因用戶端類型的不同而有所不同。如需詳細資訊，請參閱 RADIUS 用戶端文件。



### 注意

RADIUS 用戶端必須在其傳送的驗證和帳戶處理訊息中包括 **User-Name** 和 **Framed-IP-Address** 屬性。RADIUS Agent 會使用這些屬性的值來解譯並儲存使用者名稱 / IP 位址組。如果您的 RADIUS 用戶端預設未產生這項資訊，則設定用戶端產生資訊 (請參閱 RADIUS 用戶端文件)。

## 設定 RADIUS 伺服器

啓動 Websense RADIUS Agent 與 RADIUS 伺服器之間的適當通訊的方法如下：

- ◆ 將 RADIUS Agent 電腦的 IP 位址加入 RADIUS 伺服器的用戶端清單。如需相關指示，請參閱 RADIUS 伺服器文件。
- ◆ 定義 RADIUS 伺服器，以及所有使用代理程式與 RADIUS 伺服器通訊之 RADIUS 用戶端之間的共用密碼。共用密碼一般指定為驗證安全性選項。

設定 RADIUS 用戶端與 RADIUS 伺服器的共用密碼可確保安全傳輸 RADIUS 訊息。一般來說，共用密碼是一個通用文字字串。如需相關指示，請參閱 RADIUS 伺服器文件。



### 注意

RADIUS 伺服器必須在驗證和帳戶處理訊息中包括 **User-Name** 和 **Framed-IP-Address** 屬性。RADIUS Agent 會使用這些屬性的值來解譯並儲存使用者名稱/IP 位址組。如果您的 RADIUS 伺服器預設未產生這項資訊，則設定伺服器產生資訊 (請參閱 RADIUS 伺服器文件)。

## eDirectory Agent

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [設定 eDirectory Agent](#)，第 196 頁
- ◆ [為每個代理程式實例配置不同的設定](#)，第 201 頁

Websense eDirectory Agent 與 Novell eDirectory 一起作業，從而無障礙地識別使用者，讓 Websense 軟體得以根據指派給使用者、群組、網域或組織單位的政策來篩選使用者。

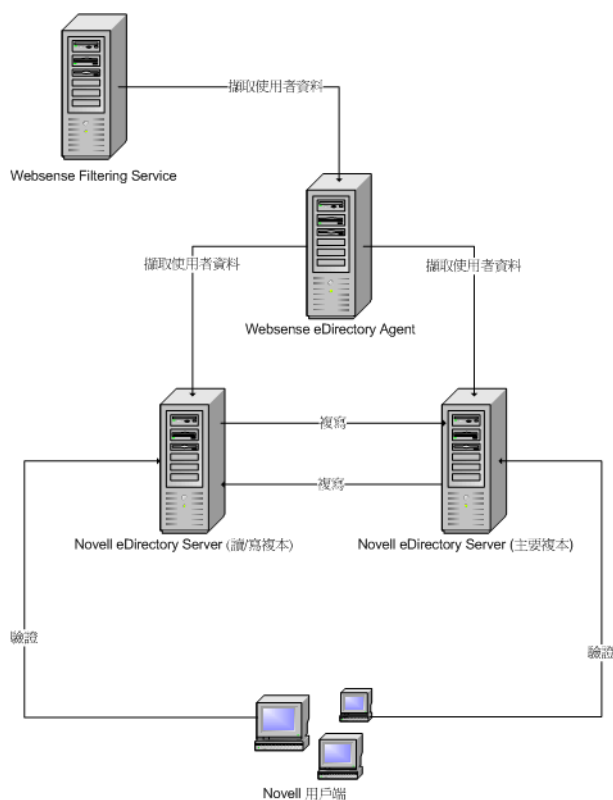
eDirectory Agent 會從驗證登入網路之使用者的 Novell eDirectory 收集使用者登入工作階段資訊。接著，代理程式會將每個經過驗證的使用者與某個 IP 位址關聯，並且將使用者名稱與 IP 位址組記錄到本機使用者地圖。然後，eDirectory Agent 再將這項資訊傳給 Filtering Service。



### 注意

多個使用者可以從執行 Windows 的 Novell 用戶端登入單一 Novell eDirectory 伺服器。這會將一個 IP 位址與多個使用者關聯。在此情況下，eDirectory Agent 的使用者地圖只會保留最後一位從指定 IP 位址登入之使用者的使用者名稱/IP 位址組。

一個 Websense eDirectory Agent 實例可支援一個主要 Novell eDirectory，加上任意數目的 Novell eDirectory 複本。



## 特殊配置考量

- ◆ 如果已將 Cisco Content Engine v5.3.1.5 或更新版本與 Websense 軟體整合：
  - 在安裝 Cisco Content Engine 的電腦上執行下列 Websense 服務：
    - Websense eDirectory Agent
    - Websense User Service
    - Websense Filtering Service
    - Websense Policy Server
  - 確定將所有 Novell eDirectory 複本都新增到相同電腦上的 **wseidir.ini** 檔案中。
  - 刪除 **eDirAgent.bak** 檔案。

在與安裝 Cisco Content Engine 和 Websense 軟體不同的電腦上執行 Websense Reporting Tools 服務。

- ◆ Websense 軟體支援使用 NMAS 與 eDirectory Agent。若要使用啓動 NMAS 的 eDirectory Agent，必須將 eDirectory Agent 安裝在也執行「Novell 用戶端」的電腦上。

## 設定 eDirectory Agent

相關主題：

- ◆ [無障礙識別](#)，第 175 頁
- ◆ [手動驗證](#)，第 177 頁
- ◆ [設定使用者識別方法](#)，第 177 頁
- ◆ [eDirectory Agent](#)，第 194 頁
- ◆ [設定 eDirectory Agent 使用 LDAP](#)，第 198 頁
- ◆ [設定多個代理程式](#)，第 199 頁

可使用 **設定 > 使用者識別 > eDirectory Agent** 頁面設定新的 eDirectory Agent 實例，以及設定套用至所有 eDirectory Agent 實例的全域設定。

新增 eDirectory Agent 實例的方法如下：

1. 在「基本代理程式配置」下輸入安裝代理程式之**伺服器**的 IP 位址或名稱。



### 注意

電腦名稱必須以字母字元 (a-z) 開頭，而不能以數字或特殊字元開頭。

系統可能無法正確解析包含特定的延伸 ASCII 字元的電腦名稱。如果使用非英文版的 Websense 軟體，請輸入 IP 位址而非電腦名稱。

2. 輸入 eDirectory Agent 用來與其他 Websense 元件通訊的**連接埠**。預設值是 30700。
3. 若要在 Filtering Service 與 eDirectory Agent 之間建立已驗證連線，核取**啟動驗證**，然後輸入連線的**密碼**。
4. 按一下**確定**儲存所做的變更，或者繼續在畫面的下一個區段輸入其他配置資訊。

接下來自訂全域 eDirectory Agent 通訊設定。依照預設，您在此處所做變更會影響所有 eDirectory Agent 實例。不過可以覆寫代理程式配置檔案中標記星號 (\*) 的設定，以自訂該代理程式實例的行為 (請參閱 [為每個代理程式實例配置不同的設定](#)，第 201 頁)。

1. 輸入 eDirectory Agent 與其他 Websense 元件通訊時所用的預設**通訊連接埠**。預設值是 30700。
2. 除非「Websense 技術支援部」指示這麼做，否則請勿變更**診斷連接埠**設定。預設值是 30701。
3. 在「eDirectory 伺服器」下指定一個**搜尋基礎** (根環境)，當做 eDirectory Agent 搜尋目錄中的使用者資訊的起點。

4. 提供 eDirectory Agent 用來與目錄通訊的管理使用者帳戶資訊：
  - a. 輸入 Novell eDirectory 管理使用者帳戶的**管理員識別名稱**。
  - b. 輸入該帳戶的**密碼**。
  - c. 指定**使用者項目逾時**時間間隔，決定將項目保留於代理程式之使用者地圖中的時間長短。  
此時間間隔應該比一般使用者登入工作階段長 30% 左右。這可避免在使用者完成瀏覽之前，就從地圖移除使用者項目。  
一般來說，建議使用預設值 (24 小時)。



#### 注意

在某些環境中，改為定時查詢「eDirectory 伺服器」來取得使用者登入更新，可能比使用使用者項目逾時時間間隔來決定 eDirectory Agent 更新其使用者地圖的頻率更為適合。請參閱 [啟動完整的 eDirectory 伺服器查詢](#)，第 198 頁。

5. 將主要「eDirectory 伺服器」以及所有複本加入 **eDirectory 複本**清單。若要將主要「eDirectory 伺服器」或複本新增到清單，按一下**新增**，然後根據 [新增 eDirectory 伺服器複本](#)，第 197 頁中的指示進行操作。

完成配置變更後，按一下**確定**來儲存設定。

## 新增 eDirectory 伺服器複本

一個 Websense eDirectory Agent 實例可支援一個主要 Novell eDirectory，加上在不同電腦上執行的任意數目的 Novell eDirectory 複本。

eDirectory Agent 必須能夠與每個執行目錄服務複本的電腦通訊。這可確保代理程式能夠以最快的速度取得最新的登入資訊，而且不需要等待 eDirectory 複製發生。

Novell eDirectory 會每 5 分鐘複製一次唯一識別已登入使用者的屬性。除了此複製時間延遲之外，eDirectory Agent 會在使用者登入任何 eDirectory 複本時，即時取得新的登入工作階段。

設定 eDirectory Agent 安裝與 eDirectory 通訊的方法如下：

1. 在「新增 eDirectory 複本」畫面中，輸入 eDirectory **伺服器** (主要或複本) 的 IP 位址或名稱。
2. 輸入 eDirectory Agent 用來與 eDirectory 電腦通訊的**連接埠**。
3. 按一下**確定**返回 eDirectory Agent 頁面。新的項目就會顯示在「eDirectory 複本」清單中。
4. 對其他 eDirectory 伺服器重複上述程序。
5. 按一下**確定**快取變更，然後按一下**全部儲存**。
6. 停止並啟動 eDirectory Agent，讓代理程式可開始與新的複本通訊。如需指示，請參閱 [停止和啟動 Websense 服務](#)，第 245 頁。

## 設定 eDirectory Agent 使用 LDAP

Websense eDirectory Agent 可使用 Netware Core Protocol (NCP) 或 Lightweight Directory Access Protocol (LDAP) 從 Novell eDirectory 取得使用者登入資訊。依照預設，Windows 作業系統上的 eDirectory Agent 使用 NCP。在 Linux 作業系統上，eDirectory Agent 必須使用 LDAP。

如果您在 Windows 上執行 eDirectory Agent，但是想讓代理程式使用 LDAP 查詢 Novell eDirectory，請設定代理程式使用 LDAP 而非 NCP。一般來說，NCP 提供更有效的查詢機制。

設定 Windows 上的 eDirectory Agent 使用 LDAP 的方法如下：

1. 確定網路中至少有一個包含所有要監控並篩選之目錄物件的 Novell eDirectory 複本。
2. 停止 Websense eDirectory Agent 服務 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。
3. 瀏覽至 eDirectory Agent 安裝目錄 (預設為 `\Program Files\Websense\bin`)，然後在文字編輯器中開啓 `wseidir.ini` 檔案。
4. 將 **QueryMethod** 項目修改如下：  
QueryMethod=0  
這將「代理程式」設為使用 LDAP 來查詢 Novell eDirectory。(預設值為 1，代表使用 NCP。)
5. 儲存並關閉檔案。
6. 重新啓動 Websense eDirectory Agent 服務。

## 啓動完整的 eDirectory 伺服器查詢

在小型網路中，可設定讓 Websense eDirectory Agent 定時查詢「eDirectory 伺服器」的所有已登入使用者。這讓代理程式可以偵測新登入的使用者，以及自上次查詢後已經登出的使用者，並且據以更新它的本機使用者地圖。



### 重要

不建議在大型網路設定 eDirectory Agent 使用完整查詢，因為傳回查詢結果所需的時間將根據已登入使用者人數而定。登入的使用者越多，對效能的影響就越大。

在 eDirectory Agent 啓動完整查詢之後，就不會使用**使用者項目逾時**時間間隔，因為查詢會識別已登出的使用者。依照預設，每 30 秒會執行一次查詢。

以下列兩種方式啓動這項功能會增加 eDirectory Agent 的處理時間：

- ◆ 每次執行查詢來擷取已登入使用者之名稱所需的時間
- ◆ 處理使用者名稱資訊、移除本機使用者地圖中已過時的項目，以及根據最新查詢新增項目所需的時間

eDirectory Agent 會在每次查詢之後檢查整個本機使用者地圖，而不只是識別新的登入。這項作業所需的時間取決於每個查詢所傳回的使用者人數。因此，查詢作業會同時影響 eDirectory Agent 和 Novell eDirectory 伺服器的回應時間。

啓動完整查詢的方法如下：

1. 在 eDirectory Agent 電腦上，瀏覽至 Websense **bin** 目錄 ( 預設為 C:\Program Files\Websense\bin 或 /opt/Websense/bin )。
2. 找到 **wseidir.ini** 檔案，然後在其他目錄中建立它的備份複本。
3. 在文字編輯器 (例如「記事本」或 vi) 中開啓 **wseidir.ini**。
4. 移至檔案的 **[eDirAgent]** 區段並尋找下列項目：

```
QueryMethod=<N>
```

記下 QueryMethod 值，以備稍後需要還原成預設設定時使用。

5. 將 **QueryMethod** 值更新如下：
  - 如果目前的值是 0 ( 透過 LDAP 與目錄通訊 )，則將值變更為 2。
  - 如果目前的值是 1 ( 透過 NCP 與目錄通訊 )，則將值變更為 3。



#### 注意

如果變更此查詢值讓系統效能降低，將 QueryMethod 還原回其先前的值。

6. 如果預設的查詢時間間隔 (30 秒) 不適合您的環境，請適當地編輯 **PollInterval** 值。  
請注意，間隔時間以**毫秒**為單位。
7. 儲存並關閉檔案。
8. 重新啓動 Websense eDirectory Agent 服務 (請參閱[停止和啓動 Websense 服務](#)，第 245 頁)。

## 設定多個代理程式

相關主題：

- ◆ [DC Agent](#)，第 185 頁
- ◆ [Logon Agent](#)，第 187 頁
- ◆ [RADIUS Agent](#)，第 190 頁
- ◆ [eDirectory Agent](#)，第 194 頁

您可以結合相同網路內的多個無障礙識別代理程式。如果您的網路配置需要多個代理程式，則最好是將每個代理程式安裝在不同的電腦上。不過在某些情況下，可設定讓 Websense 軟體在單一電腦上使用多個代理程式。

支援的無障礙識別代理程式組合如下：

組合	是否在相同的電腦上？	是否在相同的網路中？	所需的配置
多個 DC Agent	否	是	確定所有 DC Agent 實例都可與 Filtering Service 通訊。
多個 RADIUS Agent	否	是	設定每個實例與 Filtering Service 通訊。
多個 eDirectory Agent	否	是	設定每個實例與 Filtering Service 通訊。
多個 Logon Agent	否	是	設定每個實例與 Filtering Service 通訊。
DC Agent 搭配 RADIUS Agent	是	是	將這些代理程式安裝於不同的目錄中。設定每個代理程式使用不同的通訊連接埠與 Filtering Service 通訊。
DC Agent 搭配 eDirectory Agent	否	否	Websense 軟體不支援在同一個部署中同時與 Windows 和 Novell 目錄服務通訊。不過可以同時安裝這兩個代理程式，然後只啓用 1 個代理程式。
DC Agent 搭配 Logon Agent	是	是	設定這兩個代理程式與 Filtering Service 通訊。依照預設，每個代理程式均使用唯一的連接埠，因此除非變更連接埠，否則不會發生連接埠衝突的問題。
eDirectory Agent 搭配 Logon Agent	否	否	Websense 軟體不支援在同一個部署中同時與 Windows 和 Novell 目錄服務通訊。不過可以同時安裝這兩個代理程式，然後只啓用 1 個代理程式。
RADIUS Agent 搭配 eDirectory Agent	是	是	設定每個代理程式使用不同的通訊連接埠與 Filtering Service 通訊。
DC Agent 搭配 Logon Agent 與 RADIUS Agent	是	是	此組合很少見，但是支援。將每個代理程式安裝在不同目錄中。設定所有代理程式使用不同的通訊連接埠與 Filtering Service 通訊。



## 為每個代理程式實例配置不同的設定

Websense Manager 無障礙識別代理程式配置設定是全域性的，這些設定會套用至您安裝的所有代理程式實例。不過，如果有多個任意代理程式的實例，您可以獨立設定某一個實例。

您為某個特定代理程式實例指定的唯一設定會覆寫「設定」對話方塊中的全域設定。可以覆寫的設定會標記星號 (\*)。

1. 停止無障礙識別代理程式服務 (請參閱[停止和啓動 Websense 服務](#)，第 245 頁)。
2. 在執行代理程式實例的電腦上，瀏覽至代理程式安裝目錄，然後在文字編輯器中開啓適當的檔案：
  - 針對 DC Agent：transid.ini
  - 針對 Logon Agent：authserver.ini
  - 針對 eDirectory Agent：wsedir.ini
  - 針對 RADIUS Agent：wsradius.ini
3. 尋找要針對此代理程式實例變更的參數 (請參閱[INI 檔案參數](#)，第 202 頁)。例如，您可以在此代理程式實例與其他 Websense 服務之間啓用已認證連線。若要這麼做，請在 INI 檔案中輸入 password 參數的值：
 

```
password=[xxxxxxx]
```
4. 視需要修改其他值。
5. 儲存並關閉 INI 檔案。
6. 如果變更 DC Agent 設定，則必須移除 Websense bin 目錄 (預設為 C:\Program Files\Websense\bin) 中的 2 個檔案：
  - a. 停止 DC Agent 電腦上的所有 Websense 服務 (請參閱[停止和啓動 Websense 服務](#)，第 245 頁)。
  - b. 刪除下列檔案：
 

```
Journal.dat
XidDcAgent.bak
```

 系統會在啓動 Websense DC Agent 服務時重新建立這些檔案。
  - c. 重新啓動 Websense 服務 (包括 DC Agent)，然後跳到[步驟 8](#)。
7. 重新啓動無障礙識別代理程式服務。
8. 更新 Websense Manager 中的代理程式設定：
  - a. 移至設定 > 使用者識別。
  - b. 在無障礙識別代理程式下選擇代理程式，然後按一下編輯。



### 注意

如果修改此代理程式實例的**連接埠**值，則移除並重新新增代理程式。首先，選擇現有代理程式項目並按一下**刪除**，然後按一下**新增代理程式**。

- c. 驗證此代理程式實例使用的**伺服器 IP 或名稱**以及**連接埠**。如果在 INI 檔案中指定唯一的連接埠號碼，則確定您輸入的值與檔案中的值相同。
- d. 如果在 INI 檔案中指定唯一的驗證密碼，則確定此處顯示的**密碼**正確無誤。
- e. 按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## INI 檔案參數

<b>Websense Manager 欄位標籤</b>	<b>.ini 參數名稱</b>	<b>說明</b>
通訊連接埠 (所有代理程式)	port	代理程式與其他 Websense 服務通訊所用的連接埠。
診斷連接埠 (所有代理程式)	DiagServerPort	代理程式疑難排解工具監聽代理程式資料的連接埠。
密碼 (所有代理程式)	password	代理程式驗證其他 Websense 服務連線時所用的密碼。指定密碼即可啟動驗證。
查詢時間間隔 (DC Agent)	QueryInterval	DC Agent 查詢網域控制站的時間間隔。
伺服器 IP 或名稱 連接埠 (eDirectory Agent)	Server=IP:port	執行 eDirectory Agent 之電腦的 IP 位址和連接埠號碼。
搜尋基礎 (eDirectory Agent)	SearchBase	Novell eDirectory 伺服器的根環境。
管理員識別名稱 (eDirectory Agent)	DN	Novell eDirectory 伺服器之管理使用者的名稱。
密碼 (eDirectory Agent)	PW	Novell eDirectory 伺服器管理使用者的密碼。
RADIUS 伺服器 IP 或名稱	RADIUSHost	您 RADIUS 伺服器電腦的 IP 位址或名稱。
RRAS 電腦 IP (僅限 Windows) (RADIUS Agent)	RRASHost	執行 RRAS 之電腦的 IP 位址。Websense 會查詢此電腦的使用者登入工作階段。
驗證連接埠： 在 RADIUS Agent 與 RADIUS 伺服器之間	AuthOutPort	RADIUS 伺服器監聽驗證要求的連接埠。
驗證連接埠： 在 RADIUS 用戶端與 RADIUS Agent 之間	AuthInPort	RADIUS Agent 接受驗證要求的連接埠。

帳戶處理連接埠： 在 RADIUS Agent 與 RADIUS 伺服器之間	AccOutPort	RADIUS 伺服器監聽 RADIUS 帳戶處理訊息的連接埠。
帳戶處理連接埠： 在 RADIUS 用戶端與 RADIUS Agent 之間	AccInPort	RADIUS Agent 接受帳戶處理要求的連接埠。

## 設定代理程式忽略特定的使用者名稱

可設定無障礙識別代理程式以忽略與實際使用者沒有關聯的登入名稱。這項功能一般用於處理部份 Windows 200x 和 XP 服務與網路中的網域控制站聯繫的方式。

例如，**user1** 登入網路，且由網域控制站識別為 **computerA/user1**。該使用者由指派給 **user1** 的 Websense 政策篩選。如果在使用者的電腦啟動的服務使用 **computerA/ServiceName** 識別來聯繫網域控制站，這將會造成篩選問題。Websense 軟體會將 **computerA/ServiceName** 當做未指派政策的新使用者，然後使用電腦政策或預設政策來篩選此使用者。

解決此問題的方法如下：

1. 停止代理程式服務 (請參閱 [停止和啟動 Websense 服務](#)，第 245 頁)。
2. 瀏覽至 `\\Websense\bin\` 目錄，然後在文字編輯器中開啓 **ignore.txt** 檔案。
3. 在單獨的行中輸入每個使用者名稱。請勿包括萬用字元，例如「\*」：

```
maran01
WindowsServiceName
```

Websense 軟體將會忽略這些使用者名稱 (不論它們關聯的電腦為何)。

若要提示 Websense 軟體忽略特定網域內的使用者名稱，則使用 **username, domain** 格式。

```
aperez, engineering1
```

4. 完成之後儲存並關閉檔案。
5. 重新啟動代理程式服務。

代理程式會忽略指定的使用者名稱，而 Websense 軟體不會將這些名稱納入篩選考量。



# 11

## 委派管理

### 相關主題

- ◆ [管理角色簡介](#)，第 206 頁
- ◆ [管理員簡介](#)，第 206 頁
- ◆ [管理角色快速入門](#)，第 210 頁
- ◆ [啓用 \*Websense Manager\* 的存取權限](#)，第 216 頁
- ◆ [使用委派管理](#)，第 220 頁
- ◆ [多個存取 \*Websense Manager\* 的管理員](#)，第 228 頁
- ◆ [定義所有角色的篩選限制](#)，第 229 頁

委派管理提供多種強大且靈活的方法，可供用於管理特定用戶端群組的網際網路篩選與報告。當所有使用者都在一個集中的位置時，這是一種可以很有效的方法，可以將網際網路存取管理以及報告的責任分派給個別管理人員。這對包含多個地點與地理區域的大型組織來說特別有用，因為本機管理員可以為其地區中之使用者管理網際網路存並報告篩選活動。

實行委派管理包含替每個要由相同管理員管理的用戶端群建立管理角色。每個角色的個別管理員均可被授予管理政策或產生報告的權限，或者同時授予這兩種權限。請參閱[管理角色快速入門](#)，第 210 頁。

超級管理員角色是預先安裝的，其中包括預設的管理使用者 *Websense Administrator*。與其他角色的管理員相比，「超級管理員」可以存取更廣範圍的政策和配置設定。請參閱[超級管理員](#)，第 207 頁。

## 管理角色簡介

### 相關主題

- ◆ [管理員簡介](#)，第 206 頁
- ◆ [管理角色快速入門](#)，第 210 頁

管理角色是一個由一或多位管理員管理的受管理的用戶端集合 — 使用者、群組、網域、組織單位、電腦和網路範圍。您可以授予個別管理員可將政策套用到角色的用戶端、產生報告或這兩者皆可的權限。

Websense 軟帶有一個預先定義的「超級管理員」角色。還有一個預設使用者 `WebsenseAdministrator`，自動屬於「超級管理員」角色的一個成員。您可以新增管理員到此角色，但是無法刪除預設管理員。



### 重要

您無法刪除預先定義的「超級管理員」角色。預設使用者 `WebsenseAdministrator` 是「超級管理員」角色中的一個管理員，但是未列在角色中。您無法刪除或變更 `WebsenseAdministrator` 的權限。

您可以根據您組織的需要，建立不限數目的角色。例如，您可以替每個部門建立一個角色，讓部門經理做為管理員，並將部門成員當做受管理的用戶端。在一個地點分散的組織中，您可以為每個位置建立一個角色，然後將該位置的所有使用者指派為該角色的受管理用戶端。接著，將位於該位置的一或多位人員指派為管理員。

如需可用於定義管理員之選項的資訊，請參閱[管理員簡介](#)，第 206 頁。

如需建立角色及設定權限的指示，請參閱[使用委派管理](#)，第 220 頁。

## 管理員簡介

管理員指的是可以存取 `Websense Manager` 來管理政策或產生用戶端群組之報告的個人。管理員的具體權限會根據角色類型的不同而有所不同。

- ◆ 「超級管理員」是 `Websense Manager` 中預先定義的一個特殊角色。此角色為定義存取權限提供了最大的靈活性。請參閱[超級管理員](#)，第 207 頁。
- ◆ 委派管理角色只能由「超級管理員」建立。這些角色的管理員所具有的存取權限就比較有限制。請參閱[委派管理員](#)，第 208 頁。

除此以外，您可以建立一些只能進行報告的委派管理角色，讓不同的個人能夠產生報告，而不需要賦予他們管理政策的責任。

您可以使用管理員的網路登入認證將管理員指派給角色，或者您可以建立只用來存取 `Websense Manager` 的特殊帳戶。請參閱[啟用 `Websense Manager` 的存取權限](#)，第 216 頁。

## 超級管理員

### 相關主題

- ◆ [管理員簡介](#)，第 206 頁
- ◆ [委派管理員](#)，第 208 頁
- ◆ [具有多個角色的管理員](#)，第 209 頁

「超級管理員」角色在安裝期間建立。預設使用者 `WebsenseAdministrator` 會被自動指派給此角色。因此，當您第一次使用該使用者名稱以及在安裝時設定的密碼登入時，您具有 `Websense Manager` 中所有政策、報告和配置設定的完整管理存取權。

為了保留此帳戶的完整存取權 `WebsenseAdministrator` 並不會顯示在「超級管理員」角色的管理員清單中。您無法將它刪除，也無法修改其權限。

您可以根據需要新增管理員到「超級管理員」角色。每位管理員均可被授予下列權限：

- ◆ **政策** 權限允許「超級管理員」建立及編輯委派管理角色，以及適當地將篩選器和政策複製到這些角色。他們也可以建立及編輯篩選元件、篩選器和政策，並可將政策套用至未受其他任何角色管理的用戶端。

此外，擁有政策權限的「超級管理員」可以檢視稽核記錄，並被授予存取 `Websense` 配置和其他選項的權限，如下所示：

- **無條件** 權限可供「超級管理員」存取 `Websense` 安裝的所有系統配置設定，例如帳戶、`Policy Server` 和 `Remote Filtering Server` 設定風險等級指派以及記錄選項。

無條件「超級管理員」可以選擇建立「篩選器鎖定」針對受委派管理角色管理之所有使用者封鎖特定類別和通訊協定。如需詳細資訊，請參閱 [定義所有角色的篩選限制](#)，第 229 頁。

無條件「超級管理員」可以修改「超級管理員」角色，從而根據需要新增及刪除管理員。他們也可以刪除委派管理角色，或者刪除這些角色中的管理員或用戶端。

- **有條件** 權限可供「超級管理員」存取資料庫下載、目錄服務、使用者識別以及 `Network Agent` 配置設定。同時具有報告權限的有條件「超級管理員」可以存取報告工具的配置設定。

有條件「超級管理員」可以新增 `Websense` 使用者帳戶，但是無法刪除它們。他們可以建立及編輯委派管理角色，但是無法刪除角色、管理員或指派給他們的受管理用戶端。他們也無法刪除「超級管理員」角色中的管理員。

- ◆ **報告** 權限可供「超級管理員」存取所有報告功能以及對所有使用者進行報告。無條件「超級管理員」自動就具有報告權限。

如果管理員只擁有報告權限「常用工作」清單中的「建立政策」、「重新分類 URL」和「解除封鎖 URL」選項將不可用。另外，「工具箱」中的「檢查政策」選項。

建立多個無條件「超級管理員」可以確保在無法使用主要「超級管理員」時，另一個管理員可以存取所有 Websense 政策和配置設定。

請注意2 個管理員不能同時登入以管理相同角色的政策。如需預防衝突的資訊，請參閱[多個存取 Websense Manager 的管理員](#)，第 228 頁。

「超級管理員」角色的獨特權限讓此角色中的管理員能夠存取所有角色。若要在登入之後切換至其他角色，請移至標題中的**角色**下拉式清單，然後選取角色。

變更角色之後，您的政策權限將只限於委派管理角色的權限。您所建立的篩選器和政策只能供該角色的管理員使用。它們只能套用到該角色中的受管理用戶端。請參閱[委派管理員](#)，第 208 頁。

報告權限是累計的，亦即您具有您屬於其管理員之所有角色的結合權限。無條件「超級管理員」具有完整的報告權限，而不論存取什麼角色。

## 委派管理員

### 相關主題

- ◆ [管理員簡介](#)，第 206 頁
- ◆ [超級管理員](#)，第 207 頁
- ◆ [具有多個角色的管理員](#)，第 209 頁

委派管理員可管理指派給特定角色的用戶端。您可以將政策權限、報告權限或兩者同時指派給每位管理員。

具有**政策**權限的委派管理員可套用政策到指派給其角色的用戶端，藉此決定每個用戶端的網際網路存取權。在這個責任範圍內，委派管理員可以建立、編輯及刪除受限於「超級管理員」建立之「篩選器鎖定」的政策和篩選器。請參閱[定義所有角色的篩選限制](#)，第 229 頁。



### 注意

委派的管理員對他們所管理之用戶端的網際網路活動具有很大的控制權。為了確保能夠負責地實行這項控制並使其符合您組織可接受的使用政策，「超級管理員」應該使用「稽核記錄」頁面來監督管理員所做的變更。請參閱[檢視並匯出稽核記錄](#)，第 244 頁。

委派管理員不能刪除「預設」政策。

委派管理員可以編輯篩選器元件，但是會有一些限制。如需詳細資訊，請參閱[建立政策和篩選器](#)，第 214 頁。

擁有政策權限且使用 Websense 使用者帳戶登入 Websense Manager 的管理員也可以變更他們自己的 Websense 密碼 (請參閱[Websense 使用者帳戶](#)，第 218 頁)。



擁有**報告**權限的委派管理員可使用的選項將根據角色的設定方式不同而有所不同。他們也許只能夠對受他們的角色管理之用戶端進行報告，或者可對所有用戶端進行報告。他們也許可以存取所有報告功能，或者只能存取比較有限的報告功能。如需詳細資訊，請參閱[編輯角色](#)，第 221 頁。

只擁有報告權限的管理員只能使用右側捷徑窗格（「常用工作」和「工具箱」）中的部份選項。

## 具有多個角色的管理員

### 相關主題

- ◆ [管理員簡介](#)，第 206 頁
- ◆ [超級管理員](#)，第 207 頁
- ◆ [委派管理員](#)，第 208 頁

根據您組織之需求的不同，可以指派多個角色給同一個管理員。指派給多個角色的管理員在登入時必須選擇單一角色進行管理。

登入之後，您所具備的權限如下：

- ◆ **政策**：您可以新增及編輯在登入時選取之角色的篩選器和政策，並可將政策套用到該角色的受管理用戶端。「委派管理」頁面中列有指派給您的所有角色，供您檢視每個角色的受管理用戶端和報告權限。
- ◆ **報告**：您具有您所屬所有角色的結合報告權限。例如，假設為您指派了 3 個角色，分別具有如下報告權限：

- 角色 1：不報告
- 角色 2：僅有受管理用戶端的報告，僅限調查報告
- 角色 3：執行所有用戶端的報告擁有所有的報告，功能的完全存取權限

在此情況下不論您在登入時選擇哪個角色，您都可以檢視「今天」和「記錄」頁面中的報告，以及使用所有報告功能執行所有用戶端的報告。

如果您登入只為執行報告，標題列的「角色」欄位會指示您是否具有「完整報告」（對所有用戶端的報告）或「受限報告」（僅有受管理用戶端的報告）權限。

## 管理角色快速入門

### 相關主題

- ◆ [管理角色簡介](#)，第 206 頁
- ◆ [通知管理員](#)，第 212 頁
- ◆ [委派管理員工作](#)，第 212 頁

若要開始進行委派管理「超級管理員」需要完成下列工作：

- ◆ 決定管理員登入 Websense Manager 的方式。請參閱[啟用 Websense Manager 的存取權限](#)，第 216 頁。
- ◆ 新增角色並設定它們。請參閱[使用委派管理](#)，第 220 頁。
- ◆ 告知管理員他們的職責與選項。請參閱[通知管理員](#)，第 212 頁。

除了這些必要的工作之外，委派管理另外還有一些相關的選擇性工作。

### 建立「篩選器鎖定」

無條件「超級管理員」可以建立「篩選器鎖定」指定針對所有委派管理角色中的受管理用戶端封鎖特定類別和通訊協定。對於在委派管理角色中建立或複製到委派管理角色的所有篩選器，這些限制會自動強制執行，而且無法由委派管理員修改。



#### 注意

「篩選器鎖定」不適用於由「超級管理員」角色管理的用戶端。

「篩選器鎖定」也可以封鎖並鎖定與所選類別相關的檔案類型和關鍵字，並且強制記錄所選的通訊協定。請參閱[建立「篩選器鎖定」](#)，第 230 頁。

### 移動用戶端

若您以「超級管理員」身份登入時將用戶端新增到「用戶端」頁面，則會將該用戶端指派給「超級管理員」角色。您無法在「編輯角色」頁面中，將該用戶端新增到委派管理角色。理想上，您應該直接將用戶端新增到角色，而不是在「超級管理員」角色內指派政策。不過，這並不一定可行。

若要將「超級管理員」角色的用戶端轉移到其他角色，請使用「用戶端」頁面中的**移至角色**選項。請參閱[將用戶端移到角色](#)，第 63 頁。

移動時，會將套用於「超級管理員」角色的政策複製到委派管理角色。政策強制執行的篩選器也會一併複製。在這個複製過程中，會更新篩選器，使其強制執行「篩選器鎖定」的限制，如果有的話。

在目標角色中系統會在篩選器或政策名稱的結尾加上「(已複製)」標記。該角色的管理員即可容易的識別新項目並適當地加以更新。



### 注意

每次複製篩選器或政策到同一個角色時，「(已複製)」標記後會有一個數字並隨著每次新的複製增加：「(已複製 1)」、「(已複製 2)」以此類推。每個複本都會變成角色內單獨的篩選器或政策。

建議角色中的管理員重新命名篩選器和政策，並視需要對其進行編輯，以釐清它們的設定並將重複項目減至最低。這些變更可以簡化未來的維護工作。

「超級管理員」角色中的「全部允許」篩選器允許存取所有類別或通訊協定，但是無法編輯。為了保有「超級管理員」執行「篩選器鎖定」的能力，這些篩選器無法複製到委派管理角色。

如果指派給正在移動之用戶端的政策強制執行「全部允許」篩選器，則此用戶端要等到您套用未使用「全部允許」篩選器的政策之後才可以移動。

將用戶端移至新角色之後，只有該角色的管理員才可以修改用戶端的政策或政策強制執行的篩選器。變更「超級管理員」角色中的原始政策或篩選器並不會影響委派管理角色中的政策或篩選器複本。

## 複製篩選器和政策

最初，「超級管理員」建立的篩選器和政策只能供「超級管理員」角色中的管理員使用。而您可以使用**複製到角色**選項，將篩選器和政策複製到委派管理角色，不需要將用戶端移至角色。請參閱[將篩選器和政策複製到角色](#)，第 149 頁。

直接複製篩選器和政策時，其限制與在移動用戶端時複製的篩選器和政策所受的限制相同。

- ◆ 「篩選器鎖定」限制會在進行複製時執行。
- ◆ 「全部允許」類別和通訊協定篩選器無法複製。
- ◆ 角色中複製的篩選器和政策的名稱中會有一個「(已複製)」標記做為識別。

開始複製之前，請編輯政策說明，讓目標角色中的管理員可以清楚知道政策的用途。

## 將政策套用到其餘的用戶端

未特別指派給委派管理角色的用戶端將由「超級管理員」管理。系統不會提供「超級管理員」角色的「受管理的用戶端」清單。

若要在這些用戶端套用政策，請將它們增加到「政策管理」>「用戶端」頁面。請參閱[新增用戶端](#)，第 61 頁。尚未被指派具體政策的用戶端將由其角色的「預設」政策管理。

您有時候可能會無法將用戶端新增到「用戶端」頁面。當用戶端屬於指派給另一個角色之網路、群組、網域或組織單位的成員時，就會發生此情況。如果其他角色的管理員已對網路或群組的個別成員套用政策，就無法將這些用戶端新增到「超級管理員」角色。

## 通知管理員

### 相關主題

- ◆ [管理角色簡介](#)，第 206 頁
- ◆ [管理角色快速入門](#)，第 210 頁

將個別人員指派為任一管理角色中的管理員之後，請務必告知他們下列資訊。

- ◆ 用於登入 Websense Manager 的 URL。預設為：  
`https://<ServerIP>:9443/mng/`  
使用執行 Websense Manager 之機器的 IP 位址來代替 <ServerIP>。
- ◆ 登入時選擇的 Policy Server (如果適用)。在有多個 Policy Server 的環境中，管理員在登入時必須要選擇一個 Policy Server。他們必須選擇設定為與驗證其管理之用戶端的目錄服務通訊的 Policy Server。
- ◆ 登入 Websense Manager 時應該要使用他們的網路登入帳戶，還是使用 Websense 使用者帳戶。如果管理員使用 Websense 使用者帳戶登入，請提供使用者名稱和密碼。
- ◆ 他們的權限；建立並套用政策至角色中的用戶端、產生報告，或者兩者均可。告知管理員誰同時具備政策和報告權限，便於考慮在工作階段中計畫執行之活動。如果他們只計畫產生報告，那麼建議他們前往標題中的**角色**欄位，然後選擇**釋放政策權限**。這會釋放角色的政策權限，讓其他管理員能夠存取 Websense Manager 並管理該角色的政策。
- ◆ 如何尋找受其角色管理的用戶端。管理員可以前往「政策管理」>「委派管理」，然後按一下他們的角色名稱來顯示「編輯角色」頁面，其中包含受管理的用戶端的清單。
- ◆ 「篩選器鎖定」所施加的限制 (若有任何類別或通訊協定已被封鎖並鎖定)。
- ◆ 一般由管理員執行的工作。請參閱[委派管理員工作](#)，第 212 頁。

新增或變更自訂檔案類型和通訊協定時，請務必通知委派管理員。這些元件會自動顯示在所有角色的篩選器和政策中，所以知道什麼時候做了變更對於這些管理員很重要。

## 委派管理員工作

### 相關主題

- ◆ [管理角色簡介](#)，第 206 頁
- ◆ [管理角色快速入門](#)，第 210 頁
- ◆ [通知管理員](#)，第 212 頁

具有**政策**權限的委派管理員可以執行下列工作。

- ◆ [檢視您的使用者帳戶](#)，第 213 頁
- ◆ [檢視您的角色定義](#)，第 213 頁
- ◆ [新增用戶端到「用戶端」頁面](#)，第 214 頁
- ◆ [建立政策和篩選器](#)，第 214 頁
- ◆ [將政策套用至用戶端](#)，第 216 頁

**報告**權限可以精細地指派。授予您角色的特定報告權限決定了具有報告權限的管理員可以執行下列的哪些工作。請參閱[產生報告](#)，第 216 頁。

## 檢視您的使用者帳戶

### 相關主題

- ◆ [委派管理員工作](#)，第 212 頁
- ◆ [檢視您的角色定義](#)，第 213 頁
- ◆ [新增用戶端到「用戶端」頁面](#)，第 214 頁
- ◆ [建立政策和篩選器](#)，第 214 頁
- ◆ [將政策套用至用戶端](#)，第 216 頁

如果您使用網路認證登入 Websense Manager，系統將會透過您的網路目錄服務處理密碼變更。請洽詢您的系統管理員取得協助。

如果已經為您指派有 Websense 使用者名稱和密碼，您可以檢視您帳戶的相關資訊，以及變更您在 Websense Manager 內的密碼。

1. 前往**政策管理** > **委派管理**。
2. 按一下頁面頂部的**管理 Websense 使用者帳戶**。
3. 若要變更您的密碼，請按一下**變更密碼**。請參閱[變更 Websense 使用者的密碼](#)，第 219 頁。
4. 按一下**檢視**，即可顯示您為管理員的角色清單。

## 檢視您的角色定義

### 相關主題

- ◆ [委派管理員工作](#)，第 212 頁
- ◆ [檢視您的使用者帳戶](#)，第 213 頁
- ◆ [新增用戶端到「用戶端」頁面](#)，第 214 頁
- ◆ [建立政策和篩選器](#)，第 214 頁
- ◆ [將政策套用至用戶端](#)，第 216 頁

開啟「委派管理」頁面並按一下您的角色名稱，即可顯示「編輯角色」頁面，其中列示角色的受管理用戶端。此頁面中同時顯示具有此角色之報告權限的管理員所能執行的報告功能。

只有報告權限的管理員無法檢視此頁面。這些管理員只能使用指定的報告功能。

## 新增用戶端到「用戶端」頁面

### 相關主題

- ◆ [委派管理員工作](#)，第 212 頁
- ◆ [檢視您的使用者帳戶](#)，第 213 頁
- ◆ [檢視您的角色定義](#)，第 213 頁
- ◆ [建立政策和篩選器](#)，第 214 頁
- ◆ [將政策套用至用戶端](#)，第 216 頁

「超級管理員」可將受管理的用戶端指派給角色，而委派管理員必須將它們加到「用戶端」頁面後才能套用政策。如需指示，請參閱[新增用戶端](#)，第 61 頁。

將用戶端新增到角色的受管理用戶端清單之後，它們便可立即由該角色的「預設」政策篩選。從「超級管理員」的「用戶端」頁面移到角色的用戶端是由「超級管理員」套用的政策來管理，這些政策是在移動用戶端時複製到角色。

「委派管理」>「編輯角色」頁面所列示的屬於您角色的任何用戶端均可新增到「用戶端」頁面並為其指派政策。您也可以新增屬於指派為您角色中受管理用戶端(群組、網域、組織單位或網路範圍)之成員的個別使用者或電腦。

由於使用者可能屬於多個群組、網域或組織單位，若不同的角色管理包含共同成員的群組、網域或組織單位，新增來自比較大之用戶端群組的個人可能會產生衝突。如果不同角色中的管理員同時存取 **Websense Manager**，他們有可能會將同一用戶端(例如群組的個別成員)新增到他們的「用戶端」頁面。在此情況下，該用戶端的網際網路篩選將由替每個角色建立的優先順序決定。請參閱[管理角色衝突](#)，第 226 頁。

## 建立政策和篩選器

### 相關主題

- ◆ [委派管理員工作](#)，第 212 頁
- ◆ [檢視您的使用者帳戶](#)，第 213 頁
- ◆ [檢視您的角色定義](#)，第 213 頁
- ◆ [新增用戶端到「用戶端」頁面](#)，第 214 頁
- ◆ [將政策套用至用戶端](#)，第 216 頁

建立角色時，它會自動繼承在當時定義之預先安裝的「預設」政策、類別篩選器和通訊協定篩選器。「超級管理員」也可能選擇一些政策和篩選器，將其複製到您的角色。

除了政策和篩選器之外，您將同時繼承「超級管理員」所建立的任何自訂檔案類型和通訊協定。

您可以編輯繼承自「超級管理員」的政策和篩選器。您所做的變更只會影響您的角色。「超級管理員」對您先前繼承的政策和篩選器所做的任何變更並不會影響您的角色。



#### 注意

「超級管理員」對自訂檔案類型和通訊協定所做的變更會自動影響您角色中的篩選器和政策。

當您的「超級管理員」通知您這些元件有所變更之後，請檢閱您的篩選器和政策，確認它們得到正確處理。

您也可以根據需要，建立不限數目的新篩選器和政策。委派管理員所建立的篩選器和政策只供登入您角色的管理員使用。如需建立政策的指示，請參閱[使用政策](#)，第 67 頁。如需建立篩選器的指示，請參閱[使用篩選器](#)，第 42 頁。

您可以編輯您角色的篩選器元件，但是有一些限制。

- ◆ **類別**：新增自訂類別以及編輯 Master Database 和自訂類別，以定義角色內所使用的已重新分類 URL 和關鍵字；變更在其建立的類別篩選器中預設套用的動作和進階篩選選項（對類別的預設動作所做的變更只有當類別未由「篩選器鎖定」鎖定時才會執行）。
- ◆ **通訊協定**：變更在其建立的通訊協定篩選器中預設套用的動作和進階篩選選項（對通訊協定的預設動作所做的變更只有當通訊協定未由「篩選器鎖定」鎖定時才會執行）。委派管理員無法新增或刪除通訊協定定義。
- ◆ **檔案類型**：檢視指派給每個檔案類型的副檔名。委派管理員無法新增檔案類型或變更指派給檔案類型的副檔名。
- ◆ **未篩選的 URL**：新增 URL 並新增代表網站只允許角色中所有受管理的用戶端存取的正規表示式。

如需詳細資訊請，參閱[建立篩選器元件](#)，第 151 頁。

如果「超級管理員」已執行「篩選器鎖定」限制，則可能會有一些類別或通訊協定會自動被封鎖，而且無法在您建立及編輯的篩選器中變更。請參閱[定義所有角色的篩選限制](#)，第 229 頁。

## 將政策套用至用戶端

### 相關主題

- ◆ [委派管理員工作](#)，第 212 頁
- ◆ [檢視您的使用者帳戶](#)，第 213 頁
- ◆ [檢視您的角色定義](#)，第 213 頁
- ◆ [新增用戶端到「用戶端」頁面](#)，第 214 頁
- ◆ [建立政策和篩選器](#)，第 214 頁

建立政策之後，您可以按一下**套用至用戶端**按鈕，直接將該政策套用到已新增至「用戶端」頁面的用戶端。請參閱[將政策指派到用戶端](#)，第 70 頁。

或者，您可以前往「用戶端」頁面，新增應該由此政策管理的用戶端。請參閱[使用用戶端](#)，第 54 頁。

## 產生報告

如果您有報告權限，則由「超級管理員」設定可以使用的具體報告選項。若要瞭解您可以使用的功能，請前往「委派管理」頁面，然後按一下角色名稱。「編輯角色」頁面中就會顯示您有權使用的報告功能。如需詳細資訊，請參閱[編輯角色](#)，第 221 頁。

## 啓用 Websense Manager 的存取權限

設定委派管理角色時，您需要決定管理員所能存取的 Websense Manager 功能。爲了確保登入 Websense Manager 的個人可使用適當的功能，每一位人員均必須以使用者名稱和密碼登入。可使用的帳戶有兩種類型：

- ◆ **網路帳戶**：使用已在您網路目錄服務中建立的認證（請參閱[目錄帳戶](#)，第 216 頁）。
- ◆ **Websense 使用者帳戶**：供您建立專門用於 Websense Manager 的使用者名稱和密碼（請參閱[Websense 使用者帳戶](#)，第 218 頁）。

## 目錄帳戶

### 相關主題

- ◆ [啓用 Websense Manager 的存取權限](#)，第 216 頁
- ◆ [Websense 使用者帳戶](#)，第 218 頁



無條件「超級管理員」可以使用**設定 > 一般 > 登入目錄**頁面，輸入所需的目錄服務資訊，以便管理員能夠使用他們的網路認證登入 Websense Manager。



### 注意

這項資訊只用於驗證 Websense Manager 使用者，不會套用至篩選用戶端。用戶端目錄服務資訊在「設定」>「目錄服務」頁面中設定 (請參閱[目錄服務](#)，第 56 頁)。

系統會針對單一目錄服務驗證 Websense Manager 使用者的網路認證。如果您的網路包含多項目錄服務，您在 Websense Manager 設定的「登入目錄」服務和其他目錄服務之間必須存在信任關係。

如果無法定義搭配 Websense Manager 使用的單一目錄服務，請考慮替管理員建立 Websense 使用者帳戶 (請參閱[Websense 使用者帳戶](#)，第 218 頁)。

若要定義供 Websense Manager 用來驗證管理員的目錄服務，請先檢查使用目錄服務來驗證管理員的方塊是否已核取，然後從清單中選取**目錄服務**類型。

如果您選擇 **Windows NT Directory / Active Directory (混合模式)** 這個預設值，則不需要做進一步的設定。按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。

如果您選取 **Active Directory (原生模式)** 或其他 **LDAP 目錄**，請提供下列的額外資訊

1. 輸入安裝目錄服務之機器的 IP 位址或名稱。
  - 如果您使用「Active Directory (原生模式)」並且已設定用於容錯移轉的全域目錄伺服器，那麼您可以輸入 DNS 網域名稱。
2. 輸入用於目錄服務通訊的**連接埠**。
3. 若要加密目錄服務通訊，請選擇**使用 SSL**。
4. 輸入 Websense 軟體用以連接至目錄服務的**使用者識別名稱**和**密碼**。
5. 輸入 Websense 軟體驗證管理員時所使用的**預設網域內容**。
  - 如果您使用「Active Directory (原生模式)」那麼配置就已完成。按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。
  - 如果您使用其他以 LDAP 為基礎的目錄服務，請繼續。
6. 提供的**使用者登入 ID 屬性**和**使用者搜尋篩選器** (如果有) Websense 軟體可將其用來加速使用者驗證。  
**設定 > 目錄服務**頁面的**進階目錄設定**下也會顯示這項資訊。如果有需要，您可以複製並貼上值。
7. 在「群組選項」下，指定您的 LDAP 綱要是否包括 **memberOf** 屬性：
  - 若未使用 **memberOf**指定 Websense 軟體驗證管理員時應該要套用的**使用者群組搜尋篩選器**。
  - 如果使用 **memberOf**指定應該要套用的**群組屬性**。
8. 如果您的 LDAP 綱要包括巢狀群組，請選擇執行額外的**巢狀群組搜尋**。

9. 如果您的目錄服使用 LDAP 參照，請指定 Websense 軟體是應該使用或忽略參照。
10. 按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## Websense 使用者帳戶

### 相關主題

- ◆ [啟用 Websense Manager 的存取權限](#)，第 216 頁
- ◆ [新增 Websense 使用者帳戶](#)，第 218 頁

「超級管理員」可使用 **委派管理 > 管理 Websense 使用者帳戶** 頁面，建立讓管理員不需要輸入網路目錄認證即可存取 Websense Manager 的帳戶。「超級管理員」也可以在此頁面變更 Websense 使用者帳戶的密碼，以及檢視 Websense 使用者被指派為其管理員的角色。

無條件「超級管理員」也可以使用此頁面來刪除 Websense 使用者帳戶。

委派管理員可使用此頁面來變更他們的 Websense 密碼，以及檢視他們被指派為其管理員的角色。

選項	說明
新增	開啓用於建立新 Websense 使用者帳戶的頁面。請參閱 <a href="#">新增 Websense 使用者帳戶</a> ，第 218 頁。
變更密碼	開啓用於變更相關帳戶之密碼的頁面。請參閱 <a href="#">變更 Websense 使用者的密碼</a> ，第 219 頁。
檢視	顯示此使用者被指派為其管理員的角色清單。
刪除	核取一或多個已過時之使用者帳戶的核取方塊，然後按一下此按鈕將它們刪除。
關閉	返回「委派管理」頁面。

## 新增 Websense 使用者帳戶

### 相關主題

- ◆ [啟用 Websense Manager 的存取權限](#)，第 216 頁
- ◆ [Websense 使用者帳戶](#)，第 218 頁
- ◆ [變更 Websense 使用者的密碼](#)，第 219 頁

使用委派管理 > 管理 Websense 使用者帳戶 > 新增 Websense 使用者頁面來新增 Websense 使用者帳戶。

- 輸入最多 50 個字元的唯一**使用者名稱**。  
名稱長度必須介於 1 到 50 個字元之間，且不能包含下列任何字元：  
\* < > ' { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,  
使用者名稱可以包含空格和橫線。
- 輸入並確認此使用者的**密碼** (4-255 個字元)。  
建議使用強式密碼：長度為 8 個字元或更長，且其中至少各包含一個下列項目：
  - 大寫字母
  - 小寫字母
  - 數字
  - 特殊字元 (例如連字號、底線或空格)
- 完成變更後，按一下**確定**來快取變更並返回「管理 Websense 使用者帳戶」頁面。按一下**全部儲存**才能使變更生效。

## 變更 Websense 使用者的密碼

### 相關主題

- ◆ [啟用 Websense Manager 的存取權限](#)，第 216 頁
- ◆ [Websense 使用者帳戶](#)，第 218 頁
- ◆ [新增 Websense 使用者帳戶](#)，第 218 頁

委派管理員可以使用委派管理 > 管理 Websense 使用者帳戶 > 變更密碼頁面來變更他們自己之 Websense 使用者帳戶的密碼。「超級管理員」則可以使用此頁面來變更任何 Websense 使用者帳戶的密碼。

- 驗證頁面最上方顯示的**使用者名稱**是否正確。
- 輸入並確認此使用者的新**密碼** (4-255 個字元)。  
建議使用強式密碼長度為 8 個字元或更長且其中至少各包含一個下列項目
  - 大寫字母
  - 小寫字母
  - 數字
  - 特殊字元 (例如連字號、底線或空格)
- 完成變更後按一下**確定**來快取變更並返回「管理 Websense 使用者帳戶」頁面。按一下**全部儲存**才能使變更生效。

## 使用委派管理

### 相關主題

- ◆ [管理角色簡介](#)，第 206 頁
- ◆ [管理角色衝突](#)，第 226 頁

**政策管理 > 委派管理** 頁面提供的選項會根據檢視者是「超級管理員」或委派管理員而有所不同。

「超級管理員」會見到一份目前定義之所有角色的清單，其中有下列選項。

選項	說明
新增	按一下即可新增新的角色。請參閱 <a href="#">新增角色</a> ，第 221 頁。
角色	按一下即可檢視或設定角色。請參閱 <a href="#">編輯角色</a> ，第 221 頁。
刪除	按一下即可刪除清單中標記的任何角色。此選項只有無條件「超級管理員」可以使用。 如需有關角色被刪除後如何管理角色之用戶端的資訊，請參閱 <a href="#">特殊考量</a> ，第 227 頁。
進階	按一下即可存取「管理角色優先順序」功能。
管理角色優先順序	按一下即可指定若由不同角色管理的多個群組中有相同的用戶端存在時，應該使用哪一個角色的政策設定。請參閱 <a href="#">管理角色衝突</a> ，第 226 頁。
管理 Websense 使用者帳戶	按一下即可新增、編輯及刪除只用於存取 Websense Manager 之帳戶的使用者名稱和密碼。請參閱 <a href="#">Websense 使用者帳戶</a> ，第 218 頁。
管理自訂 LDAP 群組	按一下即可新增、編輯及刪除可指派為委派管理角色中之受管理用戶端的自訂 LDAP 群組。請參閱 <a href="#">使用自訂 LDAP 群組</a> ，第 60 頁。 若設定的目錄服務為「Windows NT/Active Directory (混合模式)」則無法使用此選項。

委派管理員只能看到他們為管理員的角色，而且可以存取的選項更加有限。

選項	說明
角色	按一下即可檢視指派給角色的用戶端，以及授予的具體報告權限。請參閱 <a href="#">編輯角色</a> ，第 221 頁。
管理 Websense 使用者帳戶	按一下即可存取用以變更您的 Websense Manager 密碼以及檢視指派給您的角色的選項。請參閱 <a href="#">Websense 使用者帳戶</a> ，第 218 頁。

## 新增角色

### 相關主題

- ◆ [編輯角色](#)，第 221 頁
- ◆ [特殊考量](#)，第 227 頁

您可以使用[委派管理](#) > [新增角色](#)頁面，提供新角色的名稱和說明。

1. 輸入新角色的**名稱**。

名稱長度必須介於 1 到 50 個字元之間，且不能包含下列任何字元

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

角色名稱可以包含空格和橫線。

2. 輸入新角色的**說明**。

說明最長為 255 個字元。適用於角色名稱的字元限制也適用於說明，但有 2 個例外：說明可包含句點 (.) 和逗號 (,)。

3. 按一下**確定**來顯示[編輯角色](#)頁面，然後定義此角色的特性。請參閱[編輯角色](#)，第 221 頁。

下次您登入 Websense Manager 時，新的角色就會加到標題的「角色」下拉式清單中。

## 編輯角色

### 相關主題：

- ◆ [使用委派管理](#)，第 220 頁
- ◆ [新增角色](#)，第 221 頁
- ◆ [管理角色衝突](#)，第 226 頁

委派管理員可以使用[委派管理](#) > [編輯角色](#)頁面，檢視受他們的角色管理的用戶端以及授予的具體報告權限。

「超級管理員」可以使用此頁面來選取角色的管理員和用戶端，以及設定管理員權限，如下所述。只有無條件「超級管理員」才可以刪除角色的管理員和用戶端。

1. 視需要變更角色**名稱**和**說明**。



### 注意

「超級管理員」角色的名稱無法變更。

2. 新增及刪除此角色的管理員 (只有「超級管理員」可以執行如果您以委派管理員身份登入，就不會顯示此部分)。

項目	說明
使用者名稱	管理員的使用者名稱。
帳戶類型	指示使用者是定義於網路目錄服務 (目錄) 或定義為 Websense 使用者帳戶 (Websense)。
報告	若核取此核取方塊即可授予管理員使用報告工具的權限。
政策	若核取此核取方塊，即可授予管理員建立篩選器和政策，以及將政策套用到角色的受管理用戶端的權限。 在「超級管理員」角色中，擁有政策權限的管理員也可以管理特定的 Websense 配置設定。請參閱 <a href="#">超級管理員</a> ，第 207 頁。
無條件	僅適用於「超級管理員」角色，若核取此核取方塊，即可授予管理員管理所有 Websense 配置設定以及「篩選器鎖定」的權限。 只有無條件「超級管理員」可以將無條件權限授予新的管理員。
新增	開啓 <a href="#">新增管理員</a> 頁面。請參閱 <a href="#">新增管理員</a> ，第 224 頁。
刪除	將「管理員」清單中標記的所有管理員自角色中移除 (只有無條件「超級管理員」才可執行)。

3. 新增及刪除角色的受管理的用戶端 (只有「超級管理員」才能夠進行變更。委派管理員可以檢視指派給他們之角色的用戶端)。

項目	說明
<名稱>	顯示明確指派給角色之每個用戶端的名稱。角色中的管理員必須將用戶端加到「用戶端」頁面後才可以套用政策。請參閱 <a href="#">委派管理員工作</a> ，第 212 頁。
新增	開啓 <a href="#">新增受管理的用戶端</a> 頁面。請參閱 <a href="#">新增受管理的用戶端</a> ，第 225 頁。
刪除	此按鈕只有無條件「超級管理員」可以使用它可將受管理的用戶端清單中標記的所有用戶端自角色移除。 有些用戶端無法直接從受管理的用戶端清單中刪除。如需詳細資訊，請參閱 <a href="#">特殊考量</a> ，第 227 頁。

4. 使用**報告權限**區域，選取此角色中具有報告存取權限之管理員可以使用的功能。

## a. 選擇一般層級的報告權限

選項	說明
所有用戶端的報告	選取此選項即可授與管理員產生所有網路使用者之報告的權限。 使用「報告權限」區域中其餘的選項，設定此角色中管理員的具體權限。
僅有受管理用戶端的報告	選取此選項即可限制管理員，使其只能執行指派給此角色之受管理用戶端的報告。然後，選取這些管理員可以存取的調查報告功能。 只能執行受管理用戶端之報告的管理員無法存取「今天」和「記錄」頁面中的簡報報告或以使用者為基礎的報告。他們也無法管理記錄資料庫設定。

## b. 核取允許角色中適當管理員使用之每一項報告功能的核取方塊。

選項	說明
存取簡報報告	啟用存取簡報報告功能。此選項只有在管理員可以執行所有用戶端的報告時才能夠使用。請參閱 <a href="#">簡報報告</a> ，第 86 頁。
檢視「今天」與「記錄」頁面的報告	啟用在這些頁面中顯示網際網路活動的圖表。請參閱 <a href="#">今天：自午夜算起的健全度、安全性及數值</a> ，第 21 頁和 <a href="#">記錄：最後 30 天</a> ，第 23 頁。 若取消選取此選項，管理員只能檢視「今天」頁面的「健全度警示」和「值」區域以及「記錄」頁面中的「估計值」。
存取調查報告	啟用存取基本調查報告功能。選取此選項時，也可以選取其他調查報告功能。請參閱 <a href="#">調查報告</a> ，第 102 頁。
檢視調查報告中的使用者名稱	如果此角色中的管理員登入，讓他們可以檢視使用者名稱。請參閱 <a href="#">設定用於記錄的 Filtering Service</a> ，第 265 頁。 若取消選取此選項，則只會顯示系統產生的識別代碼，而非名稱。 此選項只有在管理員被授予調查報告存取權限時才能夠使用。
將調查報告儲存為我的最愛	讓此角色中的管理員可以建立我的最愛調查報告。請參閱 <a href="#">我的最愛調查報告</a> ，第 118 頁。 此選項只有在管理員被授予調查報告存取權限時才能夠使用。

選項	說明
排程調查報告	讓此角色中的管理員可以將調查報告排程於未來的時間執行或重複執行。 請參閱 <a href="#">排程調查報告</a> ，第 120 頁。 此選項只有在管理員可以將調查報告儲存到我的最愛時才能夠使用。
管理記錄資料庫	讓管理員可以存取「設定」>「記錄資料庫」頁面。請參閱 <a href="#">記錄資料庫管理設定</a> ，第 279 頁。 此選項只有在管理員可以執行所有用戶端的報告時才能夠使用。

5. 完成變更後，按一下**確定**來快取變更並返回「委派管理」頁面。按一下**全部儲存**才能使變更生效。

## 新增管理員

相關主題：

- ◆ [編輯角色](#)，第 221 頁
- ◆ [啟用 Websense Manager 的存取權限](#)，第 216 頁

「超級管理員」可以使用[委派管理](#) > [編輯角色](#) > [新增管理員](#)頁面，將個人指定為角色的管理員。



### 注意

管理員可以新增到多個角色。這些管理員在登入時必須選擇一個角色。在此情況下，管理員具有所有角色的結合報告權限。

委派的管理員對他們所管理之用戶端的網際網路活動具有很大的控制權。為了確保能夠負責地實行這項控制並使其符合您組織可接受的使用政策，「超級管理員」應該使用「稽核記錄」頁面來監督管理員所做的變更。請參閱[檢視並匯出稽核記錄](#)，第 244 頁。

1. 如果您計畫新增目錄帳戶做為委派管理員，請確定登入其「目錄服務」配置 (請參閱[目錄服務](#)，第 56 頁) 與「登入目錄」配置 (請參閱[目錄帳戶](#)，第 216 頁) 相符合的 Policy Server。

如果您只新增 Websense 使用者帳戶做為管理員，那麼您可以登入任何 Policy Server。

2. 在[目錄帳戶](#)下，核取一或多個使用者的核取方塊，然後按一下向右箭頭 (>) 按鈕，將他們移到已選取清單中。



### 注意

自訂 LDAP 群組不能新增為管理員。



如果您的環境使用「Active Directory (原生模式)」或其他以 LDAP 為基礎的目錄服務，您就可以搜尋目錄來尋找特定使用者、群組、網域或組織單位名稱。請參閱[搜尋目錄服務](#)，第 62 頁。

3. 在 **Websense 帳戶** 下，核取一或多個使用者的核取方塊，然後按一下向右箭頭按鈕，將反白顯示的使用者移到**已選取**清單中。
4. 為此角色中的管理員設定**權限**。

選項	說明
政策	若核取此選項，即可讓此角色中的管理員套用政策到他們所管理的用戶端。這同時會授予存取特定 Websense 配置設定的權限。
無條件	若核取此選項可授予存取所有 Websense 配置設定的權限。 此選項只有當無條件「超級管理員」將管理員新增到擁有政策權限的「超級管理員」角色時才能夠使用。
報告	核取此選項可授予存取報告工具的權限。使用「編輯角色」頁面，以設定允許使用的特定報告功能。

5. 完成變更後，按一下**確定**以返回「編輯角色」頁面。
6. 按一下「編輯角色」頁面中的**確定**來快取您所做的變更。按一下**全部儲存**才能使變更生效。

## 新增受管理的用戶端

相關主題：

- ◆ [使用委派管理](#)，第 220 頁
- ◆ [編輯角色](#)，第 221 頁

受管理的用戶端指的是指派給角色的使用者和電腦，它們的政策由角色的管理員設定。目錄用戶端（使用者、群組、網域和組織單位）、電腦和網路全部都可定義為受管理的用戶端。

「超級管理員」可以使用[委派管理 > 編輯角色 > 新增受管理的用戶端](#)頁面，根據需要新增不限數目的用戶端到角色。每個用戶端只能指派給一個角色。

如果您將網路範圍指派為一個角色的受管理的用戶端，就不能將該範圍內的個別 IP 位址指派給其他角色。除此以外，您也不能特別將某個使用者、群組、網域或組織單位指派給 2 個不同的角色。不過，您可以將某個使用者指派給一個角色，然後將使用者屬於其成員的群組、網域或組織單位指派給不同的角色。



### 注意

如果某個群組是一個角色中的受管理用戶端，且該角色的管理員套用政策到群組的每個成員，則不能於稍後將該群組中的個別使用者指派給其他角色。

新增受管理的用戶端時，請考慮要包括哪些用戶端類型。如果您新增 IP 位址到某個角色，該角色的管理員便可執行指定機器的**所有**活動的報告。如果您新增使用者到某個角色，管理員便可執行這些使用者之**所有**活動的報告，而不論發生活動的機器為何。

系統不會自動將管理員包含為他們管理之角色中受管理的用戶端，因為這會讓他們設定自己的政策。若要讓管理員能夠檢視他們自己的網際網路使用狀況，請啟動自行報告 (請參閱 [自行報告](#)，第 291 頁)。

如果您的組織已部署多個 Policy Server 且這些 Policy Server 與不同的目錄通訊，請確定選取連接至特定目錄的 Policy Server 該目錄中包含您想新增的用戶端。



#### 注意

最佳作法是讓同一個角色中的所有受管理用戶端來自相同的目錄服務。

#### 1. 選取角色的用戶端：

- 在**目錄**下，核取一或多個使用者的核取方塊。  
如果您的環境使用「Active Directory (原生模式)」或其他以 LDAP 為基礎的目錄服務，您就可以搜尋目錄來尋找特定使用者、群組、網域或組織單位名稱。請參閱 [搜尋目錄服務](#)，第 62 頁。
  - 在**電腦**下，輸入要新增到此角色之電腦的 IP 位址。
  - 在**網路**下，輸入要新增為單位之電腦範圍的第一個和最後一個 IP 位址。
2. 按一下用戶端類型旁邊的向右箭頭 (>) 按鈕，將用戶端移到**已選取**清單中。
  3. 完成變更後，按一下**確定**以返回「編輯角色」頁面。
  4. 按一下「編輯角色」頁面中的**確定**來快取您所做的變更。按一下**全部儲存**才能使變更生效。

## 管理角色衝突

相關主題：

- ◆ [使用委派管理](#)，第 220 頁
- ◆ [新增受管理的用戶端](#)，第 225 頁

目錄服務讓同一個使用者可以隸屬多個群組。因此，單一使用者可存在於由不同委派管理角色管理的群組中。網域和組織單位也存在相同的情況。

此外，使用者也可能受一個角色管理，但屬於受其他角色管理的群組、網域或組織單位。如果這些角色的管理員同時登入，在負責管理群組的管理員套用政策到群組的個別成員時，負責管理使用者的管理員可能同時套用政策到該使用者。

您可以使用 **委派管理 > 角色優先順序** 頁面告知 Websense 軟體若因重疊關係而將不同的政策套用到同一使用者時，應該要如何處理。發生衝突時，Websense 軟體會套用此清單中優先順序最高之角色的篩選政策。

1. 選取清單中除「超級管理員」以外的任一個角色。

**注意**

「超級管理員」角色始終是此清單中的第一個項目，而且無法移動。

2. 按一下**上移**或**下移**來變更它在清單中的位置。
3. 重複步驟 1 和步驟 2 直到所有角色都具有所需的優先順序為止。
4. 完成變更後，按一下**確定**來快取變更並返回「委派管理」頁面。按一下**全部儲存**才能使變更生效。

## 特殊考量

**相關主題**

- ◆ [使用委派管理](#)，第 220 頁
- ◆ [編輯角色](#)，第 221 頁

刪除委派管理角色或刪除角色的受管理用戶端之前，請先檢閱下列資訊。

### 刪除角色

在**委派管理**頁面中，無條件「超級管理員」可將任何已過時的角色加以刪除。

刪除角色時，會同時將該角色的管理員新增到「用戶端」頁面中的所有用戶端移除。角色刪除之後，若那些用戶端屬於受其他角色管理的網路、群組或網域的話，它們將由套用於那些角色的適當政策管理（請參閱[篩選順序](#)，第 71 頁）。否則，它們將由「超級管理員」的「預設」政策管理。

1. 在**委派管理**頁面中，核取要刪除之角色旁邊的核取方塊。

**注意**

您無法刪除「超級管理員」角色。

2. 按一下**刪除**。
3. 確認刪除要求，以將選取的角色自「委派管理」頁面移除。按一下**全部儲存**才能使變更生效。

下次您登入 Websense Manager 時已刪除的角色就會從標題的「角色」下拉式清單中清除。

## 刪除受管理的用戶端

下列任一情況存在時，無法直接將用戶端從受管理的用戶端清單刪除（「委派管理」>「編輯角色」）

- ◆ 管理員已套用政策至用戶端
- ◆ 管理員已套用政策至網路、群組、網域或組織單位的一或多個成員

若「超級管理員」在登入 Websense Manager 時，選擇不是與包含要刪除之用戶端的目錄服務通訊的 Policy Server 也可能會發生問題。在此情況下，目前的 Policy Server 和目錄服務將無法辨識用戶端。

無條件「超級管理員」可確保能夠刪除適當的用戶端，如下所述。

1. 登入 Websense Manager 選取其目錄服務包含要刪除之受管理用戶端的 Policy Server。您必須使用無條件「超級管理員」權限登入。
2. 開啟標題中的**角色**清單，然後選取要從中刪除受管理用戶端的角色。
3. 前往**政策管理 > 用戶端**，檢視委派管理員已明確指派政策的用戶端清單。  
這可能包括角色的受管理用戶端清單中特別指定的用戶端，以及屬於受管理用戶端清單中網路、群組、網域或組織單位之成員的用戶端。
4. 刪除適當的用戶端。
5. 按一下**確定**來快取變更。
6. 開啟標題中的**角色**清單，然後選取**超級管理員**角色。
7. 前往**政策管理 > 委派管理 > 編輯角色**。
8. 將適當的用戶端自受管理的用戶端清單中刪除，然後按一下**確定**以確認刪除要求。
9. 按一下「編輯角色」頁面中的**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## 多個存取 Websense Manager 的管理員

相關主題：

- ◆ [管理員簡介，第 206 頁](#)
- ◆ [啟用 Websense Manager 的存取權限，第 216 頁](#)

不同角色中的管理員可以同時存取 Websense Manager 以執行他們的角色權限所允許的任何活動。例如，角色 A 和角色 B 都具有政策權限，其中的管理員可能同時登入 Websense Manager。因為他們管理不同的用戶端，所以他們可以建立並套用政策，而且不會發生衝突。

如果同一個角色中具有政策權限的多個管理員同時登入，情況就有所不同。爲了維持政策結構和指派項目的完整性，一次只允許某個角色的一位管理員使用政策權限存取 **Websense Manager**。若同一個角色中具有政策權限的第二位管理員嘗試在第一位管理員尚未登出時登入，系統將會提示第二位管理員做選擇。

- ◆ 只登入執行報告 (如果管理員擁有報告權限)。
- ◆ 登入其他角色 (如果管理員被指派給其他角色)。
- ◆ 在第一位管理員登出後再嘗試。

當同時具有政策與報告權限的多個管理員登入以產生報告時，他們應該要立即釋放其政策權限，讓角色中的其他管理員可以執行政策管理活動。

- ▶ 前往標題中的**角色**下拉式清單，然後選擇**釋放政策權限**。

另一個方法是替每個角色建立特別的 **Websense** 使用者帳戶 (請參閱 [Websense 使用者帳戶](#)，第 218 頁)，然後只將報告權限授予該使用者。提供登入認證 (使用者名稱和密碼) 給角色中同時具有政策與報告權限的管理員。當管理員需要執行報告時，他們可以以此報告管理員身份登入，讓其他管理員可以存取政策。

## 定義所有角色的篩選限制

相關主題：

- ◆ [管理員簡介](#)，第 206 頁
- ◆ [建立「篩選器鎖定」](#)，第 230 頁

**Websense** 軟體讓無條件「超級管理員」能夠建立「篩選器鎖定」，它可針對受委派管理角色管理之所有用戶端封鎖類別和通訊協定。如需詳細資訊，請參閱 [建立「篩選器鎖定」](#)，第 230 頁。

這些角色的管理員可以套用任何篩選動作到他們政策中的其他類別和通訊協定，但是「篩選器鎖定」中封鎖的那些類別和通訊協定除外。

儲存對「篩選器鎖定」所做的變更之後，就會立即在所有受管理的用戶端生效。當變更生效時，正在使用 **Websense Manager** 的委派管理員將不會在他們的篩選器見到變更，直到下次登入時才會見到。



### 注意

將某個篩選器從「超級管理員」角色複製到另一個角色時，複本會繼承「篩選器鎖定」的限制。

「超級管理員」並不會受到「篩選器鎖定」的限制。他們可以定義政策，該政策允許存取已針對委派管理角色封鎖並鎖定之類別和通訊協定。因此，需要特別存取權的個人應該受「超級管理員」角色管理。

## 建立「篩選器鎖定」

### 相關主題

- ◆ [定義所有角色的篩選限制](#)，第 229 頁
- ◆ [鎖定類別](#)，第 230 頁
- ◆ [鎖定通訊協定](#)，第 231 頁

您可以在**政策管理 > 篩選器鎖定**頁面，選擇是否編輯針對委派管理角色中之所有受管理用戶端封鎖的類別或通訊協定。「篩選器鎖定」中封鎖的任何類別或通訊協定功能都被視為**已封鎖且已鎖定**。

- ◆ 按一下**類別**按鈕即可封鎖並鎖定特定類別或類別元素 (關鍵字和檔案類型)。請參閱[鎖定類別](#)，第 230 頁。
- ◆ 按一下**通訊協定**按鈕即可封鎖並鎖定通訊協定或通訊協定記錄。請參閱[鎖定通訊協定](#)，第 231 頁。

## 鎖定類別

### 相關主題

- ◆ [定義所有角色的篩選限制](#)，第 229 頁
- ◆ [建立「篩選器鎖定」](#)，第 230 頁
- ◆ [鎖定通訊協定](#)，第 231 頁

使用**政策管理 > 篩選器鎖定 > 類別**頁面，選取要針對委派管理角色的所有成員封鎖並鎖定的類別。您也可以封鎖並鎖定某個類別的關鍵字和檔案類型。

1. 在樹狀結構中選取類別。  
委派管理角色無法存取「超級管理員」所建立的自訂類別。因此，此樹狀結構中不會顯示自訂類別。
2. 在類別樹狀結構旁邊的方塊中設定此類別的限制。

選項	說明
鎖定類別	封鎖並鎖定對此類別中網站的存取。
鎖定關鍵字	根據替每個角色中的這個類別定義的關鍵字封鎖並鎖定存取。

選項	說明
鎖定檔案類型	封鎖並鎖定為此類別中網站的已選檔案類型。 請確定核取每個要封鎖並鎖定之檔案類型的核取方塊。 此清單中包括「超級管理員」所建立的自訂檔案類型，因為委派管理角色可以使用這些檔案類型。
套用至下層類別	對此類別的所有下層類別套用相同的設定。

如果適用，您可以一次封鎖並鎖定所有類別的已選元素。在樹狀結構中選取**所有類別**，然後選取要針對所有類別封鎖的元素。然後，按一下**套用至下層類別**。

- 完成變更後，按一下**確定**來快取變更並返回「篩選器鎖定」頁面。按一下**全部儲存**才能使變更生效。

## 鎖定通訊協定

### 相關主題

- ◆ [定義所有角色的篩選限制](#)，第 229 頁
- ◆ [建立「篩選器鎖定」](#)，第 230 頁
- ◆ [鎖定類別](#)，第 230 頁

您可以使用**政策管理 > 篩選器鎖定 > 通訊協定**頁面，針對受委派管理角色管理的所有用戶端，封鎖並鎖定存取所選的通訊協定，或者鎖定它的記錄。



### 注意

通訊協定記錄與通訊協定使用警示有關。若要能夠產生通訊協定的使用警示，您至少必須在一個通訊協定篩選器中設定記錄。透過「篩選器鎖定」啓用**鎖定通訊協定記錄**選項，可確保能夠產生通訊協定的使用警示。請參閱[設定通訊協定使用警示](#)，第 251 頁。

- 在樹狀結構中選取通訊協定。  
委派管理角色可以存取「超級管理員」所建立的自訂通訊協定。因此，此樹狀結構中會顯示自訂通訊協定。
- 在通訊協定樹狀結構旁邊的方塊中設定此通訊協定的限制。

選項	說明
鎖定通訊協定	封鎖並鎖定使用此通訊協定對應用程式和網站進行的存取。

選項	說明
鎖定通訊協定記錄	記錄與存取此通訊協定有關的資訊，並且禁止委派管理員停用記錄。
套用至群組	對群組中的所有通訊協定套用相同的設定。

3. 完成變更後，按一下**確定**來快取變更並返回「篩選器鎖定」頁面。按一下**全部儲存**才能使變更生效。



# 12

## Websense Server 管理

相關主題：

- ◆ [Websense 產品元件](#)，第 234 頁
- ◆ [使用 Policy Server](#)，第 239 頁
- ◆ [檢視並匯出稽核記錄](#)，第 244 頁
- ◆ [停止和啓動 Websense 服務](#)，第 245 頁
- ◆ [警示](#)，第 246 頁
- ◆ [備份與還原 Websense 資料](#)，第 253 頁

網際網路使用篩選需要在幾個 Websense 軟體元件之間進行互動：

- ◆ 由 Network Agent 或協力廠商整合產品收到使用者的網際網路存取要求。
- ◆ 要求被傳送至 Websense Filtering Service 進行處理。
- ◆ Filtering Service 與 Policy Server 和 Policy Broker 通訊，以套用適當的政策來回應要求。

在大多數環境中，不論環境中有一個或是多個 Policy Server，皆使用一個 Policy Database 來保存用戶端、篩選器、政策和一般配置資訊。

Websense Manager 的每個實例都與一個 Policy Database 關聯，並且實例可用於設定與該資料庫關聯的每個 Policy Server。

由於在 Websense Manager 中所執行的政策設定是儲存在中央資料庫中，因此政策資訊自動用於所有與該 Policy Database 關聯的 Policy Server。

## Websense 產品元件

---

相關主題：

- ◆ [篩選元件](#)，第 235 頁
- ◆ [報告元件](#)，第 237 頁
- ◆ [使用者識別元件](#)，第 237 頁
- ◆ [使用 Policy Server](#)，第 239 頁
- ◆ [停止和啓動 Websense 服務](#)，第 245 頁
- ◆ [檢閱目前的系統狀態](#)，第 252 頁

Websense 軟體由數個元件組成，這些元件共同運作以提供使用者識別、網際網路篩選和報告功能。本節提供每個元件的概覽，以協助您瞭解並管理篩選環境。

主要的 Websense 元件包括：

- ◆ Policy Database
- ◆ Policy Broker
- ◆ Policy Server
- ◆ Filtering Service
- ◆ Network Agent
- ◆ Master Database
- ◆ Websense Manager
- ◆ Usage Monitor
- ◆ User Service
- ◆ Log Server
- ◆ Log Database

Websense 軟體還包含選用的無障礙識別代理程式：

- ◆ DC Agent
- ◆ RADIUS Agent
- ◆ eDirectory Agent
- ◆ Logon Agent

其他選用元件包括：

- ◆ Remote Filtering Server
- ◆ Remote Filtering Client
- ◆ Websense Content Gateway

## 篩選元件

元件	說明
<b>Policy Database</b>	儲存 Websense 軟體設定與政策資訊。
<b>Policy Broker</b>	管理來自 Websense 元件的政策與一般配置資訊要求。
<b>Policy Server</b>	<ul style="list-style-type: none"> <li>識別及追蹤其他 Websense 元件的位置和狀態。</li> <li>儲存單一 Policy Server 實例特有的配置資訊。</li> <li>將配置資料傳送給 Filtering Service，以用於篩選網際網路要求。</li> </ul> <p>在 Websense Manager 中設定 Policy Server 設定 (請參閱 <a href="#">使用 Policy Server</a>，第 239 頁)。</p> <p>政策與大部分配置設定會在共用 Policy Database 的 Policy Server 之間共用 (請參閱 <a href="#">在多 Policy Server 環境中運作</a>，第 240 頁)。</p>
<b>Filtering Service</b>	<p>與 Network Agent 或協力廠商整合產品一起提供網際網路篩選。當使用者要求某個網站時，Filtering Service 會接收要求並決定要套用哪些政策。</p> <ul style="list-style-type: none"> <li>必須執行 Filtering Service，以便篩選及記錄網際網路要求。</li> <li>每個 Filtering Service 實例都會下載自己的 Websense Master Database 複本。</li> </ul> <p>在 Websense Manager 中設定篩選和 Filtering Service 行為 (請參閱 <a href="#">網際網路使用量篩選器</a>，第 33 頁和 <a href="#">設定 Websense 篩選設定</a>，第 49 頁)。</p>
<b>Network Agent</b>	<ul style="list-style-type: none"> <li>加強篩選和記錄功能</li> <li>啟動通訊協定管理</li> <li>在單機環境中啟動篩選</li> </ul> <p>如需詳細資訊，請參閱 <a href="#">網路配置</a>，第 293 頁。</p>
<b>Master Database</b>	<ul style="list-style-type: none"> <li>包含超過 3,600 萬個網站，儲存在超過 90 個類別和下層類別中</li> <li>包含超過 100 個用於篩選通訊協定的通訊協定定義</li> </ul> <p>下載 Websense Master Database 以啟動網際網路篩選，並確認資料庫保持在最新狀態。如果 Master Database 超過 2 個星期沒有更新，則不會進行篩選。如需詳細資訊，請參閱 <a href="#">Websense Master Database</a>，第 29 頁。</p>
<b>Websense Manager</b>	<p>作為 Websense 軟體的配置和管理介面。</p> <p>使用 Websense Manager 來定義及自訂網際網路存取政策、新增或移除篩選用戶端，以及設定 Websense 軟體元件等等。</p> <p>如需詳細資訊，請參閱 <a href="#">使用 Websense Manager</a>，第 16 頁。</p>

元件	說明
<b>Usage Monitor</b>	<p>根據網際網路使用量啓動警示。</p> <p>Usage Monitor 會追蹤 URL 類別與通訊協定存取，並根據您所設定的警示行爲產生警示訊息。</p> <p>如需詳細資訊，請參閱 <a href="#">警示</a>，第 246 頁。</p>
<b>Remote Filtering Client</b>	<ul style="list-style-type: none"> <li>位在網路防火牆之外的用戶端電腦上。</li> <li>將電腦識別爲要篩選的用戶端，並與 Remote Filtering Server 進行通訊。</li> </ul> <p>如需詳細資訊，請參閱 <a href="#">篩選遠端用戶端</a>，第 137 頁。</p>
<b>Remote Filtering Server</b>	<ul style="list-style-type: none"> <li>允許篩選網路防火牆之外的用戶端。</li> <li>與 Filtering Service 進行通訊以提供遠端電腦的網際網路存取管理。</li> </ul> <p>如需詳細資訊，請參閱 <a href="#">篩選遠端用戶端</a>，第 137 頁。</p>
<b>Websense Content Gateway</b>	<ul style="list-style-type: none"> <li>提供強大的代理與快取平台。</li> <li>可即時分析網站與檔案的內容，以分類先前未分類的網站。</li> </ul> <p>請參閱 <a href="#">使用即時選項分析內容</a>，第 127 頁。</p>
<b>Websense Security Gateway</b>	<p>除了標準 Websense Content Gateway 功能之外：</p> <ul style="list-style-type: none"> <li>分析 HTML 程式碼以尋找安全威脅（例如網路釣魚、URL 重新導向、Web 入侵和以 Proxy 規避封鎖）。</li> <li>檢查檔案內容以指派威脅類別（例如病毒、特洛伊木馬程式或蠕蟲）。</li> <li>抽除特定網頁中的主動式內容。</li> </ul> <p>請參閱 <a href="#">使用即時選項分析內容</a>，第 127 頁。</p>

## 報告元件

元件	說明
Log Server	<p>記錄網際網路要求資料，包括：</p> <ul style="list-style-type: none"> <li>• 要求來源</li> <li>• 與要求關聯的類別或通訊協定</li> <li>• 要求被允許或封鎖</li> <li>• 是否套用關鍵字封鎖、檔案類型封鎖、配額分配、頻寬等級或密碼保護。</li> </ul> <p>藉由 Network Agent 和某些整合產品，Log Server 也可儲存所用頻寬數量的相關資訊。</p> <p>Log Server 必須安裝在 Windows 電腦上，才能在 Websense Manager 中啟動調查與簡報報告，以及「今天」和「記錄」頁面圖表。</p> <p>安裝了 Log Server 之後，設定 Filtering Service 以便將記錄資料傳送至正確位置（請參閱<a href="#">設定用於記錄的 Filtering Service</a>，第 265 頁）。</p>
記錄資料庫	<p>儲存 Log Server 所收集的網際網路要求資料，以供 Websense 報告工具使用。</p>

## 使用者識別元件

元件	說明
User Service	<ul style="list-style-type: none"> <li>• 與您的目錄服務進行通訊。</li> <li>• 將使用者相關資訊（包括使用者對群組及使用者對網域的關係）傳達給 Policy Server 和 Filtering Service，以便用於套用篩選政策。</li> </ul> <p>如果已安裝並設定 Websense 無障礙識別代理程式（請參閱<a href="#">無障礙識別</a>，第 175 頁），User Service 可協助解譯使用者登入工作階段資訊，並使用此資訊將使用者名稱與 IP 位址的關聯提供給 Filtering Service。</p> <p>將使用者和群組新增為 Websense 用戶端時（請參閱<a href="#">新增用戶端</a>，第 61 頁），User Service 會將來自目錄服務的名稱和路徑資訊提供給 Websense Manager。</p> <p>如需有關設定目錄服務存取的資訊，請參閱<a href="#">目錄服務</a>，第 56 頁。</p>
DC Agent	<ul style="list-style-type: none"> <li>• 為以 Windows 為基礎之目錄服務中的使用者提供無障礙使用者識別。</li> <li>• 與 User Service 進行通訊，以便將最新的使用者登入工作階段資訊提供給 Websense 軟體用於篩選。</li> </ul> <p>如需詳細資訊，請參閱<a href="#">DC Agent</a>，第 185 頁。</p>

元件	說明
<b>Logon Agent</b>	<ul style="list-style-type: none"> <li>在 Linux 和 Windows 網路中提供無可比擬的無障礙使用者識別正確性。</li> <li>在擷取使用者登入工作階段時不依賴目錄服務或其他媒介。</li> <li>偵測發生的使用者登入工作階段。</li> </ul> <p>Logon Agent 會與用戶端電腦上的登入應用程式進行通訊，以確保由 Websense 軟體來直接擷取和處理個別使用者登入工作階段。</p> <p>如需詳細資訊，請參閱 <a href="#">Logon Agent</a>，第 187 頁。</p>
<b>eDirectory Agent</b>	<ul style="list-style-type: none"> <li>與 Novell eDirectory 配合運作，以無障礙方式識別使用者。</li> <li>從驗證登入網路之使用者的 Novell eDirectory 收集使用者登入工作階段資訊。</li> <li>將每個已驗證的使用者與 IP 位址關聯，然後與 User Service 配合運作，將資訊提供給 Filtering Service。</li> </ul> <p>如需詳細資訊，請參閱 <a href="#">eDirectory Agent</a>，第 194 頁。</p>
<b>RADIUS Agent</b>	<p>啟動使用撥接、虛擬私人網路 (VPN)、數位訂閱線 (DSL) 或其他遠端連線來存取網路之使用者的無障礙識別。</p> <p>如需詳細資訊，請參閱 <a href="#">RADIUS Agent</a>，第 190 頁。</p>

## 瞭解 Policy Database

Websense Policy Database 會儲存 Websense Manager 中所指定的政策資料 (包括用戶端、篩選器、篩選器元件和委派管理設定) 和全域配置設定。特定於一個 Policy Server 實例的設定會單獨儲存。

在大部分多 Policy Server 環境中，由一個 Policy Database 來保存多個 Policy Server 的政策和一般配置資料。

1. 在啟動時，每個 Websense 元件會透過 Policy Broker 向 Policy Database 要求適用的配置資訊。
2. 執行中的元件會經常檢查 Policy Database 的變更情況。
3. 每次當管理員在 Websense Manager 中執行變更並按一下「全部儲存」時，就會更新 Policy Database。
4. 變更了 Policy Database 之後，每個元件會要求並收到影響其功能的變更。

請定期備份 Policy Database 以保障重要配置和政策資訊的安全。如需詳細資訊，請參閱 [備份與還原 Websense 資料](#)，第 253 頁。

## 使用 Policy Server

Policy Server 是 Websense 軟體元件，用於管理政策資訊並與 Filtering Service 進行通訊以協助政策強制執行。Policy Server 還負責識別其他元件並追蹤其位置與狀態。

登入 Websense Manager 時，會登入 Policy Server 的圖形介面。

- ◆ 必須先設定 Websense Manager 與 Policy Server 進行通訊，然後才能登入 Websense Manager。
- ◆ 如果 Websense 軟體安裝包含多個 Policy Server，可在登入時選擇不同的 Policy Server 實例。
- ◆ 可在 Websense Manager 中新增及移除 Policy Server 實例。

在預設情況下，Websense Manager 與中央 Policy Server 實例之間的通訊會在 Websense Manager 安裝期間建立。

大部分環境只需要一個 Policy Server。一個 Policy Server 能與多個 Filtering Service 和 Network Agent 實例進行通訊，以達到負載平衡。不過，在非常大的組織中 (超過 10,000 個使用者)，安裝多個 Policy Server 實例可能有所幫助。如果您安裝了額外的 Policy Server，請將每個實例新增至 Websense Manager (請參閱 [新增及編輯 Policy Server 實例](#)，第 239 頁)。

## 新增及編輯 Policy Server 實例

使用 **設定 > Policy Server** 頁面，將 Policy Server 實例新增至 Websense Manager，或者設定或移除現有的 Policy Server。

若要新增 Policy Server 實例：

1. 按一下 **新增**。「新增 Policy Server」頁面隨即開啓。
2. 在 **伺服器名稱或 IP** 欄位中，輸入 Policy Server 電腦的 IP 位址或主機名稱。
3. 輸入 Websense Manager 應該用來與 Policy Server 實例進行通訊的 **連接埠**。預設值是 **55806**。
4. 按一下 **確定** 返回 Policy Server 頁面。新的 Policy Server 實例會顯示在清單中。
5. 按一下 **確定** 來快取對 Policy Server 頁面的所有變更。按一下 **全部儲存** 才能使變更生效。

若要編輯 Policy Server 實例 (例如，Policy Server 電腦 IP 位址或名稱變更時)，在 Policy Server 清單中選取 IP 位址或主機名稱，然後按一下 **編輯**。

若要刪除 Policy Server 實例，在 Policy Server 清單中選取 IP 位址或主機名稱，然後按一下 **刪除**。按一下「刪除」會從 Websense Manager 中移除 Policy Server 實例，但是不會解除安裝或停止 Websense Policy Server 服務。如果僅列出了一個 Policy Server 實例，該實例將不能被刪除。

## 在多 Policy Server 環境中運作

在某些具有大量使用者的分散式環境中，可能適合安裝多個 Policy Server。這牽涉到一些特殊考量。

- ◆ 如果實施的配置允許根據目前的負載，由不同 Policy Server 來管理相同用戶端，則**不能**執行以時間為基礎的政策動作：

- 密碼覆寫
- 確認
- 配額

與這些功能關聯的時間資訊不會在 Policy Server 之間共用，且授予用戶端的網際網路存取可能會比您預期的更多或更少。

請記得，每當用戶端未套用任何其他政策時，會強制執行「預設」政策。如果用戶端可由一個以上的 Policy Server 來控管，最好確認「預設」政策不會強制執行套用以時間為基礎之動作的類別篩選器。

- ◆ 由於政策資訊儲存在 Policy Database 中，因此按一下**全部儲存**時，政策變更會自動在所有 Policy Server 之間共用。
- ◆ 許多全域配置設定 (例如風險等級定義和警示選項) 也會在 Policy Server 之間共用。
- ◆ 特定於一個 Policy Server 的配置設定 (例如其 Filtering Service 和 Network Agent 連線) 由每個 Policy Server 本機儲存，而不會被發佈。

若要在 Websense Manager 中切換 Policy Server，以檢閱或設定套用至一個 Policy Server 實例的設定：

1. 在 Websense 標題中，展開 **Policy Server** 清單並選取 IP 位址。
2. 如果目前的 Policy Server 實例有未儲存的變更，則會顯示變更清單。執行下列其中之一：
  - 按一下**全部儲存並登出**，以儲存變更並登出目前的 Policy Server。
  - 按一下**取消變更並登出**，以放棄變更並登出目前的 Policy Server。
  - 按一下**返回**，以繼續設定目前的 Policy Server。

如果有未儲存的變更，則會直接引導至登入畫面。

3. 在登入畫面上，輸入使用者名稱和密碼以登入所選 Policy Server，然後按一下**登入**。

## 變更 Policy Server IP 位址

在變更 Policy Server 電腦的 IP 位址之前，在電腦上**停止所有 Websense 服務**。如果電腦上也安裝有 Websense Manager，這將包括 Apache2Websense 和 ApacheTomcatWebsense 服務。

變更了 IP 位址之後，必須先手動更新 Websense Manager、Policy Server 及其他 Websense 服務所用的 Websense 配置檔案，然後才能繼續進行篩選。



## 步驟 1：更新 Websense Manager 配置

更新 Websense Manager 以使用新的 IP 位址來連線到 Policy Server。

1. 在 Websense Manager 電腦上，停止 **Apache2Websense** 和 **ApacheTomcatWebsense** 服務 (如有必要)。
 

如果此相同的電腦上安裝有 Websense Manager 和 Policy Server，則 Apache 服務應該已停止。
2. 瀏覽至以下目錄：
  - Windows：
 

```
C:\Program Files\Websense\tomcat\conf\Catalina\localhost\
```
  - Linux：
 

```
/opt/Websense/tomcat/conf/Catalina/localhost/
```
3. 找到 **mng.xml** 檔案，然後在其他目錄中建立其備份複本。
4. 在文字編輯器 (如「記事本」或 vi) 中開啓 **mng.xml**，並以新的 Policy Server IP 位址實例來取代每個舊實例。
 

Policy Server IP 位址會出現兩次：做為 **ps/default/host** 值和 **psHosts** 值。
5. 完成之後儲存並關閉檔案。

完成本節中其餘的配置更新之前，請勿重新啓動 Apache 服務。

## 步驟 2：更新 Policy Server 配置

更新 Policy Server 配置檔案以及用於設定 Websense 元件之間通訊的初始化檔案。

1. 如果尚未這麼做，請在 Policy Server 電腦上停止所有 Websense 服務 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。
2. 瀏覽至 Websense **bin** 目錄。
  - Windows：
 

```
C:\Program Files\Websense\bin
```
  - Linux
 

```
/opt/Websense/bin
```
3. 找到 **config.xml** 檔案，然後在其他目錄中建立其備份複本。
4. 在文字編輯器中開啓 **config.xml**，並以新的 Policy Server IP 位址實例來取代每個舊實例。
5. 完成之後儲存並關閉檔案。
6. 在 **bin** 目錄中，找到 **websense.ini** 檔案，然後在其他目錄中建立備份複本。
7. 在文字編輯器中開啓 **websense.ini**，並以新的 Policy Server IP 位址實例來取代每個舊實例。
8. 完成之後儲存並關閉檔案。

### 步驟 3：驗證記錄資料庫連線

使用 Policy Server 電腦上的 Windows ODBC 資料來源管理員來驗證與記錄資料庫的 ODBC 連線情況。

1. 前往開始 > 設定 > 控制台 > 系統管理工具 > 資料來源 (ODBC)。
2. 在系統資料來源名稱標籤上，選取適當的資料來源名稱 (預設為 **wslogdb70**)，然後按一下設定。
3. 確認選取了正確的資料庫伺服器電腦，然後按下一步。
4. 輸入用於連線到資料庫的認證，然後按下一步。
5. 在接下來的兩個畫面上接受預設值，然後按一下**測試資料來源**。



#### 注意

如果測試失敗，檢查資料庫伺服器電腦的名稱，然後再試一次。

如果電腦名稱正確，但測試仍然失敗，確認使用了正確的連接埠，並且防火牆允許在所選連接埠上進行通訊。

### 步驟 4：重新啓動 Websense 服務

1. 重新啓動 Policy Server 電腦。確認電腦上的所有 Websense 服務都正常重新啓動。
2. 如果其他電腦上安裝有用於設定此 Policy Server 的 Websense Manager，在該電腦上重新啓動 **Apache2Websense** 和 **ApacheTomcatWebsense** 服務。



#### 注意

如果 Websense Manager 與 Policy Server 安裝在同一台電腦上，管理員必須使用新 IP 位址來登入。

## 使用 Filtering Service

Filtering Service 是 Websense 軟體元件，它可與 Network Agent 或協力廠商整合產品配合運作來篩選網際網路活動。當使用者要求某個網站時，Filtering Service 會接收要求、決定套用哪些政策，並使用相關政策來決定如何篩選網站。

每個 Filtering Service 實例都會下載自己的 Websense Master Database 複本，以用於決定如何篩選網際網路要求。

Filtering Service 還會將網際網路活動的相關資訊傳送給 Log Server，以便記錄資訊並將其用於報告。

登入 Websense Manager 時，「狀態」>「今天」頁面上的 **Filtering Service 摘要** 中會列出每個與目前 Policy Server 關聯之 Filtering Service 實例的 IP 位址與目前狀態。按一下 Filtering Service IP 位址，可取得所選 Filtering Service 的詳細資訊。

## 檢閱 Filtering Service 詳細資料

使用狀態 > 今天 > **Filtering Service 詳細資料** 頁面來檢閱單個 Filtering Service 實例的狀態。

該頁面會列出：

- ◆ Filtering Service IP 位址
- ◆ 是否正在執行所選實例
- ◆ Filtering Service 版本  
應符合 Websense 軟體版本，包括任何已套用的修正檔。
- ◆ 在 Filtering Service 電腦上執行的作業系統
- ◆ Websense 軟體平台  
指出 Websense 軟體是在單機模式下執行，還是與協力廠商產品整合。
- ◆ 與所選 Filtering Service 進行通訊之任何 Network Agent 實例的 IP 位址和狀態。

按一下 **關閉** 返回「今天」頁面。

## 檢閱 Master Database 下載狀態

網路中的每個 Filtering Service 實例都會下載自己的 Master Database 複本。使用 Websense Manager 時，如果正在進行 Master Database 下載或下載嘗試失敗，「狀態」 > 「今天」頁面上的「健全度警示摘要」會顯示狀態訊息。

如需最近或進行中資料庫下載的詳細資訊，按一下「今天」頁面工具列上的 **資料庫下載**。「資料庫下載」頁面包括每個與目前 Policy Server 關聯之 Filtering Service 實例的項目。

一開始，「資料庫下載」頁面會顯示快速下載摘要，指出下載資料庫的位置、下載的資料庫版本，以及下載是否成功。可從此摘要檢視執行以下操作：

- ◆ 開始一個 Filtering Service 的資料庫下載 (按一下 **更新**)。
- ◆ 開始所有列出之 Filtering Service 實例的資料庫下載 (按一下 **全部更新**)。
- ◆ 取消一個或全部進行中的更新。

在右邊的清單中按一下 IP 位址，以檢閱所選 Filtering Service 的資料庫下載狀態的詳細資料。

- ◆ 如果所選 Filtering Service 遇到下載問題，可能會顯示解決該問題的建議。
- ◆ 若要手動開始所選 Filtering Service 的資料庫下載，按一下 **更新**。

在資料庫下載期間，狀態畫面會顯示下載程序每個階段的詳細進度資訊。按一下 **關閉** 隱藏進度資訊，並繼續使用 Websense Manager。

## 可繼續的 Master Database 下載

如果 Master Database 下載被中斷，Websense 軟體會自動嘗試繼續下載。如果 Filtering Service 能夠重新連線至下載伺服器，則會從中斷之處繼續進行下載。

可手動重新啓動失敗或中斷的下載。這樣不會從中斷點繼續下載，而是會從頭重新啓動下載程序。

1. 在 Websense Manager 中，前往**狀態 > 今天**，然後按一下**資料庫下載**。
2. 按一下**停止所有更新**來停止中斷的程序。
3. 選取 Filtering Service 實例並按一下**更新**，或按一下**全部更新**，以從頭重新啓動下載程序。

## 檢視並匯出稽核記錄

Websense 軟體會提供稽核線索，顯示哪些管理員曾存取 Websense Manager，以及對政策與設定所做的任何變更。此資訊只會提供給被授予政策權限的「超級管理員」（請參閱[超級管理員](#)，第 207 頁）。

委派的管理員對他們所管理之用戶端的網際網路活動具有很大的控制權。透過稽核記錄來監控其變更，可確保他們以負責的方式並根據貴組織可接受的使用政策來運用此控制權。

使用**狀態 > 稽核記錄**頁面來檢視稽核記錄，並根據需要將所選的記錄部分匯出至 Excel 試算表 (XLS) 檔案。

稽核記錄會儲存 60 天。若要將稽核記錄保留超過 60 天，可使用匯出選項定期匯出記錄。匯出不會將記錄從稽核記錄中移除。

「稽核記錄」頁面開啓時會顯示最近的記錄。使用記錄上方的捲軸和分頁按鈕來檢視較舊的記錄。

記錄會顯示以下資訊。如果某個項目被截斷，按一下部份項目可在彈出式對話方塊中顯示完整記錄。

欄位	說明
日期	變更的日期與時間，根據時區來調整。 若要確保稽核記錄中資料的一致性，請確認所有執行 Websense 元件的電腦都已同步處理其日期與時間設定。
使用者	執行變更之管理員的使用者名稱。
伺服器	執行受變更影響之 Policy Server 的電腦 IP 位址或名稱。 這樣僅會顯示影響 Policy Server 的變更，例如在「設定」標籤上所做的變更。

欄位	說明
角色	受變更影響的委派管理角色。 當變更影響明確指派為委派管理員角色中受管理之用戶端的用戶端時，變更會顯示為影響「超級管理員」角色。如果變更影響的用戶端是指派給角色之網路範圍、群組、網域或組織單位的成員，變更會顯示為影響委派管理員的角色。
類型	已變更的配置要素，例如政策、類別篩選器或登入/登出。
要素	已變更之特定物件的識別碼，例如類別篩選器名稱或角色名稱。
動作	所做的變更類型，例如新增、刪除、變更、登入等等。
前一個	變更之前的值。
目前	變更之後的新值。

並非所有項目都會顯示給所有記錄。例如，角色不會顯示給登入和登出記錄。

若要匯出稽核記錄：

1. 從**匯出範圍**清單中選取時段。  
選取**過去 60 天**以匯出整個稽核記錄檔。
2. 按一下**開始**。  
如果執行 Websense Manager 的電腦上安裝有 Microsoft Excel，將開啓匯出的檔案。使用 Excel 中的選項來儲存或列印檔案。  
如果執行 Websense Manager 的電腦上未安裝 Microsoft Excel，請依照畫面上的指示找到軟體或儲存檔案。

## 停止和啓動 Websense 服務

Websense 服務被設定為在每次電腦重新啓動時啓動。不過，有時您需要重新啓動電腦單獨停止或啓動一或多個產品元件。



### 注意

如果 Filtering Service 正在下載 Master Database，必須等到下載完成之後才會停止 Filtering Service。

停止所有 Websense 服務時，務必按照所示以下順序以下列服務來結束：

1. Websense Policy Server
2. Websense Policy Broker
3. Websense Policy Database

請注意，除非問題明確與 Policy Broker 或 Policy Database 有關，否則很少需要重新啓動這些服務。盡量避免重新啓動這些服務。

啓動所有 Websense 服務時，務必按照所示順序從下列服務開始：

1. Websense Policy Database
2. Websense Policy Broker
3. Websense Policy Server

### Windows

1. 開啓「Windows 服務」對話方塊(開始 > 設定 > 控制台 > 系統管理工具 > 服務)。
2. 以滑鼠右鍵按一下 Websense 服務名稱，然後選取**停止或啓動**。

### Linux

在 Linux 電腦上，使用此程序時，所有服務會一起停止或啓動。

1. 前往 `/opt/Websense` 目錄。
2. 使用下列指令檢查 Websense 服務的狀態：
  - `./WebsenseAdmin status`
3. 使用下列指令停止、啓動或重新啓動所有 Websense 服務：
  - `./WebsenseAdmin stop`
  - `./WebsenseAdmin start`
  - `./WebsenseAdmin restart`



#### 警告

請勿使用 **kill** 指令來停止 Websense 服務，如此可能會損毀服務。

---

## 警示

---

相關主題：

- ◆ [流量控制](#)，第 247 頁
- ◆ [設定一般警示選項](#)，第 248 頁
- ◆ [設定系統警示](#)，第 249 頁
- ◆ [設定類別使用警示](#)，第 250 頁
- ◆ [設定通訊協定使用警示](#)，第 251 頁

爲有利於追蹤與管理 Websense 軟體和用戶端網際網路活動，「超級管理員」可設定在發生所選事件時傳送警示。

- ◆ **系統警示**：有關訂閱狀態和 Master Database 活動的通知。

- ◆ **使用警示**：特定類別或通訊協定之網際網路活動達到所設定的臨界值時的通知。

可透過電子郵件、螢幕上彈出式訊息 (Windows **net send** 訊息) 或 SNMP 訊息，將警示傳送給所選收件人。



#### 注意

螢幕上的彈出式警示無法傳送至 Linux 電腦。不過，只要 Linux 電腦上安裝有 Samba 用戶端，便可將警示從執行 Policy Server 的 Linux 電腦傳送至 Windows 電腦。請參閱**部署手冊**。

可為 Websense 定義及自訂的類別或通訊協定產生使用警示。

## 流量控制

相關主題：

- ◆ [警示，第 246 頁](#)
- ◆ [設定一般警示選項，第 248 頁](#)
- ◆ [設定類別使用警示，第 250 頁](#)
- ◆ [設定通訊協定使用警示，第 251 頁](#)

使用警示有一些內建控制項，用於避免產生過多數目的警示訊息。使用**每一使用類型的每日警示數目上限**設定，來指定回應使用者對特定類別和通訊協定之要求時傳送的警示數目限制。如需詳細資訊，請參閱[設定一般警示選項，第 248 頁](#)。

也可為每個類別和通訊協定使用警示設定臨界值限制。例如，如果您特定類別設定的臨界值限制為 10，則會在要求該類別 10 次之後 (由任何用戶端的組合) 產生警示。如需詳細資訊，請參閱[設定類別使用警示，第 250 頁](#)和[設定通訊協定使用警示，第 251 頁](#)。

假設每日警示數目上限設定為 20，且類別警示臨界值為 10，則只會將超過臨界值的前 20 次類別要求的警示提供給管理員。這表示只有前 200 次發生的情況會導致警示訊息 (臨界值 10 乘以警示限制 20)。

## 設定一般警示選項

相關主題：

- ◆ [警示，第 246 頁](#)
- ◆ [設定系統警示，第 249 頁](#)
- ◆ [設定類別使用警示，第 250 頁](#)
- ◆ [設定通訊協定使用警示，第 251 頁](#)

Websense 軟體可通知管理員各種不同的系統事件，例如 Master Database 類別和訂閱問題的更新，以及超過定義的臨界值的網際網路使用。

使用**設定 > 警示與通知 > 警示**頁面來選取並設定所需的通知方法(如以下所述)。然後，使用「設定」>「警示與通知」區段中的其他頁面來啟動您想要接收的警示。

1. 在**每一使用類型的每日警示數目上限**欄位中輸入數字，以限制每日為每個類別和通訊協定使用警示產生的警示總數。

例如，可設定要求「體育運動」類別中網站的次數每達 5 次(臨界值)便傳送使用警示。視使用者人數及其網際網路使用模式而定，每天可能會產生數百個警示。

如果輸入 10 做為每一使用類型的每日警示數目上限，則每天只會針對「體育運動」類別產生 10 個警示訊息。在此範例中，這些訊息會針對「體育運動」網站的前 50 個要求提供警示(每一警示 5 個要求乘以 10 個警示)。

2. 標記**啟動電子郵件警示**核取方塊，以透過電子郵件傳送警示與通知。然後，設定這些電子郵件設定。

SMTP 伺服器 IP 或名稱	應該用來傳送電子郵件警示的 SMTP 伺服器 IP 位址或名稱。
寄件者電子郵件位址	用作電子郵件警示寄件者的電子郵件位址。
管理員電子郵件位址(收件者)	電子郵件警示主要收件人的電子郵件位址。
收件人電子郵件位址(副本)	其他收件人的電子郵件位址，最多為 50 個。每個位址必須放在單獨的行中。

3. 標記**啟動彈出式警示**核取方塊，以便在特定電腦上顯示彈出式訊息。然後，在單獨的行中輸入最多 50 個**收件人**的 IP 位址或電腦名稱。



### 注意

彈出式警示無法傳送至 Linux 電腦。不過，只要 Linux 電腦上安裝有 Samba 用戶端，便可將警示從執行 Policy Server 的 Linux 電腦傳送至 Windows 電腦。請參閱**部署手冊**。



- 標記**啓動 SNMP 警示**核取方塊，以便透過安裝在網路中的 SNMP Trap 系統來傳送警示訊息。然後，提供 SNMP Trap 系統的相關資訊。

社群名稱	SNMP Trap 伺服器上 trap 社群的名稱。
伺服器 IP 或名稱	SNMP Trap 伺服器的 IP 位址或名稱。
連接埠	SNMP 訊息使用的連接埠號碼。

- 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

## 設定系統警示

相關主題：

- ◆ [警示，第 246 頁](#)
- ◆ [設定一般警示選項，第 248 頁](#)
- ◆ [檢閱目前的系統狀態，第 252 頁](#)

Websense Manager 會透過**狀態 > 警示** (詳細資訊) 頁面，顯示系統健全度與狀態的詳細資訊，如[檢閱目前的系統狀態，第 252 頁](#)中所述。

爲確保管理員收到重大系統事件的通知，例如資料庫下載失敗或訂閱即將到期，可以設定當管理員未登入 Websense Manager 時，便透過電子郵件、彈出式訊息或 SNMP Trap 系統來發佈 Websense 系統警示。

在「設定」標籤上，使用**警示與通知 > 系統**頁面，來選取向 Websense 管理員傳送這些警示的方法，以及要傳送哪些警示。

- 針對每個警示，標記要使用的傳送方法。視在「警示」頁面上的啓動方法而定，可以選擇**電子郵件**、**彈出式**和**SNMP**方法。



### 注意

除了產生警示之外，有關 Master Database 下載失敗和超出訂閱等級的資訊會記錄在 Windows 事件檢視器 (僅 Windows) 及 Websense.log 檔案 (Windows 和 Linux) 中。

警示可用於以下事件：

- 您的訂閱將於一週內到期。
- 「搜尋篩選」支援的搜尋引擎已變更。
- Websense Master Database 下載失敗。
- 已從 Master Database 新增或移除類別或通訊協定。
- 目前的使用者人數已超出您的訂閱等級。
- 目前的使用者人數已達到訂閱等級的 90%。

- 您的訂閱將於一個月內到期。
  - Websense Master Database 已更新。
2. 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

## 設定類別使用警示

相關主題：

- ◆ [警示](#)，第 246 頁
- ◆ [流量控制](#)，第 247 頁
- ◆ [設定一般警示選項](#)，第 248 頁
- ◆ [新增類別使用警示](#)，第 250 頁

Websense 軟體可在特定 URL 類別的網際網路活動達到定義的臨界值時通知您。可為類別的允許要求或封鎖要求定義警示。

例如，您可能希望在每次有 50 個針對「購物」類別中網站的要求被允許時收到警示，以協助決定是否要對該類別應用限制。或者，您可能希望在每次有 100 個針對「娛樂」類別中網站的要求遭封鎖時收到警示，以瞭解使用者是否適應新的網際網路使用政策。

在「設定」標籤上，使用**警示與通知 > 類別使用**頁面來檢視已建立的警示，以及新增或刪除使用警示類別。

1. 檢視**允許的類別使用警示**和**封鎖的類別使用警示**清單，以瞭解哪些類別設定了警示、每個警示的臨界值以及所選的警示方法。
2. 在相關清單底下按一下**新增**，以開啓「新增類別使用警示」頁面（請參閱[新增類別使用警示](#)，第 250 頁）並為其他 URL 類別設定警示。
3. 標記所有想要從其清單中刪除之類別的核取方塊，然後在相關底下按一下**刪除**。
4. 完成之後，按一下**確定**來快取變更並返回「類別使用量」頁面。按一下**全部儲存**才能使變更生效。

## 新增類別使用警示

相關主題：

- ◆ [警示](#)，第 246 頁
- ◆ [設定一般警示選項](#)，第 248 頁
- ◆ [設定類別使用警示](#)，第 250 頁

在「類別使用警示」頁面上按一下「新增」之後，會出現**新增類別使用警示**頁面。可在此選取要設定使用警示的新類別、建立這些警示的臨界值以及選取警示方法。

1. 標記每個用相同臨界值和警示方法新增的類別旁的核取方塊。



#### 注意

不能為記錄中不存在的所有類別新增使用警示。請參閱**設定用於記錄的 Filtering Service**，第 265 頁。

2. 選取會導致警示產生的要求數目以設定**臨界值**。
3. 為這些類別標記每個所需警示方法 (**電子郵件、彈出式、SNMP**) 的核取方塊。只能選取已在「警示」頁面上啟動的警示方法 (請參閱**設定一般警示選項**，第 248 頁)。
4. 按一下**確定**來快取變更並返回「類別使用警示」頁面 (請參閱**設定類別使用警示**，第 250 頁)。按一下**全部儲存**才能使變更生效。

## 設定通訊協定使用警示

相關主題：

- ◆ [警示](#)，第 246 頁
- ◆ [流量控制](#)，第 247 頁
- ◆ [設定一般警示選項](#)，第 248 頁
- ◆ [新增通訊協定使用警示](#)，第 252 頁

Websense 軟體可在特定通訊協定的網際網路活動達到定義的臨界值時通知您。可為所選通訊協定的允許要求或封鎖要求定義警示。

例如，您可能希望在每次有 50 個針對特定即時訊息傳送通訊協定的要求被允許時收到警示，以協助決定是否要對該通訊協定應用限制。或者，您可能希望在每次有 100 個針對特定端對端檔案共用通訊協定的要求遭封鎖時收到警示，以瞭解使用者是否適應新的網際網路使用政策。

在「設定」標籤上，使用**警示與通知 > 通訊協定使用量**頁面來檢視已建立的警示，以及新增或刪除用於使用警示的通訊協定。

1. 檢視**允許的通訊協定使用警示**和**封鎖的通訊協定使用警示**清單，以瞭解哪些通訊協定設定了警示、每個警示的臨界值以及所選的警示方法。
2. 在相關底下按一下**新增**，以開啓「新增通訊協定使用警示」頁面 (請參閱**新增通訊協定使用警示**，第 252 頁) 並為其他通訊協定設定警示。
3. 選取所有想要刪除之通訊協定的核取方塊，然後在相關底下按一下**刪除**。
4. 完成之後，按一下**確定**來快取變更並返回「通訊協定使用警示」頁面。按一下**全部儲存**才能使變更生效。

## 新增通訊協定使用警示

相關主題：

- ◆ [警示](#)，第 246 頁
- ◆ [設定一般警示選項](#)，第 248 頁
- ◆ [設定通訊協定使用警示](#)，第 251 頁

使用[通訊協定使用警示](#) > [新增通訊協定使用警示](#)頁面，來選取用於使用警示的新通訊協定、建立這些警示的臨界值以及選取警示方法。

1. 標記每個用相同臨界值和警示方法新增的通訊協定旁的核取方塊。



### 注意

除非已在一或多個通訊協定篩選器中設定記錄通訊協定，否則無法選取該通訊協定來設定警示。

通訊協定警示僅反映記錄通訊協定的通訊協定篩選器所控管之用戶端的使用情況。

2. 選取會導致警示產生的要求數目以設定**臨界值**。
3. 為這些通訊協定選取每個所需的警示方法 (**電子郵件、彈出式、SNMP**)。只能選取已在「警示」頁面上啟動的警示方法 (請參閱[設定一般警示選項](#)，第 248 頁)。
4. 按一下**確定**來快取變更並返回「通訊協定使用警示」頁面 (請參閱[設定通訊協定使用警示](#)，第 251 頁)。按一下**全部儲存**才能使變更生效。

## 檢閱目前的系統狀態

使用[狀態](#) > [警示](#)頁面，來尋找影響 Websense 軟體健全度之問題的相關資訊、取得疑難排解協助，以及檢閱 Websense Master Database 最近的即時更新詳細資訊。

**使用中的警示**清單會顯示受監控的 Websense 軟體元件的狀態。

- ◆ 如需受到監控之元件的詳細資訊，按一下警示訊息清單上方的**監控什麼？**
- ◆ 若要疑難排解問題，按一下錯誤或警告訊息旁的**解決方案**按鈕。
- ◆ 若要隱藏警示訊息，按一下**進階**。如果貴組織未使用 Log Server、Network Agent 或 User Service，或者您不打算啟動 WebCatcher，可標記核取方塊以隱藏關聯的警示。完成之後，按一下**確定**來執行變更。再按一次**進階**來隱藏進階選項。

**即時資料庫更新**清單提供 Websense Master Database 的緊急更新相關資訊，其中顯示：

- ◆ 更新何時發生
- ◆ 更新類型
- ◆ 新資料庫版本編號
- ◆ 更新原因
- ◆ 收到更新之 Filtering Service 實例的 IP 位址

這些補充更新在定期、排程的 Master Database 更新以外發生，它們可用於將暫時分類錯誤的網站重新分類等用途。Websense 軟體每小時都會檢查資料庫更新。

對於 Websense Web Security 使用者，警示頁面包含第三份清單：**即時安全性更新**。此清單與「即時資料庫更新」清單的格式相同，但會特別顯示與安全相關的資料庫更新。

在這些安全更新建立時儘速安裝他們，有助於降低下列弱點造成的威脅：新型網路釣魚 (身份詐欺) 詐騙、流氓應用程式及感染主要網站或應用程式的惡意程式碼。

如需即時安全性更新的詳細資訊，請參閱[即時安全性更新™](#)，第 30 頁。

使用頁面上方的**列印**按鈕可開啓另一個視窗，其中有「警示」區域的可列印版本。使用瀏覽器選項來列印此頁面，如此即可不列印出主要 Websense Manager 視窗中的所有瀏覽選項。

## 備份與還原 Websense 資料

相關主題：

- ◆ [排程備份](#)，第 255 頁
- ◆ [執行立即備份](#)，第 256 頁
- ◆ [維護備份檔案](#)，第 257 頁
- ◆ [還原 Websense 資料](#)，第 257 頁
- ◆ [終止已排程的備份](#)，第 258 頁
- ◆ [指令參考](#)，第 259 頁

Websense Backup Utility 可輕鬆備份 Websense 軟體設定和政策資料，並可還原至先前的配置。公用程式儲存的資料也可用於在升級之後匯入 Websense 配置資訊。

Backup Utility 會儲存：

- ◆ 儲存於 Policy Database 中的全域配置資訊，包括用戶端與政策資料。
- ◆ 由每個 Policy Server 所儲存的本機配置資訊，例如 Filtering Service 和 Log Server 設定。

- ◆ Websense 元件初始化和配置檔案。

備份程序的運作如下：

1. 開始立即備份 (請參閱 [執行立即備份](#)，第 256 頁) 或定義備份排程 (請參閱 [排程備份](#)，第 255 頁)。
  - 隨時手動啟動備份。
  - 執行或排程備份時，備份檔案會儲存在指定的目錄中。
2. Backup Utility 會檢查電腦上的所有 Websense 元件、收集適合備份的資料，並建立封存檔案。檔案名稱採用下列格式：  
`wbackup_YYYY-mm-dd_hhmmss.tar.gz`  
 其中，`YYYY-mm-dd_hhmmss` 代表備份的日期與時間，**tar.gz** 是可攜式壓縮檔格式。  
 只有根 (Linux) 和系統管理員群組的成員 (Windows) 才能存取備份檔案。

在每台包含 Websense 元件的電腦上執行 Websense Backup Utility。此工具會識別並儲存在目前電腦上所找到的下列任何檔案：

路徑	檔案名稱
<b>\Program Files\Websense\bin</b> 或 <b>/opt/Websense/bin</b>	authserver.ini BrokerService.cfg config.xml eimserver.ini LogServer.ini netcache.conf securewisproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
<b>bin/i18n</b>	i18n.ini
<b>bin/postgres/data</b>	postgresql.conf pg_hba.conf
<b>BlockPages*/Custom</b>	所有自訂封鎖頁面設定
<b>tomcat/conf/Catalina/Localhost</b>	mng.xml
<b>Windows\system32</b>	isa_ignore.txt

路徑	檔案名稱
Windows\system32\bin	ignore.txt
/etc/wsLib	wsSquid.ini

將 Websense 備份檔案儲存在安全的位置。這些檔案應該是貴組織定期備份程序的一部分。

若要還原至先前的配置：

1. 從其儲存位置擷取備份檔案。
2. 將每個備份檔案複製到建立該檔案的 Websense 電腦上。
3. 以還原模式執行 Backup Utility。



### 重要

務必使用 Backup Utility 來還原 Websense 軟體配置。請勿使用其他擷取公用程式從封存中擷取檔案。

如果備份檔案已損毀，則無法還原設定。

在還原程序進行期間，所有錯誤訊息或警告會顯示在執行還原的電腦上。

## 排程備份

相關主題：

- ◆ [執行立即備份](#)，第 256 頁
- ◆ [維護備份檔案](#)，第 257 頁
- ◆ [還原 Websense 資料](#)，第 257 頁
- ◆ [終止已排程的備份](#)，第 258 頁
- ◆ [指令參考](#)，第 259 頁

若要排程備份，開啓指令殼層並瀏覽至 Websense bin 目錄 (在預設情況下為 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**)。輸入下列指令。

```
wsbackup -s -t "<m> <h> <day_of_month> <month>
<day_of_week>" -d <directory>
```

請注意，時間資訊使用 **crontab** 格式，並且需要引號和空格。

在示例中所示的變數處提供下列資訊：

變數	資訊
<m>	0 - 59 指定啟動備份的精確分鐘。
<h>	0 - 23 指定啟動備份該日的一般小時。
<day_of_month>	1 - 31 指定執行備份的日期。如果排程在第 29 - 31 天執行備份，則公用程式會在未包含該日期的月份中，使用作業系統的標準替代程序。
<month>	1 - 12 指定執行備份的月份。
<day_of_week>	0 - 6 指定星期。0 代表星期日。

每個欄位可接受數字、星號或參數清單。請參閱任何 **crontab** 參考以取得詳細資訊。

## 執行立即備份

相關主題：

- ◆ [排程備份](#)，第 255 頁
- ◆ [維護備份檔案](#)，第 257 頁
- ◆ [還原 Websense 資料](#)，第 257 頁
- ◆ [終止已排程的備份](#)，第 258 頁
- ◆ [指令參考](#)，第 259 頁

若要啟動立即備份，開啓指令殼層並瀏覽至 Websense bin 目錄 (在預設情況下為 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**)。輸入下列指令。

```
wsbackup -b -d <目錄>
```

其中，*目錄*表示備份封存的目的目錄。



### 警告

請勿將備份檔案儲存在 Websense **bin** 目錄中。解除安裝 Websense 軟體時此目錄將被刪除。

開始立即備份時，所有錯誤訊息和通知會顯示在執行備份之電腦的主控台上。



## 維護備份檔案

相關主題：

- ◆ [排程備份](#)，第 255 頁
- ◆ [執行立即備份](#)，第 256 頁
- ◆ [還原 Websense 資料](#)，第 257 頁
- ◆ [終止已排程的備份](#)，第 258 頁
- ◆ [指令參考](#)，第 259 頁

執行備份時，會建立配置檔案 (**WebsenseBackup.cfg**)，配置檔案將與備份封存一起儲存。此配置檔案會指定：

- ◆ 備份封存在備份目錄中保存多久
- ◆ 目錄中所有備份檔案可以使用的磁碟空間容量上限

在任何文字編輯器中編輯 **WebsenseBackup.cfg** 檔案，以變更下列任一參數：

參數	值
KeepDays	封存檔案應保留在備份目錄中的天數。預設值是 365。
KeepSize	為備份檔案分配的位元組數目。預設值是 10857600。

在 **KeepDays** 值之前的任何檔案都會從備份目錄中刪除。如果超過所分配的磁碟空間容量，則會從備份目錄中刪除最舊的檔案，以釋出空間給較新的檔案。

## 還原 Websense 資料

相關主題：

- ◆ [排程備份](#)，第 255 頁
- ◆ [執行立即備份](#)，第 256 頁
- ◆ [維護備份檔案](#)，第 257 頁
- ◆ [終止已排程的備份](#)，第 258 頁
- ◆ [指令參考](#)，第 259 頁

還原 Websense 配置資料時，請確認您是為存在於目前電腦上的元件還原資料。

若要開始還原程序，開啓指令殼層並瀏覽至 Websense bin 目錄 (在預設情況下為 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**)。輸入下列指令。

```
wsbackup -r -f archive_file.tar.gz
```



### 重要

還原程序可能需要幾分鐘的時間。正在進行還原時，請勿停止程序。

在還原程序進行期間，Backup Utility 會停止所有 Websense 服務。如果公用程式無法停止服務，它會傳送訊息要求使用者手動停止服務。必須按照 [停止和啓動 Websense 服務](#)，第 245 頁中所述的順序來停止服務。

Backup Utility 會儲存一些用來與協力廠商整合產品進行通訊的檔案。由於這些檔案位在 Websense 目錄結構之外，您必須將每個檔案複製到正確的目錄以便手動還原檔案。

必須手動還原的檔案包括：

檔案名稱	還原至
isa_ignore.txt	Windows\system32
ignore.txt	Windows\system32\bin
wsSquid.ini	/etc/wsLib

## 終止已排程的備份

相關主題：

- ◆ [排程備份](#)，第 255 頁
- ◆ [執行立即備份](#)，第 256 頁
- ◆ [維護備份檔案](#)，第 257 頁
- ◆ [還原 Websense 資料](#)，第 257 頁
- ◆ [指令參考](#)，第 259 頁

若要清除備份排程並停止執行目前已排程的備份，開啓指令殼層並瀏覽至 Websense bin 目錄 (在預設情況下為 **C:\Program Files\Websense\bin** 或 **opt/Websense/bin**)。輸入下列指令：

```
wsbackup -u
```

## 指令參考

相關主題：

- ◆ [排程備份](#)，第 255 頁
- ◆ [執行立即備份](#)，第 256 頁
- ◆ [維護備份檔案](#)，第 257 頁
- ◆ [還原 Websense 資料](#)，第 257 頁
- ◆ [終止已排程的備份](#)，第 258 頁

只有根 (Linux) 或系統管理員群組的成員 (Windows) 才能執行 Backup Utility。

若要在任何時候檢視完整的 Backup Utility 指令選項清單，可輸入：

```
wbackup -h
```

或

```
wbackup --help
```

**wbackup** 指令接受下列選項：

- ◆ `-b` 或 `--backup`
- ◆ `-d directory_path` 或 `--dir directory_path`
- ◆ `-f full_file_name` 或 `--file full_file_name`
- ◆ `-h` 或 `--help` 或 `-?`
- ◆ `-r` 或 `--restore`
- ◆ `-s` 或 `--schedule`
- ◆ `-t` 或 `--time`
- ◆ `-u` 或 `--unschedule`
- ◆ `-v` 或 `--verbose [0...3]`



# 13

## 報告管理

相關主題：

- ◆ [計畫您的配置](#)，第 262 頁
- ◆ [管理報告工具的存取](#)，第 262 頁
- ◆ [基本配置](#)，第 263 頁
- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [管理記錄資料庫](#)，第 278 頁
- ◆ [設定調查報告](#)，第 287 頁
- ◆ [自行報告](#)，第 291 頁

若要使用 Websense 簡報報告和調查報告，您必須在 Windows 伺服器上同時安裝 Websense Manager 和報告元件。也必須設定 Websense 軟體記錄網際網路篩選活動。

記錄功能會將記錄傳送到 Websense Log Server，以便在必須安裝在支援之資料庫引擎中的記錄資料庫上處理：Microsoft SQL Server Desktop Engine (在此文件中通常稱為 MSDE)，或者 Microsoft SQL Server Enterprise Edition 或 Microsoft SQL Server Standard Edition (兩者通常稱為 Microsoft SQL Server)。如需安裝這些報告元件的詳細資訊，請參閱 Websense [安裝手冊](#)。

產生報告時，Websense Manager 會根據為報告定義的篩選器顯示來自記錄資料庫的資訊。

在 Linux 伺服器上安裝 Websense Manager，或想要針對其報告需求使用 Linux 的組織，可以安裝單獨的 Websense Explorer for Linux 產品來產生報告。此產品的運作與 Websense Manager 無關。如需安裝與使用該程式的指示，請參閱 Websense [Explorer for Linux 管理員手冊](#)。

## 計畫您的配置

根據您網路中的網際網路流量，記錄資料庫可能會變得非常大。為協助您的組織決定有效率的記錄和報告策略，請考慮以下問題：

- ◆ 網路流量什麼時候最繁忙？  
當流量較低時，請考慮排程資源密集的資料庫工作與報告工作。這樣會改善尖峰期間的記錄與報告效能。請參閱[設定網際網路瀏覽時間選項](#)，第 282 頁和[設定記錄資料庫維護選項](#)，第 283 頁。
- ◆ 記錄資料應該保留多久才能支援歷史報告？  
請考慮在到達此階段之後自動刪除分割區。這樣會減少記錄資料庫所需的磁碟空間量。請參閱[設定記錄資料庫維護選項](#)，第 283 頁。
- ◆ 實際上需要的詳細程度為何？  
請考慮要啟動的記錄選項：記錄完整的 URL 和點選次數會增加記錄資料庫的大小。若要減少記錄資料庫的大小，請考慮：
  - 停用完整 URL 記錄 (請參閱[設定完整 URL 記錄](#)，第 281 頁)
  - 記錄造訪次數而非點選次數 (請參閱[設定記錄快取檔案](#)，第 271 頁)
  - 啟動合併 (請參閱[設定合併選項](#)，第 272 頁)
  - 啟動選擇性類別記錄 (請參閱[設定用於記錄的 Filtering Service](#)，第 265 頁)

成功的報告實行是在符合或超出預期負載和歷史資料保存之需求的硬體上部署。

## 管理報告工具的存取

當 Websense Manager 和報告元件安裝在 Windows 伺服器上時，報告選項會出現在 Websense Manager 和 Log Server Configuration 公用程式中。

安裝報告元件時，Log Server 會連接到特定的 Policy Server。您必須在 Websense Manager 登入期間選取該 Policy Server 來存取報告功能。如果登入不同的 Policy Server，則無法存取「主要」標籤上的「簡報報告」或「調查報告」，或是「設定」標籤的整個「報告」區段。

在僅使用 WebsenseAdministrator 登入帳戶的組織中，使用 Websense Manager 的每個人都可以存取 Websense Manager 中的所有報告選項，包括簡報報告、調查報告，以及報告工具的設定。

在使用委派管理的組織中，WebsenseAdministrator 和「超級管理員」角色的成員會控制 Websense Manager 內的報告工具之存取。建立角色時，「超級管理員」會指定該角色是否可以存取特定的報告選項。

如需設定報告工具之存取的資訊，請參閱[編輯角色](#)，第 221 頁。

Log Server Configuration 公用程式從 Windows 「開始」功能表存取。只有可以存取安裝電腦的使用者可以開啓此公用程式以及修改 Log Server 設定。請參閱[Log Server Configuration 公用程式](#)，第 267 頁。

如果貴組織已在 Linux 伺服器上安裝了 Websense Manager，或選擇 Websense Explorer for Linux 報告程式，而不是使用在 Windows 上執行的報告元件，那麼 Websense Manager 就不會顯示報告選項。「今天」與「記錄」頁面上也無法顯示任何網際網路篩選圖表。如需安裝該程式及使用該程式執行報告的詳細資訊，請參閱 *Explorer for Linux 管理員手冊*。

## 基本配置

相關主題：

- ◆ [設定用於記錄的 \*Filtering Service\*，第 265 頁](#)
- ◆ [將類別指派到風險等級，第 264 頁](#)
- ◆ [設定報告偏好設定，第 265 頁](#)
- ◆ [Log Server Configuration 公用程式，第 267 頁](#)
- ◆ [管理記錄資料庫，第 278 頁](#)

可使用各種配置選項為環境自訂報告功能。

Websense Master Database 會將類別組織到**風險等級**中。風險等級指出類別中的網站可能引發之弱點的類型或層級。使用從「設定」標籤存取的「一般」>「風險等級」頁面為貴組織自訂風險等級。請參閱[將類別指派到風險等級，第 264 頁](#)。

使用從「設定」標籤存取的「報告」>「偏好設定」頁面設定用於發佈報告與啟動自行報告功能的電子郵件伺服器。請參閱[設定報告偏好設定，第 265 頁](#)。

記錄是一個程序，它在記錄資料庫中儲存 Websense 篩選活動的相關資訊以產生報告。

使用從「設定」標籤存取的「一般」>「記錄」頁面啟動記錄，選取要記錄的類別，然後決定要記錄的使用者資訊。如需詳細資訊，請參閱[設定用於記錄的 \*Filtering Service\*，第 265 頁](#)。

使用 Log Server Configuration 公用程式管理處理 Log 記錄的方式以及記錄資料庫的連線。如需詳細資訊，請參閱[Log Server Configuration 公用程式，第 267 頁](#)。

使用從「設定」標籤存取的「報告」>「記錄資料庫」頁面管理記錄資料庫，包括網際網路瀏覽時間控制、資料庫分割區選項，以及錯誤記錄。如需詳細資訊，請參閱[管理記錄資料庫，第 278 頁](#)。

## 將類別指派到風險等級

相關主題：

- ◆ [風險等級](#)，第 36 頁
- ◆ [封鎖頁面](#)，第 75 頁
- ◆ [使用報告評估篩選政策](#)，第 83 頁

Websense Master Database 會將類別組織到**風險等級**中。風險等級指出類別中的網站可能引發之弱點的類型或層級。

風險等級主要用於報告。「今天」和「記錄」頁面提供按照風險等級追蹤網際網路活動的圖表，且可產生根據風險等級來組織的簡報或調查報告。

無條件的「超級管理員」可在**設定 > 風險等級**頁面上檢視或變更構成每個風險等級的類別。例如，某些企業可能會考慮將使用者發佈的視訊網站落在法律責任、網路頻寬損失和生產力損失的風險等級。不過，如果貴公司針對特定的人口統計學進行行銷研究，您可能會考慮這些「商業使用量」風險等級的部分。



### 注意

已封鎖網站的安全封鎖頁面會出現在「安全風險」等級的預設類別中。在「安全風險」等級中，對於類別所做的變更會影響報告，但不會影響封鎖頁面。請參閱[封鎖頁面](#)，第 75 頁。

Websense 報告中的風險等級資訊會反映在此頁面上所做的指派。

1. 在**風險等級**清單中選取一個項目。
2. 檢閱**類別**清單來查看目前包含在該風險等級中的類別。  
核取記號表示該類別目前被指派給選取的風險等級。藍色 W 圖示表示預設包含在風險等級中的類別。
3. 標示或清除類別樹狀結構中的項目以包含或排除選取的風險等級中的類別。這些類別可以屬於多個風險等級。

其他選擇包括：

選項	說明
全選	選取樹狀結構中的所有類別。
全部清除	取消選取樹狀結構中的所有類別。
還原預設值	將所選風險等級的類別選擇重設為 Websense 軟體提供的類別選擇。藍色 W 圖示表示預設類別。

4. 針對每個風險等級重複此程序。
5. 按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。



## 設定報告偏好設定

相關主題：

- ◆ [自行報告](#)，第 291 頁
- ◆ [排程簡報報告](#)，第 96 頁
- ◆ [排程調查報告](#)，第 120 頁

排程要在稍後執行或重複執行的簡報報告或調查報告時，系統會透過電子郵件將這些報告發佈給指定的收件人。使用從「設定」標籤存取的[報告 > 偏好設定](#)頁面提供這些電子郵件訊息的重要資訊。

此頁面也用於啟動自行報告，讓個人可以針對自己的網際網路活動產生調查報告。

1. 透過電子郵件發佈排程報告時，輸入要在「寄件人」欄位中出現的**電子郵件位址**。
2. 為用於透過電子郵件發佈排程報告的電子郵件伺服器輸入 **SMTP 伺服器 IP 或名稱**。
3. 標示**允許自行報告**核取方塊允許組織中的一般使用者存取 Websense Manager，並針對其個人網際網路活動執行調查報告。請參閱[自行報告](#)，第 291 頁。
4. 按一下**立即儲存**以執行變更。

## 設定用於記錄的 Filtering Service

相關主題：

- ◆ [記錄資料庫簡介](#)，第 277 頁
- ◆ [Log Server Configuration 公用程式](#)，第 267 頁

使用「設定」標籤上的一般 > [記錄](#)頁面提供 IP 位址和連接埠，以便將 Log 記錄傳送到 Log Server。此頁面也可讓您選取 Websense Filtering Service 應該傳送到 Log Server，並提供給報告和類別使用警示使用的使用者資訊與 URL 類別 (請參閱[設定類別使用警示](#)，第 250 頁)。

在包含多個 Policy Server 的環境中，為每個 Policy Server 分別設定「一般」>「記錄」頁面。所有與作用中 Policy Server 關聯的 Filtering Service 都會將其 Log 記錄傳送到此頁面上識別的 Log Server。

使用多個 Policy Server 時，請謹記下列事實：

- ◆ 如果有任何 Policy Server 的 Log Server IP 位址和連接埠是空的，與該 Policy Server 關聯的 Filtering Service 就無法針對報告或警示記錄任何流量。
- ◆ 每個 Filtering Service 都會根據所連接之 Policy Server 的設定記錄流量。如果變更其他 Policy Server 的使用者資訊或類別記錄選項，則為與其他 Policy Server 關聯之使用者產生的報告可能會出現不一致。

如果您的環境同時包含多個 Policy Server 和多個 Log Server，則請確認已分別登入每個 Policy Server，並確認進行通訊的 Log Server 正確無誤。

1. 要針對存取網際網路的電腦記錄識別資訊，請標記**記錄 IP 位址**。
2. 要針對存取網際網路的使用者記錄識別資訊，請標記**記錄使用者名稱**。



#### 注意

如果沒有記錄 IP 位址或使用者名稱，則您的報告中可能沒有使用者資料。這有時候稱為**匿名記錄**。

3. 在 **Log Server IP 位址或名稱** 欄位中輸入安裝 Log Server 的 IP 位址或電腦名稱。



#### 重要

如果 Log Server 安裝在與 Policy Server 不同的電腦上，這個項目可能會預設為 localhost。如果發生這個情況，輸入 Log Server 電腦的正確 IP 位址，在「今天」和「記錄」頁面上顯示圖表，以及其他報告功能。

4. 輸入**連接埠**號碼，以便將 Log 記錄傳送到 Log Server 中。
5. 按一下**檢查狀態**來判斷 Websense Manager 是否能夠與指定的 Log Server 進行通訊。

此時會出現一個訊息來表示是否通過連接測試。如有需要，可更新 IP 位址或電腦名稱和連接埠，直到測試成功。

6. 按一下**選擇性類別記錄**按鈕來開啓指出要記錄之 URL 類別的區域。您在此所做的選擇會套用到所有作用中政策中的所有類別篩選器。



#### 注意

如果針對已設定使用警示的類別停用記錄 (請參閱**設定類別使用警示**，第 250 頁)，則無法傳送任何使用警示。

報告不得包含未記錄之類別的相關資訊。

- a. 需要時，展開或摺疊上層類別以查看感興趣的類別。
  - b. 標記每個要記錄之類別的核取方塊即可進行選取。  
您必須分別選取或取消選取每個類別。選取上層類別時，不會自動選取其下層類別。使用**全選**和**全部清除**來協助選取。
7. 按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。

## Log Server Configuration 公用程式

相關主題：

- ◆ [管理報告工具的存取](#)，第 262 頁
- ◆ [基本配置](#)，第 263 頁
- ◆ [停止和啓動 Log Server](#)，第 276 頁

在安裝期間，您會設定某些方面的 Log Server 作業，包括 Log Server 如何與 Websense 篩選元件互動。

Log Server Configuration 公用程式可讓您在需要時變更這些設定，並設定 Log Server 作業的其他詳細資訊。此公用程式與 Log Server 安裝在相同的電腦上。

1. 從 Windows「開始」功能表，選擇**程式集 > Websense > 公用程式 > Log Server Configuration**。

Log Server Configuration 公用程式隨即開啓。

2. 選擇一個標籤來顯示其選項並執行任何變更。如需詳細指示，請參閱：
  - [設定 Log Server 連接](#)，第 268 頁
  - [設定 Log Server 資料庫選項](#)，第 269 頁
  - [設定記錄快取檔案](#)，第 271 頁
  - [設定合併選項](#)，第 272 頁
  - [設定 WebCatcher](#)，第 274 頁
3. 按一下**套用**來儲存變更。
4. 使用**連接**標籤來停止及重新啓動 Log Server，以使變更生效。

### 重要

對任何「Log Server Configuration」標籤執行變更後，按一下**套用**。然後您**必須**停止並重新啓動 Log Server 才能使變更生效。若要避免多次重新啓動 Log Server，請在重新啓動 Log Server 前執行所有 Log Server Configuration 變更。

## 設定 Log Server 連接

相關主題：

- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [設定 Log Server 資料庫選項](#)，第 269 頁
- ◆ [設定記錄快取檔案](#)，第 271 頁
- ◆ [設定合併選項](#)，第 272 頁
- ◆ [設定 WebCatcher](#)，第 274 頁
- ◆ [停止和啓動 Log Server](#)，第 276 頁

Log Server Configuration 公用程式的**連接**標籤包含用來在 Log Server 與 Websense 篩選元件之間建立及維護連接的選項。

1. 接受預設的 **Log Server 輸入連接埠** (55805)，或輸入其他可用的連接埠。  
這是 Log Server 用來與 Filtering Service 通訊的連接埠。在此輸入的連接埠必須與在 Websense Manager 中的「一般」>「記錄」頁面（「設定」標籤）上輸入的連接埠相符。
2. 輸入小時數做為**使用者/群組更新間隔**，以指定 Log Server 應聯絡目錄服務以取得更新的頻率。  
Log Server 會聯絡目錄服務以取得記錄資料庫中使用者記錄的相關更新資訊，例如完整的使用者名稱與群組指派。  
已變更群組之使用者的活動仍會以先前的群組來報告，直到發生下次更新。經常更新其目錄服務或擁有大量使用者的組織應該考慮更頻繁地（少於預設的 12 小時）更新使用者/群組資訊。
3. 按一下**套**用來儲存任何變更。
4. 使用「服務狀態」區域中的按鈕來**啓動**或**停止** Log Server。按鈕的標籤會變更，以反映按一下按鈕後會發生的動作。



### 注意

當 Log Server 停止時，便無法記錄任何網際網路存取活動。

在 Log Server Configuration 公用程式中所做的變更，必須等到您停止並重新啓動 Log Server 後才會生效。

## 設定 Log Server 資料庫選項

相關主題：

- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [設定 Log Server 連接](#)，第 268 頁
- ◆ [設定資料庫連接](#)，第 270 頁
- ◆ [設定記錄快取檔案](#)，第 271 頁
- ◆ [設定合併選項](#)，第 272 頁
- ◆ [設定 WebCatcher](#)，第 274 頁
- ◆ [停止和啓動 Log Server](#)，第 276 頁

開啓 Log Server Configuration 公用程式的**資料庫**標籤，以設定 Log Server 如何與記錄資料庫搭配使用。

1. 從下列選項中選擇**記錄插入方式**。
  - 開啓資料庫連接 (ODBC)：分別將記錄插入資料庫，並使用資料庫驅動程式管理 Log Server 與記錄資料庫之間的資料。
  - 大量複製工具程式 (BCP) (*建議*)：以稱為批次的群組方式將記錄插入記錄資料庫。建議使用此選項，因為它的效率高於 ODBC 插入。



### 注意

只有將 SQL Server 用戶端工具安裝在 Log Server 電腦上時，才能使用 BCP 選項。

2. 按一下**連接**按鈕選擇記錄資料庫，以用於儲存來自 Websense 的新網際網路存取資訊。請參閱[設定資料庫連接](#)，第 270 頁。

**ODBC 資料來源名稱 (DSN)** 和 **ODBC 登入名稱** 會顯示為資料庫連接所建立的設定。

3. 如果您在步驟 1 選擇 BCP 做為記錄插入方法，請設定下列選項。如果您選擇 ODBC 做為記錄插入方法，跳過此步驟。

選項	說明
BCP 檔案路徑位置	儲存 BCP 檔案的目錄路徑。這必須是 Log Server 有權讀取和寫入的路徑。 只有當 Log Server 已安裝在記錄資料庫電腦上，或 SQL Server 用戶端工具已安裝在 Log Server 電腦上時，才能使用這個選項。

選項	說明
BCP 檔案建立速率	Log Server 在關閉批次檔並建立新檔案之前，將記錄放入批次檔中所花費的最長時間 (以分鐘為單位)。此設定可配合批次大小設定一起運作：一旦達到任一限制，Log Server 就會立即建立新的批次檔。
BCP 最大批次大小	建立新批次檔之前的最大 Log 記錄數目。此設定可配合建立速率設定一起運作：一旦達到任一限制，Log Server 就會立即建立新的批次檔。

- 設定允許的**最多連線數目**，以指出可在 Log Server 和資料庫引擎之間建立多少內部連線。可用選項取決於使用的資料庫引擎。
  - MSDE**：這個值預設為 4，且無法變更。
  - SQL Server**：根據您的 SQL Server 授權設定 4 到 50 之間的數字。最小連線數目取決於所選的記錄插入方法。



#### 注意

增加連線數目可提高 Log 記錄的處理速度，但可能影響網路中其他使用相同 SQL Server 的程序。在多數情況下，應該將連線數目設為低於 20。請聯絡您的資料庫管理員尋求協助。

- 核取或取消核取**加強記錄**以啓用或停用此選項，此選項控制 Log Server 如何在停止後繼續記錄。當取消選擇此選項時 (預設值)，Log Server 會在停止之後從最舊記錄快取檔案的開頭開始處理。這可能導致在記錄資料庫中產生一些重複的項目，但是會加速 Log Server 處理。當核取此選項時，Log Server 會追蹤它在已啓用記錄快取檔案中的位置。重新啓動之後，Log Server 會從停止之處繼續進行處理。加強記錄可能降低 Log Server 的處理速度。
- 按一下**套用**以儲存任何變更，然後停止並重新啓動 Log Server (請參閱[停止和啓動 Log Server](#)，第 276 頁)。

## 設定資料庫連接

相關主題：

- ◆ [設定 Log Server 連接](#)，第 268 頁
- ◆ [設定 Log Server 資料庫選項](#)，第 269 頁

Log Server Configuration 公用程式的「資料庫」標籤中的**連接**按鈕，可讓您選擇用於儲存來自 Websense 的內送網際網路存取資訊的記錄資料庫。這會在安裝期

間自動設定，但可在您需要變更用於記錄的資料庫時變更該設定。(資料庫必須已經存在才能建立連接。)

1. 在「資料來源」對話方塊中選擇**電腦資料來源**標籤。
2. 為要用來記錄新資訊的資料庫選擇 ODBC 連接。
3. 按一下**確定**以顯示「SQL Server 登入」對話方塊。
4. 如果**使用信任連接**選項可用，請確認針對您的環境正確設定該選項。

**MSDE 使用者**：取消核取「信任連接」選項。

**SQL Server 使用者**：聯絡您的資料庫管理員尋求協助。



#### 注意

如果您使用信任連接與 SQL Server 通訊，可能需要以信任使用者名稱和密碼設定多個 Websense 服務。如需詳細資訊，請參閱 Websense *安裝手冊*。

5. 輸入在建立資料庫時所建立的**登入 ID**和**密碼**。通常這是在 Log Server 安裝與資料庫建立期間所輸入的相同登入 ID 和密碼。
6. 在 Log Server Configuration 公用程式中執行此變更及其他任何變更後，透過**連接**標籤停止並重新啓動 Log Server。

## 設定記錄快取檔案

相關主題：

- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [設定 Log Server 連接](#)，第 268 頁
- ◆ [設定 Log Server 資料庫選項](#)，第 269 頁
- ◆ [設定合併選項](#)，第 272 頁
- ◆ [設定 WebCatcher](#)，第 274 頁
- ◆ [停止和啓動 Log Server](#)，第 276 頁

Log Server Configuration 公用程式的**設定**標籤可讓您管理記錄快取檔案建立選項，並指定 Log Server 是追蹤構成每個要求的網站的個別檔案，還是只追蹤網站。

1. 在**快取檔案路徑位置**欄位中，輸入用於儲存記錄快取檔案的路徑。預設路徑為 **<安裝目錄>\bin\Cache**。(預設安裝目錄為 C:\Program Files\WebSense\)。)
2. 針對**快取檔案建立速率**，指出 Log Server 在關閉記錄快取檔案並建立新檔案之前，應在將網際網路存取資訊傳送至記錄快取檔案 (**logn.tmp**) 上花費的最長時間 (以分鐘為單位)。

此設定可配合大小設定一起運作：一旦達到任一限制，Log Server 就會立即建立新的記錄快取檔案。

3. 針對**快取檔案最大檔案大小**，指定記錄快取檔案大小達到多少時，Log Server 就會將它關閉並建立新檔案。  
此設定可配合建立速率設定一起運作：一旦達到任一限制，Log Server 就會立即建立新的記錄快取檔案。
4. 核取**啓動造訪次數**，為每個造訪的網站建立 Log 記錄。



#### 注意

在高流量網路中，管理記錄資料庫大小是一項重要任務。啓動造訪次數記錄是一種控制資料庫大小和增加容量的方法。

當取消選擇此選項時，會為每個產生的 HTTP 要求建立個別的 Log 記錄，以顯示不同的頁面元素，例如圖形和廣告。此選項也稱為記錄點選次數，它會建立增長迅速，而且比之前大得多的記錄資料庫。

當選擇此選項時，Log Server 會將建立網頁的個別元素 (例如圖形和廣告) 結合成為單一 Log 記錄。

如果已安裝 Websense Web Security Gateway，那麼即使已啓動造訪次數記錄，但在即時掃描特有的報告上，始終會以點選次數來報告即時掃描活動。在此情況下，包含即時掃描所封鎖之流量的 Web 篩選報告上所示的數目，會低於即時掃描報告上所示的數目。



#### 注意

變更造訪次數與點選次數的記錄方法之前，最好先建立新的資料庫分割區。請參閱 Websense Manager 中的「報告」>「記錄資料庫」頁面 (「設定」標籤)，以建立新的資料庫分割區。

5. 按一下**套用**以儲存任何變更，然後停止並重新啓動 Log Server (請參閱[停止和啓動 Log Server](#)，第 276 頁)。

## 設定合併選項

相關主題：

- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [設定 Log Server 連接](#)，第 268 頁
- ◆ [設定 Log Server 資料庫選項](#)，第 269 頁
- ◆ [設定記錄快取檔案](#)，第 271 頁
- ◆ [設定 WebCatcher](#)，第 274 頁
- ◆ [停止和啓動 Log Server](#)，第 276 頁



使用 Log Server Configuration 公用程式的**合併**標籤來啓動合併及設定合併偏好設定。



#### 注意

在高流量網路中，管理記錄資料庫大小是一項重要事務。啓動合併是一種控制資料庫大小和增加容量的方法。

合併可結合共用下列要素的網際網路要求來減少記錄資料庫的大小：

- ◆ 網域名稱 (例如：www.websense.com)
- ◆ 類別
- ◆ 關鍵字
- ◆ 動作 (例如：已封鎖類別)
- ◆ 使用者 / 工作站

記錄資料庫越小，報告的執行速度就越快。不過，合併記錄資料可能會降低某些細節報告的準確性，因為個別網域名稱相同的記錄可能會遺失。



#### 重要

啓動合併可能破壞某些報告資料 (例如網際網路瀏覽時間計算) 的準確性。

1. 核取**合併 Log 記錄**來啓用合併，這會將多個類似的網際網路要求結合為單一 Log 記錄。

預設為取消選擇此選項，記錄資料庫會保留每個網際網路要求的完整點選次數或造訪次數詳細資訊 (這取決於在「設定」標籤上的選擇，請參閱[設定記錄快取檔案](#)，第 271 頁)。這可提供更多的報告詳細資訊，但會導致更大的記錄資料庫。

選擇此選項會以較少的報告詳細資訊建立較小的記錄資料庫。



#### 重要

為確保產生一致的報告，請考慮在每次啓用或停用合併時建立新的資料庫分割區。此外，請務必使用相同的合併設定從分割區產生報告。

如果已安裝 Websense Web Security Gateway，那麼即使已啓動合併，但在即時掃描特有的報告上，始終會以個別的點選次數來報告即時掃描活動。在此情況下，包含即時掃描所封鎖之流量的 Web 篩選報告上所示的數目，會低於即時掃描報告上所示的數目。

2. 為**合併時間間隔**指定第一筆與最後一筆要結合的記錄之間的最長時間。

這代表結合成為一筆合併記錄的最早記錄與最新記錄之間的最大時間差異。減少該時間間隔可提高報告的精確性。增加該時間間隔以最大化合併。請注意，更大的時間間隔也會提高記憶體、CPU 和磁碟空間等系統資源的使用量。

如果您在 Websense Manager 中的「報告」>「記錄資料庫」頁面（「設定」標籤）上啓用「完整 URL」選項，則合併的 Log 記錄將會包含 Log Server 遇到的第一個相符網站之完整路徑（最多 255 個字元）。

例如，假設某位使用者造訪下列網站，且這些網站都分類為「購物」類別。

- www.domain.com/shoeshopping
- www.domain.com/purseshopping
- www.domain.com/jewelryshopping

已啓用完整 URL 時，合併會在 URL www.domain.com/shoeshopping 下建立單一記錄項目。

3. 按一下**套用**以儲存任何變更，然後停止並重新啓動 Log Server（請參閱[停止和啓動 Log Server](#)，第 276 頁）。

## 設定 WebCatcher

相關主題：

- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [設定 Log Server 連接](#)，第 268 頁
- ◆ [設定 Log Server 資料庫選項](#)，第 269 頁
- ◆ [設定記錄快取檔案](#)，第 271 頁
- ◆ [設定合併選項](#)，第 272 頁
- ◆ [設定 WebCatcher](#)，第 274 頁
- ◆ [WebCatcher 驗證](#)，第 276 頁
- ◆ [停止和啓動 Log Server](#)，第 276 頁

WebCatcher 是選用功能，可收集無法辨識的 URL 和安全性 URL，並將它們傳送給 Websense, Inc.，以分析其潛在的安全與責任風險，以及分類。（WebCatcher 處理不需要完整 URL 記錄。）Websense, Inc. 會檢閱資訊並以新分類的 URL 更新 Master Database，從而改善篩選效能。

在 Log Server Configuration 公用程式的 **WebCatcher** 標籤上，選擇要傳送的 URL 類型，並設定檔案大小和處理時間。



### 注意

在包含多部 Log Server 的環境中，只會針對一部 Log Server 啓動 WebCatcher。一旦啓動 WebCatcher，那麼針對其他 Log Server 實例執行 Log Server Configuration tool 時，將無法使用此標籤。

傳送給 Websense, Inc. 的資訊只包含 URL，不會包含使用者資訊。

下列範例說明啓動 WebCatcher 時會傳送的資訊。此範例中的 IP 位址反映 URL 所在的電腦的位址，而非要求者的 IP 位址。

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

WebCatcher 資料會透過 HTTP Post 傳送到 Websense, Inc.。您可能需要在代理伺服器或防火牆上建立角色或執行其他變更，以允許外送 HTTP 流量。請參閱代理伺服器或防火牆文件中的指示。

1. 選擇下列某個選項：
  - **是，僅將特定 URL 傳送到 Websense** 會啓動 WebCatcher 處理。您必須指出要傳送哪些 URL。繼續進行步驟 2。
  - **否，不要傳送資訊至 Websense** 會停用 WebCatcher 處理。如果您選擇此選項，則不需要輸入其他項目。
2. 核取**傳送未分類的 URL** 以傳送在記錄資料庫中找到的所有未分類 URL 的清單。

Websense, Inc. 會分析所收到的未分類 URL，並將它們適當地新增至 Master Database 類別。這會改善所有組織的篩選準確性。



#### 注意

內部網路網站不會由 WebCatcher 傳送。這包含 IP 位址在 10.xxx.xxx.xxx、172.16.xxx.xxx 和 192.168.xxx.xxx 範圍中的所有網站。

3. 核取**傳送安全性的 URL** 以傳送在記錄資料庫中找到的所有安全性的 URL 的清單。
 

Websense, Inc. 會分析收到的安全性的 URL，以判斷「鍵盤側錄」、「惡意網站」、「網路釣魚」和「間諜軟體」類別中的網站活動。
4. 在**選擇最能代表您位置的國家/地區**下選擇記錄大部分活動的國家/地區。
5. 核取**儲存要傳送至 Websense 的資料複本**選項以儲存要傳送至 Websense, Inc. 的資料複本。
 

啓用此選項時，WebCatcher 會將資料儲存為 Websense\Reporter 目錄下的未加密 XML 檔案。這些檔案會加上日期與時間戳記。
6. 在**最大上載檔案大小**下指出檔案大小增加到多大時 (從 4096 KB 到 8192 KB) 就會將它傳送到 Websense。
 

請確認您的系統可透過 HTTP Post 發佈此大小的檔案。
7. 針對**每日啓動時間下限**，設定如果未達到該日的大小臨界值，WebCatcher 要傳送檔案的開始時間。
 

這可確保至少每天會從您的系統提交並清除資訊一次。
8. 如果 Log Server 電腦必須經過驗證後才能存取網際網路，則按一下**驗證**按鈕。如需顯示的**驗證**對話方塊的資訊，請參閱 [WebCatcher 驗證](#)，第 276 頁。
9. 按一下**套用**以儲存任何變更，然後停止並重新啓動 Log Server (請參閱 [停止和啓動 Log Server](#)，第 276 頁)。

## WebCatcher 驗證

相關主題：

- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [設定 WebCatcher](#)，第 274 頁
- ◆ [停止和啓動 Log Server](#)，第 276 頁

按一下 WebCatcher 標籤上的**驗證**後，會出現「驗證」對話方塊。

1. 如果 Log Server 電腦透過代理伺服器存取網際網路，請核取**使用代理伺服器**選項，然後提供所要求的資訊。

欄位	說明
代理伺服器名稱	輸入 Log Server 用來存取網際網路之代理伺服器的電腦名稱或 IP 位址。
代理伺服器連接埠	輸入代理伺服器用來進行通訊的連接埠號碼。

2. 如果 Log Server 電腦必須經過驗證後才能存取網際網路，則核取**使用基本驗證**選項，然後輸入用於驗證的使用者名稱和密碼。
3. 按一下**確定**來儲存任何變更並返回 WebCatcher 標籤。

## 停止和啓動 Log Server

相關主題：

- ◆ [Log Server Configuration 公用程式](#)，第 267 頁
- ◆ [設定 Log Server 連接](#)，第 268 頁

Log Server 會接收來自 Filtering Service 的資訊，並將它儲存在記錄資料庫中以用於產生報告。它會當做 Windows 服務來執行，通常會在安裝期間啓動，並在每次重新啓動電腦時啓動。

在 Log Server Configuration 公用程式中所做的變更必須在停止並重新啓動 Log Server 後才會生效。這可透過 Log Server Configuration 公用程式中的「連接」標籤輕鬆地完成。

1. 從 Windows 「開始」功能表選擇**程式集 > Websense > 公用程式 > Log Server Configuration**。
2. 在**連接**標籤中按一下**停止**。

3. 等待數秒鐘，然後按一下**啓動**來重新啓動 Log Server 服務。
4. 按一下**確定**以關閉 Log Server Configuration 公用程式。

**注意**

Websense 無法記錄在 Log Server 停止時所發生的網際網路存取。

## 記錄資料庫簡介

相關主題：

- ◆ [資料庫工作](#)，第 278 頁
- ◆ [管理記錄資料庫](#)，第 278 頁

Log Database 會儲存網際網路活動以及相關聯之 Websense 篩選動作的記錄。安裝時會建立包含目錄資料庫以及一個資料庫分割區的記錄資料庫。

**目錄資料庫**會針對各種需要存取記錄資料庫的 Websense 元件提供單一連接點：狀態頁面、Log Server、簡報報告，以及調查報告。其中包含資料庫分割區的支援資訊，包括類別名稱的清單、風險等級定義、使用者至群組的對應、資料庫工作等等。目錄資料庫也會維護所有可用資料庫分割區的清單。

**資料庫分割區**會儲存網際網路活動的個別 Log 記錄。對於 MSDE 使用者，系統會根據 Websense 軟體所建立的大小變換規則建立新的分割區。Microsoft SQL Server 使用者可以將記錄資料庫設定為根據分割區大小或日期間隔開始新的分割區 (如需詳細資訊，請參閱[設定變換選項](#)，第 280 頁)。

**注意**

只有在 Websense 軟體使用 Microsoft SQL Server 做為資料庫引擎時，才能使用以日期為基礎的分割區。

當分割區以大小為基礎時，會將所有內送 Log 記錄插入滿足大小規則的最新作用中分割區。如果分割區達到指定的大小上限，則會建立新的分割區來插入新的 Log 記錄。

當分割區以日期為基礎時，會根據建立的週期建立新的分割區。例如，如果變換選項為每月，則只要收到新月份的任何記錄，就會建立新的分割區。內送 Log 記錄會根據日期插入適當的分割區中。

資料庫分割區提供靈活性與效能上的優勢。例如，您可以從單一分割區產生報告，以限制必須進行分析的資料範圍來找出所要求的資訊。

## 資料庫工作

下列資料庫工作會隨著記錄資料庫一起安裝。SQL Server Agent 必須在執行資料庫引擎 (MSDE 或 Microsoft SQL Server) 的電腦上執行。

- ◆ 擷取、轉換以及載入 (ETL) 工作會持續執行，接收來自 Log Server 的資料、處理該資料，然後將其插入分割區資料庫中。必須執行 ETL 工作才能在記錄資料庫中處理 Log 記錄。
- ◆ 資料庫維護工作會執行資料庫維護工作並保留最佳效能。此工作預設會在夜晚執行。
- ◆ 網際網路瀏覽時間 (IBT) 工作會分析接收的資料，並針對每個用戶端計算瀏覽時間。IBT 資料庫工作是資源密集的，會影響大部分資料庫資源。此工作預設會在夜晚執行。

這些資料庫工作的某些方面可以在「設定」>「記錄資料庫」頁面上設定。如需詳細資訊，請參閱[記錄資料庫管理設定](#)，第 279 頁。

設定維護工作和網際網路瀏覽時間工作的開始時間時，請考慮系統資源與網路流量。這些工作是資源密集的，而且可能會減緩記錄和報告效能。

## 管理記錄資料庫

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定變換選項](#)，第 280 頁
- ◆ [設定網際網路瀏覽時間選項](#)，第 282 頁
- ◆ [設定完整 URL 記錄](#)，第 281 頁
- ◆ [設定記錄資料庫維護選項](#)，第 283 頁
- ◆ [設定記錄資料庫分割區建立](#)，第 284 頁
- ◆ [設定可用的分割區](#)，第 285 頁
- ◆ [檢視錯誤記錄](#)，第 286 頁

管理記錄資料庫包含控制資料庫作業的許多方面，包括：

- ◆ 資料庫工作所執行的作業及其執行時間。
- ◆ 建立新資料庫分割區的條件。
- ◆ 可用於報告的分割區。

這些及其他選項會提供給管理記錄資料庫重要控制權的人員。請參閱[記錄資料庫管理設定](#)，第 279 頁。

「超級管理員」會在建立角色時指定可以管理記錄資料庫的人。請參閱 [編輯角色](#)，第 221 頁。



#### 注意

建議限制有權變更記錄資料庫設定的管理員的數目。

## 記錄資料庫管理設定

相關主題：

- ◆ [管理記錄資料庫](#)，第 278 頁

可從「設定」標籤存取的 [報告 > 記錄資料庫](#) 頁面管理記錄資料庫作業的各個方面。這些選項會被分組為個別說明的邏輯區段。

您必須在某個區段中按一下「立即儲存」按鈕以啟動該區段中的變更。按一下 **立即儲存** 會立即記錄該區段中的變更。(不一定要同時按「全部儲存」。)

此頁面頂端會顯示作用中記錄資料庫的名稱，以及 **重新整理** 連結。這個「重新整理」連結會重新顯示目前在記錄資料庫頁面中的資訊。尚未利用適當的「立即儲存」按鈕套用的所有變更都會遺失。

如需使用每個區段的詳細指示，請按下方的適當連結。

- ◆ 資料庫變換選項：[設定變換選項](#)，第 280 頁。
- ◆ 完整 URL 記錄：[設定完整 URL 記錄](#)，第 281 頁。
- ◆ 網際網路瀏覽時間配置：[設定網際網路瀏覽時間選項](#)，第 282 頁。
- ◆ 維護配置：[設定記錄資料庫維護選項](#)，第 283 頁。
- ◆ 資料庫分割區建立：[設定記錄資料庫分割區建立](#)，第 284 頁。
- ◆ 可用的分割區：[設定可用的分割區](#)，第 285 頁。
- ◆ 錯誤記錄活動：[檢視錯誤記錄](#)，第 286 頁。

## 設定變換選項

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定網際網路瀏覽時間選項](#)，第 282 頁
- ◆ [設定完整 URL 記錄](#)，第 281 頁
- ◆ [設定記錄資料庫維護選項](#)，第 283 頁
- ◆ [設定記錄資料庫分割區建立](#)，第 284 頁
- ◆ [設定可用的分割區](#)，第 285 頁
- ◆ [檢視錯誤記錄](#)，第 286 頁

使用「報告」>「記錄資料庫」頁面（「設定」標籤）的**資料庫變換選項**區段指定記錄資料庫建立新資料庫分割區（變換）的時間。

1. 使用**變換間隔**選項指出資料庫分割區是根據大小 (MB) 還是日期 (週或月) 來變換，這取決於所使用的資料庫引擎。

MSDE 使用者必須使用大小變換選項。Microsoft SQL Server 使用者可以選擇使用大小或日期。

- 若是根據日期變換，選取**週**或**月**做為測量單位，然後指定在建立新的資料庫分割區之前，要在資料庫分割區中保留多少完整的行事曆週或月。
- 若是根據大小變換，選取 **MB**，然後指定資料庫大小必須達到多少 MB 後才開始變換。

**Microsoft SQL Server** 使用者可以設定的大小最高可達 204800 MB。

**MSDE** 使用者必須將大小設定在 100 MB 和 1536 MB 之間。



### 注意

如果變換在一天中的忙碌時段開始，則變換過程中效能可能會下降。

為避免出現這種情況，有些環境選擇自動變換到較長的時段或較大的大小上限。接著，他們會定期執行手動變換以免發生自動變換。如需手動變換的資訊，請參閱[設定記錄資料庫分割區建立](#)，第 284 頁。

請記住，不建議使用非常大的個別分割區。如果資料沒有分割成多個較小的分割區，報告效能可能會下降。

建立新的分割區資料庫時，系統會針對分割區自動啓用所依據的報告（請參閱[設定可用的分割區](#)，第 285 頁）。

2. 按一下**立即儲存**來啓動資料庫變換選項的變更。



## 設定完整 URL 記錄

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定變換選項](#)，第 280 頁
- ◆ [設定網際網路瀏覽時間選項](#)，第 282 頁
- ◆ [設定記錄資料庫維護選項](#)，第 283 頁
- ◆ [設定記錄資料庫分割區建立](#)，第 284 頁
- ◆ [設定可用的分割區](#)，第 285 頁
- ◆ [檢視錯誤記錄](#)，第 286 頁

「報告」>「記錄資料庫」頁面（「設定」標籤）的**完整 URL 記錄**區段可讓您決定每個網際網路要求要記錄的 URL 部分。



### 注意

在高流量網路中，管理記錄資料庫大小是一項重要事務。停用「完整 URL 記錄」選項是一種控制資料庫大小和增加容量的方法。

1. 標記**記錄每個要求網站的完整 URL**來記錄整個 URL，包括網域 (www.domain.com) 和特定頁面的路徑 (/products/productA.html)。



### 重要

如果您計畫產生即時掃描活動的報告，請啟動完整 URL 記錄 (請參閱[即時掃描活動的報告](#)，第 134 頁)。否則報告只能顯示已分類網站的網域 (www.domain.com)，即使該網站中的個別頁面屬於不同類別或包含不同威脅也一樣。

如果未核取此選項，則只會記錄網域名稱。這樣會使資料庫更小，但提供的細節會減少。

記錄完整 URL 會產生更大的記錄資料庫，但是會提供更多細節。

如果在啟動合併時啟動完整 URL 記錄，則合併的記錄會包含合併群組中的第一筆記錄的完整 URL。如需詳細資訊，請參閱[設定合併選項](#)，第 272 頁。

2. 按一下**立即儲存**來啟動完整 URL 記錄選項的變更。

## 設定網際網路瀏覽時間選項

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定變換選項](#)，第 280 頁
- ◆ [設定完整 URL 記錄](#)，第 281 頁
- ◆ [設定記錄資料庫維護選項](#)，第 283 頁
- ◆ [設定記錄資料庫分割區建立](#)，第 284 頁
- ◆ [設定可用的分割區](#)，第 285 頁
- ◆ [檢視錯誤記錄](#)，第 286 頁

網際網路瀏覽時間 (IBT) 報告可以檢視使用者在網路網路上所花費的時間。夜晚的資料庫工作會根據當天收到的新 Log 記錄計算每個用戶端的瀏覽時間。在「設定」>「記錄資料庫」頁面的**網際網路瀏覽時間配置**區段中設定瀏覽時間選項。

### 1. 為 IBT 資料庫工作選擇工作開始時間。

此工作所需的時間和系統資源會隨著每天記錄的資料數量而改變。最好在與夜晚維護工作不同的時間執行此工作 (請參閱[設定記錄資料庫維護選項](#)，第 283 頁)，並且選擇網路緩慢的時間，從而將對產生報告的影響降至最低。

IBT 資料庫工作是資源密集的，會影響大部分資料庫資源。如果啓用此項工作，則需要設定開始時間，使其不會干擾資料庫系統處理排程報告與其他重要作業的能力。同時還要監控工作，以判斷是否需要功能更強的硬體來滿足所有處理需求。

### 2. 為**閱讀時間臨界值**設定讀取特定網站的平均分鐘數。

閱讀時間臨界值會為網際網路瀏覽時間報告定義瀏覽工作階段。開啓瀏覽器會產生 HTTP 流量。這表示開始瀏覽工作階段。只要在此設定的時間內繼續產生 HTTP 流量，就會開啓此工作階段。一旦在此時間內沒有通過任何 HTTP 流量，就會將此瀏覽工作階段視為關閉。只要再次產生 HTTP 流量，就會開始新的瀏覽工作階段。



#### 注意

最好盡量少變更「閱讀時間臨界值」，並在您每次進行變更時開始新的資料庫分割區。

為避免報告上的資料發生不一致，從資料庫分割區產生使用相同「閱讀時間臨界值」的 IBT 報告。

請注意，某些網站使用自動重新整理技術頻繁地更新資訊。其中一個範例是旋轉最新新聞顯示的新聞網站。這個重新整理會產生新的 HTTP 流量。因此，如果此種網站保持開啓，則每次網站重新整理時，都會產生新的 Log 記錄。在 HTTP 流量中沒有缺口，因此不會關閉瀏覽器工作階段。

3. 設定**最後閱讀時間**值來計算結束瀏覽工作階段前，讀取最後一個網站所花費的時間。  
當 HTTP 流量的時間間隔大於閱讀時間臨界值時，就會結束工作階段，並將「最後閱讀時間」的值加入工作階段時間。
4. 按一下**立即儲存**來啟動網際網路瀏覽時間配置的變更。

## 設定記錄資料庫維護選項

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定變換選項](#)，第 280 頁
- ◆ [設定網際網路瀏覽時間選項](#)，第 282 頁
- ◆ [設定完整 URL 記錄](#)，第 281 頁
- ◆ [設定記錄資料庫分割區建立](#)，第 284 頁
- ◆ [設定可用的分割區](#)，第 285 頁
- ◆ [檢視錯誤記錄](#)，第 286 頁

使用「報告」>「記錄資料庫」頁面（「設定」標籤）的**維護配置**區段控制資料庫處理的某些方面，例如執行資料庫維護工作的時間、執行的部分工作，以及刪除資料庫分割區和錯誤記錄。

1. 為**維護開始時間**選取一天中執行資料庫維護工作的時間。  
此工作所需的時間和系統資源會隨著在此區域中選取的工作而改變。若要將對於其他活動和系統的影響降至最低，最好在網路緩慢的時段執行此工作，而且執行時間與設定 IBT 工作的時間不同（請參閱[設定網際網路瀏覽時間選項](#)，第 282 頁）。
2. 核取**自動刪除分割區**，然後指定刪除分割區前的天數（2 天到 365 天）。



### 警告

刪除分割區之後，資料便無法復原。如需其他刪除分割區的方式，請參閱[設定可用的分割區](#)，第 285 頁。

3. 核取**啓動自動重新建立索引**，然後選取一週中的某一天以在每個星期自動執行此項處理。  
重新建立資料庫的索引對於維護資料庫的完整性以及最佳化報告速度相當重要。



### 重要

最好在網路比較空閒的時間執行此項處理。重新建立資料庫分割區的索引相當耗費資源與時間。不應在處理期間執行報告。

- 核取**刪除失敗批次檔前的天數**，然後輸入刪除任何失敗批次檔前的天數 (0 天到 90 天)。

如果未核取此選項，失敗批次檔會無限期地保留以供後續處理之用。

如果磁碟空間不足或資料庫權限不當，則無法將 Log 記錄插入資料庫，而是將這些記錄標示為**失敗批次檔**。這些批次檔通常可以成功經過重新處理，並在夜晚資料庫維護工作期間插入資料庫。

不過，如果尚未解決磁碟空間或權限問題，這個重新處理則無法成功。此外，如果未選取**處理未處理批次檔**，則絕不會重新處理失敗批次檔。這些批次檔會在此處所指定的時間後被刪除。

- 核取**處理未處理批次檔**，讓夜晚的資料庫維護工作重新處理所有失敗批次檔。如果未核取此選項，則絕不會重新處理失敗批次檔。這些批次檔會在以上指定的時間後被刪除 (如果有)。

- 核取**刪除錯誤記錄前的天數**，然後輸入從目錄資料庫刪除資料庫錯誤記錄前的天數 (0 天到 90 天)。

如果未核取此選項，就會無限期地保留錯誤記錄。

- 按一下**立即儲存**來啟動維護配置選項的變更。

## 設定記錄資料庫分割區建立

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定變換選項](#)，第 280 頁
- ◆ [設定網際網路瀏覽時間選項](#)，第 282 頁
- ◆ [設定完整 URL 記錄](#)，第 281 頁
- ◆ [設定記錄資料庫維護選項](#)，第 283 頁
- ◆ [設定可用的分割區](#)，第 285 頁
- ◆ [檢視錯誤記錄](#)，第 286 頁

使用「報告」>「記錄資料庫」頁面（「設定」標籤）的**資料庫分割區建立**區段來定義新資料庫分割區的特性，例如位置和大小選項。此區域也可讓您立即建立新的分割區，而不用等待計畫的變換（請參閱[設定變換選項](#)，第 280 頁）。

- 輸入**檔案路徑**來建立新資料庫分割區的**資料**和**記錄**檔案。
- 在**初期大小**下，針對新資料庫分割區的**資料**和**記錄**檔案設定初期的檔案大小 (100 MB 到 204800 MB)。

**Microsoft SQL Server 使用者**：可接受的範圍為 100 - 204800

**MSDE 使用者：**可接受的範圍為 100 - 1500



### 注意

最佳作法建議計算一段時間的平均分割區大小。然後將初期大小更新為該值。這個方法會將必須擴充分割區的次數降至最低，並釋放資源來處理分割區中的資料。

3. 在**增加容量**下設定需要額外空間時，分割區的**資料**和**記錄**檔案大小的增量 (以 MB 為單位)。

**Microsoft SQL Server 使用者：**可接受的範圍為 1 - 999999

**MSDE 使用者：**可接受的範圍為 1 - 450

4. 按一下**立即儲存**來實行輸入的路徑、大小，以及增加容量。  
在這些變更之後建立的資料庫分割區會使用新的設定
5. 按一下**立即建立**在下次 ETL 工作執行 (請參閱**資料庫工作**，第 278 頁) 時建立新的分割區 (不管自動變換設定為何)。此程序通常需要幾分鐘的時間。  
若要讓新的分割區使用在此區段中進行的變更，請務必按一下**立即儲存**，然後再按一下**立即建立**。  
定期在內容窗格中按一下「重新整理」連結。建立程序完成時，「可用的分割區」區域將會顯示新的分割區。

## 設定可用的分割區

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定變換選項](#)，第 280 頁
- ◆ [設定網際網路瀏覽時間選項](#)，第 282 頁
- ◆ [設定完整 URL 記錄](#)，第 281 頁
- ◆ [設定記錄資料庫維護選項](#)，第 283 頁
- ◆ [設定記錄資料庫分割區建立](#)，第 284 頁
- ◆ [檢視錯誤記錄](#)，第 286 頁

「報告」>「記錄資料庫」頁面 (「設定」標籤) 的**可用的分割區**區段會列出所有可用於報告的資料庫分割區。此清單會顯示所涵蓋的日期，以及每個分割區的大小和名稱。

使用此清單控制要包含在報告中的資料庫分割區，以及選取各個要刪除的分割區。

1. 核取每個要包含在報告中的分割區旁邊的**啟動**。

如果適當，使用清單上方的**全選**和**全都不選**選項。

您必須至少為報告啟動一個分割區。使用**全都不選**選項一次停用所有分割區，然後就可以只啟動部分分割區。

產生報告和速度報告處理時，使用這些選項來管理資料被分析的程度。例如，如果打算產生一系列的六月報告，則取消選取六月日期之外的所有分割區。



### 重要

這個選項會影響排程的報告以及以互動方式執行的報告。為避免產生沒有資料的報告，請確認在排程要執行的報告時，啟動相關的分割區。

2. 如果不再需要某個分割區，按一下該分割區名稱旁邊的**刪除**選項。下次夜晚的資料庫維護工作執行時，會實際刪除該分割區。



### 警告

請小心使用此選項。您無法復原刪除的分割區。

刪除已過時的分割區會將記錄資料庫中的分割區數目降至最低，這樣會增進資料庫和報告的效能。若有需要，使用此「刪除」選項刪除個別的分割區。如果想根據排程刪除舊的分割區，請參閱[設定記錄資料庫維護選項](#)，第 283 頁。

3. 按一下**立即儲存**來啟動可用分割區選項的變更。

## 檢視錯誤記錄

相關主題：

- ◆ [記錄資料庫管理設定](#)，第 279 頁
- ◆ [設定變換選項](#)，第 280 頁
- ◆ [設定網際網路瀏覽時間選項](#)，第 282 頁
- ◆ [設定完整 URL 記錄](#)，第 281 頁
- ◆ [設定記錄資料庫維護選項](#)，第 283 頁
- ◆ [設定記錄資料庫分割區建立](#)，第 284 頁
- ◆ [設定可用的分割區](#)，第 285 頁

使用「報告」>「記錄資料庫」頁面（「設定」標籤）的**錯誤記錄活動**區段來檢視工作在 Websense 記錄資料庫上執行期間所發生的錯誤記錄（請參閱[資料庫工作](#)，第 278 頁）。此資訊可能有助於疑難排解。

選擇下列某個選項：

- ◆ 從下拉式清單中選擇一個數目來顯示多個錯誤記錄項目。
- ◆ 選擇**全部檢視**來顯示所有錯誤記錄項目。
- ◆ 選擇**不檢視**來隱藏所有錯誤記錄項目。

## 設定調查報告

相關主題：

- ◆ [資料庫連接與報告預設值](#)，第 287 頁
- ◆ [顯示與輸出選項](#)，第 289 頁

調查報告可讓您以互動方式向下查看貴組織之網際網路使用量的相關資訊。請參閱[調查報告](#)，第 102 頁。

能夠透過主要調查報告頁面上的「選項」連結來修改用於報告的記錄資料庫。也可使用它來修改細節報告的預設檢視。請參閱[資料庫連接與報告預設值](#)，第 287 頁。

**wse.ini** 檔可讓您設定某些預設值來檢視摘要報告與多層級報告。它也讓您控制報告輸出為 PDF 時所使用的預設頁面大小。請參閱[顯示與輸出選項](#)，第 289 頁。

## 資料庫連接與報告預設值

相關主題：

- ◆ [設定調查報告](#)，第 287 頁
- ◆ [顯示與輸出選項](#)，第 289 頁
- ◆ [摘要報告](#)，第 103 頁
- ◆ [多層級摘要報告](#)，第 106 頁

使用[調查報告 > 選項](#)頁面連接到所需的記錄資料庫，並控制調查報告細節檢視的預設值。

對此頁面所做的變更會影響您的報告。其他管理員，甚至是登入自行報告的使用者，可以針對自己的報告活動變更這些值。

1. 選擇記錄資料庫以使用於調查報告。
  - 核取**檢視目錄資料庫**來連接到 Log Server 正在記錄的記錄資料庫。繼續進行步驟 2。
  - 若要存取不同的記錄資料庫：
    - a. 取消核取**檢視目錄資料庫**選項。

- b. 輸入下列資訊來識別所需的記錄資料庫 ( 調查報告可以從 6.3.x 版或 7.0 版資料庫產生 )。

欄位	說明
伺服器	輸入記錄資料庫所在的電腦名稱或 IP 位址。
資料庫	輸入記錄資料庫的名稱。
使用者 ID	為有權存取資料庫的帳戶輸入使用者 ID。 如果已安裝 Log Server 使用信任連接來存取記錄資料庫，請將此欄位留空。 如果您不確定，輸入 <b>sa</b> 。這是 MSDE 的預設使用者 ID，也是 Microsoft SQL Server 中的預設管理員 ID。
密碼	輸入指定使用者 ID 的密碼。若是信任的連接，請將此欄位留空。

2. 為細節報告選取下列預設值。

欄位	說明
選取預設的「調查報告」日期範圍	選擇初始摘要報告顯示的日期範圍。
選擇預設細節報告格式	選擇 <b>智慧欄位選擇</b> 來顯示為要報告的資訊設定之預設欄位的細節報告。 選擇 <b>自訂欄位選擇</b> 在所有細節報告上指定初始顯示的確實欄位。使用「可選擇的欄位」清單來選擇。 使用者可以修改產生報告後顯示的欄位。
選取報告類型	選擇是否要開啓細節報告，並在一開始顯示： <ul style="list-style-type: none"> <li>• <b>細節</b>：每筆記錄都會出現在單獨的列上，而且可以顯示時間。</li> <li>• <b>摘要</b>：將共用公共元素的所有記錄分組成一個項目。取決於要報告的資訊，特定的元素會有所不同。一般而言，測量之前的最右側欄位會顯示摘要的元素。無法顯示時間。</li> </ul>
可選擇的欄位 / 目前報告	在「可選擇的欄位」清單中選取一個欄位名稱，然後按一下適當的箭頭將其移到「目前報告」清單中。在「目前報告」清單上最多可以有 7 個欄位。 在「目前報告」清單包含所有用於初始細節報告的欄位之後，設定欄位的順序。在清單中選取一個項目，然後使用向上和向下箭頭按鈕變更其位置。

3. 按一下**儲存選項**立即儲存所有變更。



## 顯示與輸出選項

相關主題：

- ◆ [設定調查報告，第 287 頁](#)
- ◆ [資料庫連接與報告預設值，第 287 頁](#)
- ◆ [輸出至檔案，第 123 頁](#)

您可以調整某些報告選擇和報告結果在摘要和多層級調查報告中顯示的方式，並在報告輸出成 PDF 格式時指定預設頁面大小。

這些調查報告配置選項在 **wse.ini** 檔中設定。預設位置為：

C:\Program Files\WebSense\webroot\Explorer\wse.ini

下表列出的參數會影響調查報告的顯示和輸出、每個參數控制的行為及其預設值（「請勿」修改 wse.ini 檔中的其他任何設定）。

參數	說明
maxUsersMenu	資料庫的使用者數目必須少於這個值 (預設為 5000)，才能將「使用者」顯示為「網際網路使用者」清單中的報告選擇。
maxGroupsMenu	資料庫的群組數目必須少於這個值 (預設為 3000)，才能將「群組」顯示為「網際網路使用者」清單中的報告選擇。 <b>注意：</b> 「群組」必須有 2 個或多個群組，才會出現在「網際網路使用者」清單中。 「網域」也必須有 2 個或多個網域，才會出現在「網際網路使用者」清單中。網域沒有最大值。
maxUsersDrilldown	此參數會搭配 warnTooManyHits 參數使用，以控制使用以紅色顯示「使用者」選項的時機。紅色字母表示選取「使用者」將會產生非常大的報告，產生報告所花費的時間可能很長。 如果使用者的數目多於這個值 (預設為 5000)，而且點選次數高於 warnTooManyHits 值，則「使用者」選項在各個下拉式清單和值清單中就會顯示為紅色。 如果使用者的數目多於這個值，但點選次數低於 warnTooManyHits 值，則「使用者」選項會以正常色彩顯示，因為產生的報告將會是比較合理的大小。
maxGroupsDrilldown	如果預期的報告所包括之群組的數目多於這個值 (預設為 2000)，則「群組」選項在向下查看期間會顯示為紅色。紅色字母表示選取「群組」將會產生非常大的報告，產生報告所花費的時間可能很長。

參數	說明
warnTooManyHits	<p>此參數會搭配 maxUsersDrilldown 參數使用，以控制使用以紅色顯示「使用者」選項的時機。</p> <p>如果使用者的數目多於 maxUsersDrilldown 值，但點選次數低於此值（預設為 10000），則「使用者」選項就不會顯示成紅色。</p> <p>如果使用者的數目多於 maxUsersDrilldown 值，而且點選次數高於此值，則「使用者」選項就會顯示成紅色。紅色字母表示選取「使用者」將會產生非常大的報告，產生報告所花費的時間可能很長。</p>
hitsPerPage	<p>這會決定每頁顯示的最大項目數（預設為 100）。（這不會影響列印的報告。）</p>
maxOutputBufferSize	<p>這是可以顯示在主要調查報告頁面上的最大資料數（以位元組為單位）。如果要求的資料超出此限制（預設為 4000000 或 4 百萬位元組），就會出現一個訊息，敘述某些沒有顯示的結果會在報告尾端以紅色顯示。</p> <p>如果這是一個問題，那麼值越大，可在一個報告中顯示的資料也越多。不過，如果碰到記憶體錯誤，請考慮減少此值。</p>
sendMulti	<p>根據預設，此選項是停用的 (0)。將其設定為 1 (啟動) 可將非常大的排程細節報告分為多個各含 10,000 列的檔案。代表一個報告的檔案會經過壓縮，並傳送給電子郵件收件人。這些報告檔案可以使用最常見的檔案壓縮公用程式解壓縮。</p>
maxSlices	<p>這是圓形圖中不同片段的最大數目（預設為 6），包括「其他」片段，這會結合所有沒有個別片段的值。</p>
timelineCompressionThreshold	<p>當「群組相似點選次數/檢視所有點選次數」選項可用時，此選項僅用於「使用者每日/月活動」。此報告會折疊此處所設定之秒數（預設為 10）內發生的相同類別之所有點選次數。</p>
PageSize	<p>調查報告結果可以輸出成可攜式文件格式 (PDF)，以便輕鬆發佈或列印。頁面大小（預設為 Letter）可以是：</p> <ul style="list-style-type: none"> <li>• A4 (8.27 X 11.69 英寸)</li> <li>• Letter (8.5 X 11 英寸)</li> </ul>

## 自行報告

相關主題：

- ◆ [設定報告偏好設定](#)，第 265 頁
- ◆ [存取自行報告](#)，第 124 頁
- ◆ [調查報告](#)，第 102 頁

自行報告是一種功能，可啟動該功能讓使用者檢視其個人網際網路活動的調查報告。這可讓他們查看要收集與監控哪種類型的相關資訊，以配合許多國家/地區的政府法規。此外，檢視自己的活動可能會鼓勵某些使用者改變他們的瀏覽習慣，以符合組織的網際網路政策。



### 注意

只有在 Websense Manager 和報告元件安裝在 Windows 作業系統上時，才能使用自行報告。如需其他資訊，請參閱 [部署手冊](#)。

若要啟動自行報告：

1. 前往 **設定 > 一般 > 目錄服務**，然後設定利用使用者的網路認證驗證存取 Websense Manager 之使用者所使用的目錄服務。您可能要事先完成此動作，才能依使用者和群組名稱進行篩選。請參閱 [目錄服務](#)，第 56 頁。  
如果您的安裝包含多個 Policy Server，則必須登入每個 Policy Server，然後以適當目錄服務的資訊設定「目錄服務」頁面。
2. 前往 **設定 > 報告 > 偏好設定**，然後標記 **允許自行報告** 核取方塊。請參閱 [設定報告偏好設定](#)，第 265 頁。

啟動選項之後，必須提供使用者所需的資訊才能執行報告：

- ◆ 存取自行報告介面的 URL。提醒使用者可以將 URL 儲存為我的最愛或書籤，供日後使用。  
讀取關於 URL 的詳細資訊。
- ◆ 要在登入期間選取的 Policy Server。  
只有一個 Policy Server 的網路不需要這個動作。包含多個 Policy Server 的網路則需要向使用者提供 Policy Server 的 IP 位址，並設定為與驗證其網路登入的目錄服務進行通訊。這也是在安裝 Log Server 時指定的 Policy Server。
- ◆ 要在登入期間使用的使用者名稱和密碼。  
自行報告使用者必須在登入期間輸入其網路使用者名稱和密碼。

存取自行報告介面的 URL 為：

```
https://<ServerIP>:9443/mng/login/pages/  
selfReportingLogin.jsf
```

使用執行 Websense Manager 之電腦的 IP 位址來代替 <ServerIP>。

管理員和使用者也可以開啓 Websense Manager 登入頁面，然後按一下「自行報告」連結來存取自行報告登入頁面。

如果網路包含**多個 Policy Server**，則必須通知使用者要在自行報告登入期間選擇哪一個 Policy Server。

# 14

## 網路配置

相關主題：

- ◆ [硬體配置](#)，第 294 頁
- ◆ [Network Agent 配置](#)，第 295 頁
- ◆ [驗證 Network Agent 配置](#)，第 301 頁

當您以單機模式 (未整合代理或防火牆產品) 執行 Websense 軟體時，Websense Network Agent 會啟用：

- ◆ 網際網路內容篩選
- ◆ 網路通訊協定與網際網路應用程式管理
- ◆ 頻寬管理
- ◆ 已傳送位元組的記錄

在整合的 Websense 軟體部署中，可能會有協力廠商產品負責處理將使用者要求路由傳送至 Websense 軟體以便篩選，以及將封鎖頁面路由傳送回用戶端。在此種環境中，可能依然會使用 Network Agent 來篩選非 HTTP 要求，提供加強記錄詳細資料，或兩者都執行。

Network Agent 會持續監控整體網路使用情況，包括網路上傳送的位元組。代理程式會以預先定義的間隔，將使用摘要傳送至 Websense 軟體。每個摘要會包含開始時間與結束時間、已使用的總位元組，以及每個通訊協定使用的位元組。

根據預設，Network Agent 也會將頻寬使用資料提供給 Policy Server，並將篩選記錄資料提供給 Filtering Service。

Network Agent 通常會設定為檢視您網路中的所有流量。代理程式會區分下列兩者：

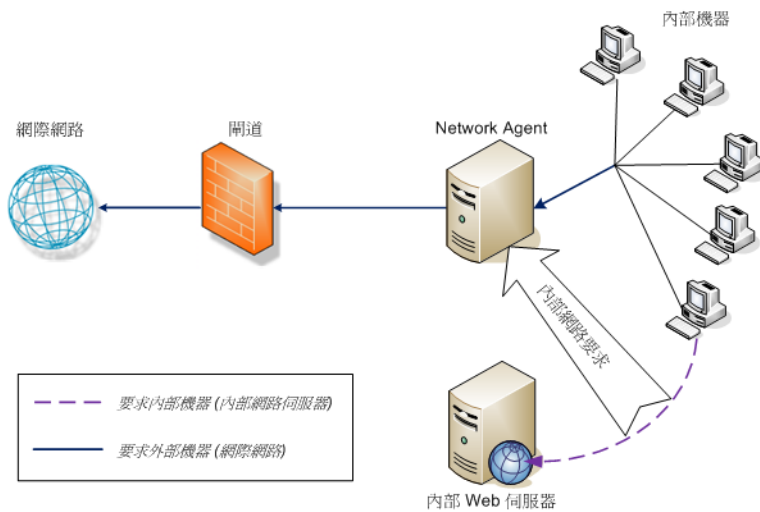
- ◆ 從內部電腦傳送到內部電腦的要求 (例如，對內部伺服器的點選)
- ◆ 從內部電腦傳送到外部電腦 (例如 Web 伺服器) 的要求 (例如，使用者網際網路要求)

後者是監控員工網際網路使用的主要目標。

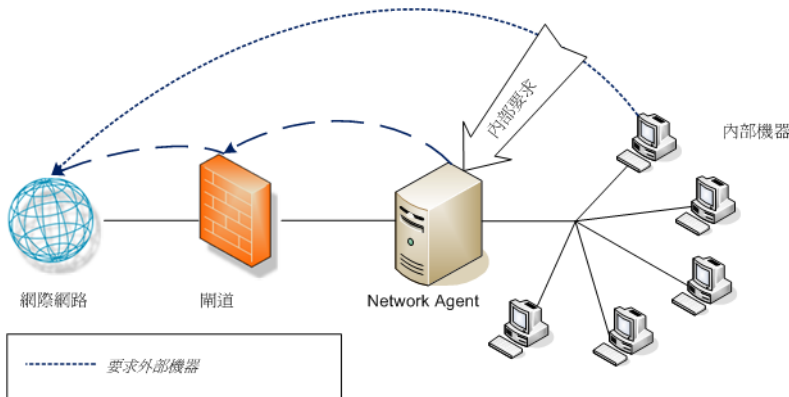
## 硬體配置

每個 Network Agent 實例會監控來自您識別為屬於您網路之電腦的流量。根據預設，它只會監控去往您指定之內部電腦的流量 (例如，內部 Web 伺服器)。

您可以自訂哪些內部電腦 (網路區段) 要由每個 Network Agent 實例監控，或甚至由 Network Agent 電腦上的每個網路介面卡 (NIC) 監控。



監控對內部電腦的要求



監控對外部電腦的要求

每個 Network Agent 實例必須：

- ◆ 放置在網路中適當位置，以便偵測往來所有受監控電腦的流量。
- ◆ 至少有 1 個網路卡專門用來監控流量。

Network Agent 可以安裝在具有多個網路卡的電腦上，也可以使用多個網路卡來監控要求與傳送封鎖頁面。如果您在 Network Agent 電腦上新增網路卡，請重新啟動 Network Agent 服務，然後設定新的網路卡 (請參閱 [設定網路卡設定](#)，第 298 頁)。

**注意**

若要判斷 Network Agent 是否可以看到網路區段內的流量，使用「網路流量偵測器」公用程式。請參閱 [驗證 Network Agent 配置](#)，第 301 頁。

有關放置 Network Agent 與網路卡需求的詳細資訊，請參閱 [部署手冊](#)。

有關設定 Network Agent 以監控內部網路要求、使用特定網路卡及執行加強記錄的詳細資訊，請參閱 [Network Agent 配置](#)，第 295 頁。

## Network Agent 配置

相關主題：

- ◆ [硬體配置](#)，第 294 頁
- ◆ [設定全域設定](#)，第 296 頁
- ◆ [設定本機設定](#)，第 297 頁
- ◆ [設定網路卡設定](#)，第 298 頁
- ◆ [新增或編輯 IP 位址](#)，第 300 頁

安裝 Network Agent 之後，使用 Websense Manager 設定其網路監控行為。Network Agent 設定分成兩個主要區域：

- ◆ **全域設定** 會影響所有 Network Agent 實例。使用這些設定來執行下列項目：
  - 識別網路上的電腦。
  - 列出在您網路中，Network Agent 應該監控其內送要求的電腦 (例如，內部 Web 伺服器)。
  - 指定頻寬計算與通訊協定記錄行為。
- ◆ **本機設定** 只會套用到所選的 Network Agent 實例。使用這些設定來執行下列項目：
  - 識別與每個 Network Agent 相關聯的是哪個 Filtering Service 實例。
  - 記錄這個 Network Agent 監控之電腦所使用的代理與快取。
  - 設定如何使用 Network Agent 電腦中的每個網路卡 (NIC) (用於監控要求、傳送封鎖頁面，或兩者皆執行)。

網路卡設定也會決定每個 Network Agent 實例監控哪個網路區段。

## 設定全域設定

相關主題：

- ◆ [硬體配置](#)，第 294 頁
- ◆ [設定本機設定](#)，第 297 頁
- ◆ [設定網路卡設定](#)，第 298 頁
- ◆ [新增或編輯 IP 位址](#)，第 300 頁

使用**設定 > Network Agent > 全域**頁面為 Network Agent 的所有實例定義基本監控與記錄行為。

**內部網路定義**清單可識別屬於您網路的電腦。根據預設，Network Agent 不會監控那些電腦之間傳送的流量 (內部網路通訊)。

預設會提供初始的項目集。您可以新增額外項目，或者編輯或刪除現有項目。

**要監控的內部流量**清單包括「內部網路定義」中您要 Network Agent 監控其流量的所有電腦。例如，這可能會包含內部 Web 伺服器，以協助您追蹤內部連線。

從網路中任何位置傳送到指定內部電腦的所有要求，都要加以監控。此清單預設為空白。

- ◆ 按一下**新增**以便將 IP 位址或範圍新增至適當的清單。如需詳細資訊，請參閱[新增或編輯 IP 位址](#)，第 300 頁。
- ◆ 若要編輯此清單中的項目，按一下 IP 位置或範圍。如需詳細資訊，請參閱[新增或編輯 IP 位址](#)，第 300 頁。
- ◆ 若要從清單中移除項目，標記 IP 位址或範圍旁的核取方塊，然後按一下**刪除**。

**其他設定**選項可讓您決定 Network Agent 計算頻寬使用量的頻率，以及是否記錄通訊協定流量及記錄頻率：

欄位	執行的工作
頻寬計算時間間隔	輸入 1 至 300 之間的數字，以秒為單位，指定 Network Agent 應該計算頻寬使用量的頻率。例如，如果項目設為 300，Network Agent 將會每 5 分鐘計算一次頻寬。 預設值是 10 秒。
定期記錄通訊協定流量	標記此選項可啟用「記錄時間間隔」欄位。
記錄時間間隔	輸入 1 至 300 之間的數字，以分鐘為單位，指定 Network Agent 記錄通訊協定的頻率。例如，如果項目設為 60，Network Agent 將會每隔一小時寫入記錄檔一次。 預設值是 1 分鐘。

完成變更之後，按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。



## 設定本機設定

相關主題：

- ◆ [硬體配置](#)，第 294 頁
- ◆ [設定全域設定](#)，第 296 頁
- ◆ [設定網路卡設定](#)，第 298 頁

使用 **設定 > Network Agent > 本機設定** 頁面以針對所選的 Network Agent 實例設定篩選行為、代理資訊及其他設定。所選 Network Agent 實例的 IP 位址會顯示在內容窗格的標題列中，並會在左側瀏覽窗格中反白顯示。

使用 **Filtering Service 定義** 設定來指定哪個 Filtering Service 要與所選 Network Agent 實例相關聯，以及在 Filtering Service 無法使用時應如何回應網際網路要求。

欄位	執行的工作
Filtering Service IP 位址	選取與這個 Network Agent 相關聯的 Filtering Service。
如果 Filtering Service 無法使用	選取 <b>允許</b> 以允許所有要求，或選取 <b>封鎖</b> 以封鎖所有要求，直到 Filtering Service 可以再次使用為止。預設值是「允許」。

若要確保使用者要求都能加以正確地監控、篩選並記錄，請使用 **代理與快取清單** 來指定與 Network Agent 通訊之所有代理或快取伺服器的 IP 位址。

- ◆ 按一下 **新增** 以便將 IP 位址或範圍新增至清單。如需詳細資訊，請參閱 [新增或編輯 IP 位址](#)，第 300 頁。
- ◆ 若要編輯此清單中的項目，按一下 IP 位置或範圍。
- ◆ 若要從清單中移除項目，標記 IP 位址或範圍旁的核取方塊，然後按一下 **刪除**。

使用 **網路介面卡** 清單來設定個別的網路卡。在 **名稱** 欄位中按一下網路卡，然後參閱 [設定網路卡設定](#)，第 298 頁，以獲得進一步指示。

如果您網路中的 HTTP 要求是通過非標準的连接埠，按一下 **進階 Network Agent 設定**，提供 Network Agent 的正確连接埠，以便監控。根據預設，HTTP 流量使用的连接埠是 **8080、80**。

本區段中的其他設定不應該變更，除非「Websense 技術支援部」指示您這麼做。

欄位	說明
模式	<ul style="list-style-type: none"> <li>• 無 (預設)</li> <li>• 一般</li> <li>• 錯誤</li> <li>• 細節</li> <li>• 頻寬</li> </ul>
輸出	<ul style="list-style-type: none"> <li>• 檔案 (預設)</li> <li>• 視窗</li> </ul>
連接埠	55870 (預設)

完成 Network Agent 設定的變更之後，按一下**確定**以快取變更。按一下**全部儲存**才能使變更生效。

## 設定網路卡設定

相關主題：

- ◆ [硬體配置](#)，第 294 頁
- ◆ [Network Agent 配置](#)，第 295 頁
- ◆ [設定網路卡的監控設定](#)，第 299 頁
- ◆ [新增或編輯 IP 位址](#)，第 300 頁

使用 **Network Agent > 本機設定 > 網路卡配置** 頁面來指定 Network Agent 如何使用每個可用的網路介面卡 (NIC) 以監控與管理網路使用。

**網路卡資訊** 區域會提供您所執行之變更的內容，顯示 **IP 位址**、網路卡簡短說明，以及網路卡名稱。使用此資訊來確保您設定的是正確的網路卡。

### 監控

在多個網路卡配置中，您可以指定一個網路卡監控網路流量，另一個網路卡提供封鎖頁面。至少有一個網路卡必須用來監控，而一個以上的網路卡可以監控流量。

使用**監控**區段來指示是否要**使用此網路卡監控流量**。

- ◆ 如果此網路卡沒有用來監控，取消選取該核取方塊，然後繼續進行下一個區段。
- ◆ 如果該網路卡用來監控，選取該核取方塊，然後按一下**設定**。接下來，您會進入「設定監控行為」頁面。如需指示，請參閱[設定網路卡的監控設定](#)，第 299 頁。

## 其他網路卡選項

除了設定監控選項之外，您也可以決定網路卡的其他行為：

1. 在「封鎖」之下，確認**封鎖網路卡**欄位中已列出適當的網路卡。如果您設定多個網路卡，那麼在這個欄位中，每一個網路卡的設定應該會顯示相同的值。也就是說，只有一個網路卡是用來封鎖的。
2. 如果您是以**單機**模式執行 Websense 軟體，那麼**篩選及記錄 HTTP 要求**就已經選取，而且無法變更。
3. 如果您已將 Websense 軟體與協力廠商裝置或應用程式整合，請使用**整合**選項來指示此 Network Agent 應該如何篩選及記錄 HTTP 要求。不適用您環境的選項會停用。
  - 選取**記錄 HTTP 要求**以改善 Websense 報告中的準確性。
  - 選取**篩選不是透過 HTTP 連接埠傳送的所有要求**以使用 Network Agent 僅篩選不是透過整合產品傳送的那些 HTTP 要求。
4. 在「通訊協定管理」之下，指示 Network Agent 是否應該使用此網路卡來篩選非 HTTP 通訊協定：
  - 核取**篩選非 HTTP 通訊協定要求**以啟動通訊協定管理功能。這可讓 Websense 軟體篩選網際網路應用程式與資料傳輸方法，例如用於即時訊息傳送、串流媒體、檔案共用、網際網路郵件等等。如需詳細資訊，請參閱[篩選類別和通訊協定](#)，第 34 頁和[使用通訊協定](#)，第 160 頁。
  - 核取**測量依通訊協定分類的頻寬使用量**以啟動 Bandwidth Optimizer 功能。Network Agent 會使用此網路卡來追蹤每個通訊協定或應用程式的網路頻寬使用量。如需詳細資訊，請參閱[使用 Bandwidth Optimizer 管理頻寬](#)，第 166 頁。

## 設定網路卡的監控設定

使用**本機設定 > 網路卡配置 > 監控清單**頁面來指定 Network Agent 電腦要透過所選的網路介面卡 (NIC) 監控哪些電腦。

1. 在「監控清單」之下，指定 Network Agent 要監控哪些要求：
  - **全部**：Network Agent 會使用所選網路卡監控它所看到的、來自所有電腦的要求。一般而言，這包含與目前 Network Agent 電腦或網路卡相同網路區段中的所有電腦。
  - **無**：Network Agent 不監控任何要求。
  - **特定**：Network Agent 僅監控「監控清單」中包含的網路區段。
2. 如果您選擇了「特定」，按一下**新增**，然後指定 Network Agent 應該監控的電腦 IP 位址。如需詳細資訊，請參閱[新增或編輯 IP 位址](#)，第 300 頁。



### 注意

您不能輸入重疊的 IP 位址範圍。如果範圍重疊，網路頻寬測量可能會不準確，而且以頻寬為基礎的篩選可能無法正確套用。

若要從清單中移除 IP 位址或網路範圍，核取適當的清單項目，然後按一下**刪除**。

3. 在「監控清單例外」之下，識別 Network Agent 不應監控的任何內部電腦。例如，Network Agent 可以忽略 CPM Server 所發出的要求。如此一來，CPM Server 要求將不會塞滿 Websense 記錄資料或任何狀態監控輸出。
  - a. 若要識別電腦，按一下**新增**，然後輸入它的 IP 位址。
  - b. 重複此程序以識別其他電腦。
4. 按一下**確定**來快取變更並返回「網路卡配置」頁面。按一下**全部儲存**才能使變更生效。

## 新增或編輯 IP 位址

相關主題：

- ◆ [設定全域設定](#)，第 296 頁
- ◆ [設定本機設定](#)，第 297 頁
- ◆ [設定網路卡設定](#)，第 298 頁

使用**新增 IP 位址**或**編輯 IP 位址**頁面，針對下列任何 Network Agent 清單進行變更：「內部網路定義」、「要監控的內部流量」、「代理與快取」、「監控清單」或「監控清單例外」。

- ◆ 當您新增或編輯 IP 位址範圍時，請確認它沒有與清單中任何現有項目 (單一 IP 位址或範圍) 重疊。
- ◆ 當您新增或編輯單一 IP 位址時，確認它屬於已經顯示在清單中的範圍。

若要新增 IP 位址或範圍：

1. 選取 **IP 位址**或 **IP 位址範圍**圓鈕。
2. 輸入有效的 IP 位址或範圍。
3. 按一下**確定**以返回上一個「Network Agent 設定」頁面。新的 IP 位址或範圍會顯示在適當的表格中。

若要返回上一頁但不快取您的變更，按一下**取消**。
4. 若有需要，針對其他 IP 位址重複此程序。

當您編輯現有的 IP 位址或範圍時，「**編輯 IP 位址**」頁面會顯示所選項目，該項目的正確圓鈕已經選取。執行任何必要的變更，然後按一下**確定**返回上一頁。

完成新增或編輯 IP 位址後，按一下「Network Agent 設定」頁面上的**確定**。按一下**全部儲存**才能使變更生效。

## 驗證 Network Agent 配置

在設定 Websense Manager 中的 Network Agent 之後，使用「網路流量偵測器」來確保 Websense 軟體可以看得到您網路上的電腦。

1. 請移至**開始 > 程式集 > Websense > 公用程式 > 網路流量偵測器**以啟動工具。
2. 從**網路介面卡**下拉式清單中選擇網路卡。
3. 檢查顯示在**監控網路範圍**清單中的位址，以確認列出所有適當的子網路。
4. 使用**新增子網路**和**移除子網路**按鈕變更要測試的網路部分。
5. 按一下**開始監控**。

「網路流量偵測器」會監控電腦透過網路傳送的資訊，以偵測網路中的電腦。**偵測到的電腦數量**清單會顯示偵測到的正在執行的電腦之數量。

6. 如需查看關於該工具偵測到的電腦的特定資訊，請在「監控網路範圍」清單中選擇子網路，然後按一下**檢視偵測電腦**。  
如果未列出特定電腦，請確認該電腦有產生網路流量。要執行此操作，請移至該電腦並啟動瀏覽器，然後瀏覽某個網站。接下來返回「網路流量偵測器」，並查看該電腦是否顯示在**偵測到的電腦**對話方塊中。
7. 完成測試網路流量能見度時，按一下**停止監控**。

如果有些電腦看不到：

- ◆ 檢閱網路配置與網路卡放置需求 (請參閱[硬體配置](#)，第 294 頁)。
- ◆ 在 Websense 軟體的**安裝手冊**中檢閱更詳細的網路配置資訊。
- ◆ 確認您已正確設定了監控網路卡 (請參閱[設定網路卡設定](#)，第 298 頁)。



# 15

## 疑難排解

使用本節可在聯繫「技術支援部」之前，找到常見問題的解決方案。

Websense 網站提供廣泛的知識庫，可從以下網址取得：[www.websense.com/global/en/SupportAndKB/](http://www.websense.com/global/en/SupportAndKB/)。可以根據關鍵字或參考編號來搜尋主題，或瀏覽最熱門的文章。

疑難排解指示分成下列各節：

- ◆ [安裝與訂閱問題](#)
- ◆ [Master Database 問題](#)，第 304 頁
- ◆ [篩選問題](#)，第 310 頁
- ◆ [Network Agent 問題](#)，第 313 頁
- ◆ [使用者識別問題](#)，第 315 頁
- ◆ [封鎖訊息問題](#)，第 324 頁
- ◆ [記錄、狀態訊息及警示問題](#)，第 327 頁
- ◆ [Policy Server 與 Policy Database 問題](#)，第 328 頁
- ◆ [委派管理問題](#)，第 329 頁
- ◆ [報告問題](#)，第 331 頁
- ◆ [疑難排解工具](#)，第 340 頁

### 安裝與訂閱問題

---

- ◆ [Websense 「狀態」顯示訂閱問題](#)，第 303 頁
- ◆ [更新之後，在 Websense Manager 中找不到使用者](#)，第 304 頁

### Websense 「狀態」顯示訂閱問題

需要有效的訂閱密碼才能下載 Websense Master Database 與執行網際網路篩選。如果您的訂閱已到期或無效，而且已超過 2 週未下載 Master Database 時，Websense 健全度監控會顯示警告。

- ◆ 確認您輸入的訂閱密碼與您收到的完全相同。密碼區分大小寫。
- ◆ 請確定您的訂閱尚未到期。請參閱[訂閱密碼](#)，第 306 頁。
- ◆ 確認已經在最近 2 週內成功下載過 Master Database。您可以在 Websense Manager 中檢查下載狀態：按一下「狀態」>「今日」頁面上的[資料庫下載](#)。如需協助疑難排解資料庫下載問題，請參閱[Master Database 未下載](#)，第 305 頁。

如果您已正確輸入密碼，但仍持續收到狀態錯誤，或者您的訂閱已到期，請聯繫 Websense, Inc. 或經過授權的代理商。

當您的訂閱到期時，Websense Manager 設定會判斷是否要針對所有使用者提供未經篩選的網際網路存取，或封鎖所有的網際網路要求。如需詳細資訊，請參閱[您的訂閱](#)，第 26 頁。

## 更新之後，在 Websense Manager 中找不到使用者

如果您已定義 Active Directory 作為您的目錄服務，在升級 Websense 軟體之後，使用者名稱可能不會出現在 Websense Manager 中。當使用者名稱含有非 UTF-8 字元集的字元時，就會發生此狀況。

為了支援 LDAP 3.0，Websense 安裝程式會在升級期間將字元集從 MBCS 變更爲 UTF-8。因此，無法正確識別含有非 UTF-8 字元的使用者名稱。

若要修正此問題，請手動將字元集變更爲 MBCS：

1. 在 Websense Manager 中，前往[設定值](#) > [目錄服務](#)。
2. 確認在頁面頂端附近的「目錄」下選取 **Active Directory (原生模式)**。
3. 按一下[進階目錄設定](#)。
4. 在「字元集」之下，按一下 **MBCS**。您可能必須向下捲動才會看到此選項。
5. 按一下[確定](#)來快取變更。按一下[全部儲存](#)才能使變更生效。

## Master Database 問題

- ◆ [正在使用初始篩選資料庫](#)，第 304 頁
- ◆ [Master Database 已超過 1 星期沒有更新](#)，第 305 頁
- ◆ [Master Database 未下載](#)，第 305 頁
- ◆ [Master Database 下載未在正確時間執行](#)，第 309 頁
- ◆ [聯繫「技術支援部」詢問資料庫下載問題](#)，第 309 頁

## 正在使用初始篩選資料庫

Websense Master Database 儲存了用來提供篩選網際網路內容之基礎的類別及通訊協定定義。



部分版本的 Master Database 已隨著您的 Websense 軟體安裝在每一個 Filtering Service 電腦上。從您輸入訂閱密碼開始，就會使用這個部分資料庫來啓用基本的篩選功能。

您必須下載完整的資料庫，才可執行完整的篩選。如需詳細資訊，請參閱 [Websense Master Database](#)，第 29 頁。

下載完整資料庫可能需要幾分鐘到 60 分鐘以上，這取決於多種因素，例如網際網路連線速度、頻寬、可用記憶體及可用磁碟空間。

## Master Database 已超過 1 星期沒有更新

Websense Master Database 儲存了用來提供篩選網際網路內容之基礎的類別及通訊協定定義。Websense 軟體會根據 Websense Manager 中定義的排程來下載 Master Database 的變更。根據預設，下載排程為每天執行一次。

若要手動開始資料庫下載：

1. 在 Websense Manager 中，前往**狀態 > 今天**頁面，然後按一下**資料庫下載**。
2. 按一下適當的 Filtering Service 實例旁的**更新**以便啓動資料庫下載，或按一下**全部更新**以啓動所有 Filtering Service 電腦上的下載。



### 注意

下載 Master Database 的更新之後，當資料庫載入本機記憶體時，CPU 使用量在短時間內可能高達 90% 或更高。建議在離峰時間執行下載。

3. 若要在資料庫下載時繼續工作，按一下**關閉**。  
隨時可以按一下**資料庫下載**按鈕來檢視下載狀態。

如果新版本的 Master Database 新增或移除類別或通訊協定，管理員在下載期間執行與類別或通訊協定相關的政策管理工作 (例如編輯類別集) 時，可能會收到錯誤。雖然這樣的更新很少見，但是最佳作法是在更新資料庫時，避免執行與類別及通訊協定相關的變更。

## Master Database 未下載

如果您無法成功下載 Websense Master Database：

- ◆ 請確認您已在 Websense Manager 中輸入正確的訂閱密碼，而且該密碼並未到期 ([訂閱密碼](#)，第 306 頁)。
- ◆ 驗證 Filtering Service 電腦是否可以存取網際網路 ([網際網路存取](#)，第 306 頁)。
- ◆ 檢查防火牆或代理伺服器設定，確保 Filtering Service 可以連線到 Websense 下載伺服器 ([驗證防火牆或代理伺服器設定](#)，第 307 頁)。
- ◆ 確認下載電腦上有足夠的磁碟空間 ([磁碟空間不足](#)，第 307 頁) 與記憶體 ([記憶體不足](#)，第 308 頁)。
- ◆ 尋找網路中可能阻擋下載連線的任何應用程式或設備，例如防毒軟體 ([限制應用程式](#)，第 309 頁)。

## 訂閱密碼

若要驗證輸入的訂閱密碼是否正確且未到期：

1. 在 Websense Manager 中，前往**設定 > 帳戶**。
2. 比較您從 Websense, Inc. 或代理商收到的密碼與**訂閱密碼**欄位中的密碼。密碼必須使用與密碼文件中相同的大小寫。
3. 檢查**密碼效期**旁邊的日期。如果資料已過期，聯繫您的代理商或 Websense, Inc. 以續訂您的訂閱。
4. 如果您變更了「設定」對話方塊中的密碼，按一下**確定**以啟動該密碼並啓用資料庫下載。

若要手動開始資料庫下載，或檢查最新資料庫下載狀態，按一下「狀態」>「今天」頁面頂端之工具列中的**資料庫下載**。

## 網際網路存取

爲了下載 Master Database，Filtering Service 電腦會傳送 **HTTP post** 指令給位於下列 URL 的下載伺服器：

```
download.websense.com
ddsdm.websense.com
ddsint.websense.com
portal.websense.com
my.websense.com
```

若要驗證 Filtering Service 是否具有與下載伺服器通訊所必需的網際網路存取權限：

1. 在執行 Filtering Service 的電腦上開啓瀏覽器。
2. 輸入下列 URL：

<http://download.websense.com/>

如果電腦可以開啓到該網站的 HTTP 連線，則會顯示重新導向頁面，然後瀏覽器會顯示 Websense 首頁。

如果此情況沒有發生，請確認電腦上的下列事項：

- 可以使用連接埠 80 來通訊，或使用您網路中供 HTTP 流量使用的連接埠來通訊
- 已正確設定爲執行 DNS 查閱
- 已設定爲使用任何必要的代理伺服器（請參閱[驗證防火牆或代理伺服器設定](#)，第 307 頁）

也請確定您的閘道不包含任何會封鎖來自 Filtering Service 電腦之 HTTP 流量的規則。

3. 使用下列其中一個方法，確認該電腦可以與下載網站通訊：

- 從命令提示字元輸入下列指令：  
ping download.websense.com

驗證此偵測是否收到來自下載伺服器的回應。

- 使用 Telnet 連線到 **download.websense.com 80**。如果您看到游標，且沒有錯誤訊息，表示您可以連線到下載伺服器。

## 驗證防火牆或代理伺服器設定

如果是透過要求驗證的防火牆或代理伺服器下載 Master Database，請確保 Filtering Service 電腦上的瀏覽器可以正確載入網頁。如果網頁正常開啓，但無法下載 Master Database，則檢查網頁瀏覽器的代理伺服器設定。

Microsoft Internet Explorer：

1. 選取**工具 > 網際網路選項**。
2. 開啓**連線標籤**。
3. 按一下**LAN 設定**。代理伺服器配置資訊會顯示在**代理伺服器**之下。  
將代理設定記下來。

Mozilla Firefox：

1. 選取**工具 > 選項 > 進階**。
2. 選取**網路標籤**。
3. 按一下**設定**。「連線設定」對話方塊會顯示該瀏覽器是否已設定為連線到代理伺服器。  
將代理設定記下來。

下一步，確認 Websense 軟體已設定使用相同的代理伺服器來執行下載。

1. 在 Websense Manager 中，前往**設定 > 資料庫下載**。
2. 確認已選擇了**使用代理伺服器或防火牆**，而且所列出的伺服器和連接埠是正確的。
3. 確認**驗證**設定是正確的。驗證使用者名稱與密碼，檢查拼字和大小寫。

如果 Websense 軟體必須提供驗證資訊，防火牆或代理伺服器必須設定為接受純文字或基本驗證。有關啓用基本驗證的資訊可以在 Websense [知識庫](#)取得。

如果在 Websense 軟體正常下載資料庫時，有防火牆限制網際網路存取，或限制可透過 HTTP 傳送的檔案大小，Websense 軟體將無法下載資料庫。若要判斷防火牆是否導致下載失敗，搜尋防火牆中可能封鎖下載的規則，若有必要，可變更 Websense Manager 中的下載時間 ([設定資料庫下載](#)，[第 30 頁](#))。

## 磁碟空間不足

Websense Master Database 儲存在 Websense **bin** 目錄 (預設為 /opt/Websense/bin or C:\Program Files\Websense\bin) 中。含有此目錄的磁碟必須有足夠空間以便下載壓縮的資料庫，也要有足夠空間讓資料庫解壓縮。

電腦上的可用磁碟空間應該至少需要 Master Database 大小的兩倍。隨著 Master Database 中的項目增加，成功下載所需的磁碟空間大小也會增加。一般而言，Websense, Inc. 建議下載磁碟機上至少要有 3 GB 的可用磁碟空間。

在 Windows 中，可使用「Windows 檔案總管」檢查可用磁碟空間：

1. 開啓「Windows 檔案總管」(不是 Internet Explorer) 中的**我的電腦**。
2. 選取安裝 Websense 軟體的磁碟機。根據預設，Websense 位於 C 磁碟機上。
3. 以滑鼠右鍵按一下並從彈出式功能表選取**內容**。
4. 在「一般」標籤上，驗證至少有 3 GB 的可用空間。如果磁碟機上的可用空間不足，刪除所有不必要的檔案，以釋放需要的空間。

在 Linux 系統上，使用 **df** 指令來驗證安裝 Websense 軟體的檔案系統中的可用空間量：

1. 開啓終端機工作階段。
2. 在提示中，輸入：

```
df -h /opt
```

Websense 軟體通常安裝在 /opt/Websense/bin 目錄中。如果安裝在其他位置，請使用該路徑。

3. 請確認至少有 3 GB 的可用空間。如果磁碟機上的可用空間不足，刪除所有不必要的檔案，以釋放需要的空間。

如果您確認有足夠的磁碟空間，但下載仍有問題，請嘗試停止所有 Websense 服務(請參閱[停止和啓動 Websense 服務](#)，第 245 頁)、刪除 **Websense.xfr** 與 **Websense** (無副檔名) 檔案、啓動服務，然後手動下載新資料庫。

## 記憶體不足

執行 Websense 軟體與下載 Master Database 所需的記憶體，會因為網路的大小而有所差異。例如，在小型網路中，建議所有平台都具備 2 GB 記憶體。

如需系統建議，請參閱[部署手冊](#)。

若要檢查 Windows 系統中的記憶體：

1. 開啓「工作管理員」。
2. 選取**效能**標籤。
3. 檢查可用的**實體記憶體**總數。
4. 如果安裝的記憶體少於 2 GB，請升級該電腦中的 RAM。

您也可以選取**控制台 > 系統管理工具 > 效能**以擷取資訊。

若要檢查 Linux 系統中的記憶體：

1. 開啓終端機工作階段。
2. 在提示中，輸入：  

```
top
```
3. 加總 **Mem: av** 與 **Swap: av**，計算出可用的記憶體總量。
4. 如果安裝的記憶體少於 2 GB，請升級該電腦中的 RAM。

## 限制應用程式

某些限制應用程式或設備，例如病毒掃描程式、大小限制應用程式或入侵偵測系統，可能會干擾資料庫下載。理想上，應該設定 Websense 軟體直接連到最後一個閘道，如此一來，它就不會連線到這些應用程式或設備。替代方案：

1. 停用與 Filtering Service 電腦以及 Master Database 下載位置有關的限制。  
如需有關變更裝置配置的指示，請參閱設備或軟體文件。
2. 嘗試下載 Master Database。

如果此變更沒有效果，重新設定應用程式或設備，使其包含執行 Filtering Service 的電腦。

## Master Database 下載未在正確時間執行

Filtering Service 電腦上的系統日期與時間可能設定錯誤。Websense 軟體會使用系統時鐘來決定下載 Master Database 的適當時間。

如果下載根本沒有執行，請參閱 *Master Database 未下載*，第 305 頁。

## 聯繫「技術支援部」詢問資料庫下載問題

如果在執行本節「說明」中的疑難排解步驟之後，依然有 Master Database 下載問題，請將下列資訊傳送到「Websense 技術支援部」：

1. 顯示在「資料庫下載」對話方塊中的確切錯誤訊息。
2. 嘗試下載資料庫之電腦的外部 IP 位址。
3. 您的 Websense 訂閱密碼。
4. 最後一次嘗試的日期與時間。
5. 已傳送的位元組數 (如果有的話)。
6. 開啓命令提示字元並執行 `nslookup` 查詢 `download.websense.com`。如果成功連線到下載伺服器，將 IP 位址傳回給「技術支援部」。
7. 開啓命令提示字元，並執行 `tracert` 追蹤 `download.websense.com`。如果成功連線到下載伺服器，將路由追蹤資訊傳送給「技術支援部」。
8. 在嘗試下載期間，Websense 下載伺服器上執行的封包追蹤或封包擷取。
9. 在相同的嘗試下載期間，網路閘道上執行的封包追蹤或封包擷取。
10. 來自 Websense `bin` 目錄的下列檔案：`websense.ini`、`eimserver.ini` 及 `config.xml`。

如需「技術支援部」聯絡資訊，請前往 [www.websense.com/SupportPortal/default.aspx](http://www.websense.com/SupportPortal/default.aspx)。

## 篩選問題

- ◆ [Filtering Service 沒有執行](#)，第 310 頁
- ◆ [無法使用 User Service](#)，第 311 頁
- ◆ [錯將網站分類為「資訊科技」](#)，第 311 頁
- ◆ [沒有對關鍵字進行封鎖](#)，第 311 頁
- ◆ [自訂或限制存取篩選器 URL 未按預期篩選](#)，第 312 頁
- ◆ [使用者無法如預期地存取通訊協定或應用程式](#)，第 312 頁
- ◆ [未如預期地封鎖 FTP 要求](#)，第 312 頁
- ◆ [Websense 軟體未套用使用者或群組政策](#)，第 313 頁
- ◆ [遠端使用者沒有經過正確政策的篩選](#)，第 313 頁

### Filtering Service 沒有執行

當 Filtering Service 沒有執行時，將無法篩選與記錄網際網路要求。

Filtering Service 可能在下列情況下停止執行：

- ◆ Filtering Service 電腦上的磁碟空間不足。
- ◆ 由於磁碟空間不足，導致 Master Database 下載失敗 (請參閱[Master Database 未下載](#)，第 305 頁)。
- ◆ 找不到 **websense.ini** 檔案或該檔案已損毀。
- ◆ 您將服務停止 (例如，在建立自訂封鎖頁面之後)，但未重新啟動。

如果您重新啟動多個 Websense 服務，但它們未以正確的順序啟動，Filtering Service 也可能顯示為已停止。當您重新啟動多個服務時，請記得先啟動 Policy Database、Policy Broker 及 Policy Server，然後才啟動其他 Websense 服務。

若要疑難排解這些問題：

- ◆ 確認 Filtering Service 電腦上至少有 3 GB 的可用磁碟空間。您可能必須移除未使用的檔案或增加額外容量。
- ◆ 瀏覽至 Websense **bin** 目錄 (預設為 C:\Program Files\Websense\bin 或 /opt/Websense/bin)，並確認您可以在文字編輯器中開啓 **websense.ini**。如果此檔案已經損毀，請以備份檔案取代它。
- ◆ 查看「Windows 事件檢視器」或 **websense.log** 檔案中來自 Filtering Service 的錯誤訊息 (請參閱[疑難排解工具](#)，第 340 頁)。
- ◆ 登出 Websense Manager，重新啟動 Websense Policy Server，然後重新啟動 Websense Filtering Service (請參閱[停止和啟動 Websense 服務](#)，第 245 頁)。請等待 1 分鐘之後再次登入 Websense Manager。

## 無法使用 User Service

當 User Service 未執行，或當 Policy Server 無法與 User Service 通訊時，Websense 軟體就無法正確套用以使用者為基礎的篩選政策。

如果您在重新啓動其他 Websense 服務之後重新啓動 Policy Server，User Service 可能會顯示已停止。若要修正此問題：

1. 重新啓動 Websense Policy Server 服務 (請參閱[停止和啓動 Websense 服務](#)，第 245 頁)。
2. 啓動或重新啓動 Websense User Service。
3. 關閉 Websense Manager。  
請等待 1 分鐘之後再次登入 Websense Manager。

如果前述步驟無法修復問題：

- ◆ 查看「Windows 事件檢視器」或 **websense.log** 檔案中來自 User Service 的錯誤訊息 (請參閱[疑難排解工具](#)，第 340 頁)。
- ◆ 瀏覽至 Websense **bin** 目錄 (預設為 C:\Program Files\Websense\bin 或 /opt/websense/bin)，並確認您可以在文字編輯器中開啓 **websense.ini**。如果此檔案已經損毀，請以備份檔案取代它。

## 錯將網站分類為「資訊科技」

Internet Explorer 4.0 版或更新版本可以接受從「網址」列中搜尋。當此選項啓用時，如果使用者僅在「網址」列輸入網域名稱 (例如，輸入 **websense**，而不是輸入 **http://www.websense.com**)，Internet Explorer 會將該項目視為搜尋要求，而不是網站要求。接著它會顯示最接近使用者尋找的網站，以及最符合的網站清單。

結果是，Websense 軟體會根據啓用的政策中的「資訊科技/搜尋引擎與入口網站」類別來允許、封鎖或限制要求，而不是根據要求之網站的類別。由於 Websense 軟體會根據要求之網站的類別來篩選，因此您必須關閉從「網址」列中搜尋：

1. 前往**工具 > 網際網路選項**。
2. 前往**進階**標籤。
3. 在「從網址列搜尋」之下，選取**不從網址列搜尋**。
4. 按一下**確定**。



### 注意

這些步驟適用於 Internet Explorer 5、6 及 7 版。

## 沒有對關鍵字進行封鎖

此問題有 2 個可能的原因：已選擇了**停用關鍵字封鎖**，或者其 URL 含有關鍵字的網站使用了 **post** 來傳送資料到您的 Web 伺服器。

若要確認已啓用關鍵字封鎖：

1. 在 Websense Manager 中，前往**設定 > 篩選**。

2. 在「一般篩選」下，檢查**關鍵字搜尋選項**清單。如果顯示**停用關鍵字封鎖**，從清單中選取另一個選項。如需有關可用選項的詳細資訊，請參閱 [設定 Websense 篩選設定](#)，第 49 頁。
3. 按一下**確定**來快取變更。按一下**全部儲存**才能使變更生效。

如果某網站使用 **post** 來傳送資料到您的 Web 伺服器，Websense 軟體會無法針對該 URL 辨識關鍵字篩選設定。除非您的整合產品可以識別透過 **post** 傳送的資料，否則使用者依然可以存取含有封鎖關鍵字的 URL。

若要檢視某網站是否使用 **post** 指令，可從瀏覽器中檢視該網站的原始檔。如果原始程式碼中包含類似 **<method=post>** 的字串，表示該網站是使用 **post** 來載入。

## 自訂或限制存取篩選器 URL 未按預期篩選

如果限制存取篩選器或自訂 URL 清單 (不論是已重新分類或未篩選) 中的 HTTPS URL 未如預期地篩選，表示可能有整合產品將 URL 轉換成 Filtering Service 無法辨識的格式。

非代理整合產品會將 URL 從網域格式轉譯為 IP 格式。例如，URL **https://<網域>** 會讀為 **https://<IP 位址>:443**。當此情況發生時，Filtering Service 就無法將從整合產品接收的 URL 與自訂 URL 或限制存取篩選器做比對，也就無法正確篩選該網站。

若要解決此問題，請使用自訂 URL 或限制存取篩選器來新增您要篩選之網站的 IP 位址及 URL。

## 使用者無法如預期地存取通訊協定或應用程式

如果您的網路包括 Microsoft ISA Server，有些驗證方法配置可能會導致與訊息應用程式的連線中斷。

如果啟動了「匿名驗證」以外的任何方法，當使用者要求應用程式連線時，代理伺服器會嘗試識別收到的資料封包。代理伺服器會無法識別資料封包，而且連線會中斷。這可能會使 Websense 通訊協定篩選活動產生偏差。

如果應用程式使用的連接埠被封鎖，也可能發生無法存取通訊協定或網際網路應用程式的情況。這可能發生在下列情況：

- ◆ 防火牆將連接埠封鎖。
- ◆ 封鎖的自訂通訊協定在其任意識別碼中包含了該連接埠 (做為單一連接埠或連接埠範圍的一部分)。

## 未如預期地封鎖 FTP 要求

當與 Check Point<sup>®</sup> 防火牆整合時，Websense 軟體需要在用戶端瀏覽器中啓用**資料夾檢視**，以便辨識與篩選 FTP 要求。

當資料夾檢視未啓用時，傳送到 FireWall-1 代理的 FTP 要求會傳送到 Websense 軟體，並帶有前置碼「**http://**」。因此，Websense 軟體會將這些要求視為 HTTP 要求來篩選，而不是 FTP 要求。



## Websense 軟體未套用使用者或群組政策

如果即使在已指派了使用者或群組政策之後，Websense 軟體仍然套用電腦或網路政策，或者預設政策，請參閱 [使用者識別問題](#)，第 315 頁。其他資訊可以透過 [知識庫](#) 取得。

## 遠端使用者沒有經過正確政策的篩選

如果使用者使用快取的網域認證 (網路登入資訊) 登入來存取網路，Websense 軟體會套用指派到該使用者的政策，或指派到使用者群組或網域的政策 (如果適用的話)。如果沒有任何指派到使用者、群組或網域的政策，或者如果使用者使用本機使用者帳戶登入電腦，Websense 軟體就會套用「預設」政策。

有時候，使用者並未經過使用者或群組政策或「預設」政策的篩選。當使用者使用本機使用者帳戶登入遠端電腦，而且遠端電腦的「媒體存取控制」(Media Access Control, MAC) 位址的最後部分與已經指派政策的網路內 IP 位址重疊時，就會發生此狀況。在此情況中，指派到該特定 IP 位址的政策就會套用到遠端使用者。

## Network Agent 問題

- ◆ [未安裝 Network Agent](#)，第 313 頁
- ◆ [Network Agent 沒有執行](#)，第 313 頁
- ◆ [Network Agent 沒有監控任何網路卡](#)，第 314 頁
- ◆ [Network Agent 無法與 Filtering Service 通訊](#)，第 314 頁

## 未安裝 Network Agent

若要啓用應用通訊協定篩選，必須要安裝 Network Agent。搭配某些整合，Network Agent 也用來提供更準確的記錄。

如果您是搭配整合產品來執行，而且不需要 Network Agent 通訊協定篩選與記錄，那麼您可以隱藏「未安裝任何 Network Agent」狀態訊息。如需指示，請參閱 [檢閱目前的系統狀態](#)，第 252 頁。

對於獨立安裝，必須安裝 Network Agent 才可監控及篩選網路流量。如需安裝指示，請參閱 [安裝手冊](#)，然後再參閱 [Network Agent 配置](#)，第 295 頁。

## Network Agent 沒有執行

若要啓用應用通訊協定篩選，必須要安裝 Network Agent。搭配某些整合，Network Agent 也用來提供更準確的記錄。

對於獨立安裝，必須執行 Network Agent，才可監控及篩選網路流量。

若要疑難排解此問題：

1. 檢查「Windows 服務」對話方塊 (請參閱 [「Windows 服務」對話方塊](#), 第 340 頁) 以查看是否已啟動 **Websense Network Agent** 服務。
2. 重新啟動 **Websense Policy Broker** 與 **Websense Policy Server** 服務 (請參閱 [停止和啟動 Websense 服務](#), 第 245 頁)。
3. 啟動或重新啟動 **Websense Network Agent** 服務。
4. 關閉 Websense Manager。
5. 請等待 1 分鐘, 然後再次登入 Websense Manager。

如果前述步驟無法修復問題：

- ◆ 查看 **Windows 事件檢視器** 中來自 Network Agent 的錯誤訊息 (請參閱 [Windows 事件檢視器](#), 第 340 頁)。
- ◆ 查看 **Websense.log** 檔案中來自 Network Agent 的錯誤訊息 (請參閱 [Websense 記錄檔](#), 第 341 頁)。

## Network Agent 沒有監控任何網路卡

Network Agent 必須至少與一個網路介面卡 (NIC) 相關聯, 才能監控網路流量。

如果您在 Network Agent 電腦上新增或移除網路卡, 必須更新您的 Network Agent 配置。

1. 在 Websense Manager 中, 前往 **設定**。
2. 在左側瀏覽窗格的 Network Agent 下, 選取 Network Agent 電腦的 IP 位址。
3. 確認所有選擇之電腦的網路卡都已列出。
4. 確認至少有一個網路卡設為監控網路流量。

如需詳細資訊, 請參閱 [Network Agent 配置](#), 第 295 頁。

## Network Agent 無法與 Filtering Service 通訊

Network Agent 必須能夠與 Filtering Service 進行通訊, 才可強制執行網際網路使用政策。

- ◆ 您是否變更了 Filtering Service 電腦的 IP 位址或重新安裝了 Filtering Service? 若是如此, 請參閱 [更新 Filtering Service IP 位址或 UID 資訊](#), 第 315 頁。
- ◆ Network Agent 電腦上是否有超過 2 個網路介面卡 (NIC)? 若是如此, 請參閱 [網路配置](#), 第 293 頁以確認您的 Websense 軟體設定。
- ◆ 您是否重新設定了連線到 Network Agent 的交換器? 若是如此, 請參考 [安裝手冊](#) 以確認您的硬體設定, 並請參閱 [Network Agent 配置](#), 第 295 頁以確認您的 Websense 設定。

如果上述這些都不適用, 請參閱 [設定本機設定](#), 第 297 頁, 獲得有關將 Network Agent 與 Filtering Service 相關聯的資訊。

## 更新 Filtering Service IP 位址或 UID 資訊

當 Filtering Service 解除安裝或重新安裝之後，Network Agent 不會自動更新 Filtering Service 的內部識別碼 (UID)。Websense Manager 會嘗試使用舊的 UID 查詢 Filtering Service，但該 UID 已經不存在了。

同樣地，當您變更 Filtering Service 電腦的 IP 位址時，此變更也不會自動登錄。

若要重新建立與 Filtering Service 的連線：

1. 開啓 Websense Manager。
  - 會出現一個狀態訊息，指出 Network Agent 實例無法連線到 Filtering Service。
2. 按一下左側瀏覽窗格頂端的**設定**。
3. 在左側瀏覽窗格的 Network Agent 下，選取 Network Agent 電腦的 IP 位址。
4. 在頁面頂端的「Filtering Service 定義」下，展開**伺服器 IP 位址**清單，然後選取 Filtering Service 電腦的 IP 位址。
5. 按一下頁面底部的**確定**來快取更新。按一下**全部儲存**才能使變更生效。

## 使用者識別問題

相關主題：

- ◆ [篩選問題，第 310 頁](#)
- ◆ [遠端使用者沒有獲得進行手動驗證的提示，第 324 頁](#)
- ◆ [遠端使用者沒有獲得正確篩選，第 324 頁](#)

如果 Websense 軟體正在使用電腦或網路政策，或者**預設**政策來篩選網際網路要求，即使您指派以使用者或群組為基礎的政策之後也是如此，或者如果套用了錯誤的以使用者或群組為基礎之政策，那麼請使用下列步驟來查明問題：

- ◆ 如果您正在使用 Microsoft ISA Server，並且變更了它的驗證方法，請確認重新啓動 Web Proxy 服務。
- ◆ 如果您正在 Windows Active Directory 中使用巢狀群組，那麼套用到上層群組的政策會套用到屬於下層群組的使用者，而不是直接套用到上層群組。如需有關使用者與群組階層的資訊，請參閱您的目錄服務文件。
- ◆ User Service 快取可能已過期。User Service 會快取使用者名稱與 IP 位址的對應達 3 小時。您可以快取 Websense Manager 中的所有變更，然後按一下**全部儲存**強制更新 User Service 快取。
- ◆ 如果錯誤篩選使用者的狀況是發生在執行 Windows XP SP2 的電腦上，那麼此問題可能是因為「Windows 網際網路連線防火牆」(ICF) 的緣故，此程式預設是包含在 Windows XP SP2 中並預設啓用。如需有關 Windows ICF 的詳細資訊，請參閱「Microsoft 知識庫文章 #320855」。

對於 DC Agent 或 Logon Agent 要從執行 Windows XP SP2 的電腦取得使用者登入資訊：

1. 在用戶端電腦上的 Windows 開始功能表中，選取設定 > 控制台 > 資訊安全中心 > Windows 防火牆。
2. 前往例外標籤。
3. 核取檔案及印表機共用。
4. 按一下確定以關閉 ICF 對話方塊，然後關閉其他所有開啓的視窗。

如果您使用 Websense 無障礙識別代理程式，請查閱相關的疑難排解各節：

- ◆ [疑難排解 DC Agent](#)，第 316 頁。
- ◆ [疑難排解 Logon Agent](#)，第 318 頁。
- ◆ [疑難排解 eDirectory Agent](#)，第 320 頁。
- ◆ [疑難排解 RADIUS Agent](#)，第 322 頁。

## 疑難排解 DC Agent

若要疑難排解 DC Agent 的使用者識別問題：

1. 檢查所有網路連線。
2. 查看「Windows 事件檢視器」中的錯誤訊息（請參閱 [Windows 事件檢視器](#)，第 340 頁）。
3. 查看 Websense 記錄檔 (Websense.log) 中的詳細錯誤資訊（請參閱 [Websense 記錄檔](#)，第 341 頁）。

DC Agent 使用者識別問題的常見原因包括：

- ◆ 網路或 Windows 服務與網域控制站的通訊方式使得 DC Agent 將服務視為尚未針對其定義政策的新使用者。請參閱 [使用者錯誤地由預設政策篩選](#)，第 316 頁。
- ◆ DC Agent 或 User Service 可能是使用「來賓」帳戶安裝為服務的，這就等於是網域控制站的匿名使用者。如果網域控制站已經設為不提供使用者與群組清單給匿名使用者，那麼 DC Agent 就無法下載清單。請參閱 [手動變更 DC Agent 與 User Service 權限](#)，第 317 頁。
- ◆ User Service 快取已過期。根據預設，User Service 會快取使用者名稱與 IP 位址對應達 3 小時。每次當您執行變更並按一下 Websense Manager 中的**全部儲存**時，也會更新快取。

### 使用者錯誤地由預設政策篩選

當某個網路或 Microsoft Windows 200x 聯繫網域控制站時，它們使用的帳戶名稱可能導致 Websense 軟體認為有無法識別的使用者正在從受篩選的電腦存取網際網路。由於沒有以使用者或群組為基礎的政策套用到這個使用者，因此會套用電腦或網路政策，或者「預設」政策。

- ◆ 網路服務可能需要網域權限才能存取網路上的資料，以及使用它們正在使用的網域使用者名稱來聯繫網域控制站。  
若要解決此問題，請參閱 [設定代理程式忽略特定的使用者名稱](#)，第 203 頁。
- ◆ Windows 200x 服務會定期以使用者名稱聯絡網域控制站；該使用者名稱是由電腦名稱加上貨幣符號所組成 (jdoe-computer\$)。DC Agent 會將該服務解譯為尚未為其指派政策的新使用者。  
若要解決此問題，設定 DC Agent 忽略任何 **computer\$** 形式的登入。
  1. 在 DC Agent 電腦上，瀏覽至 Websense **bin** 目錄 (預設為 **C:\Program Files\Websense\bin**)。
  2. 在文字編輯器中開啓 **transid.ini** 檔案。
  3. 將下列項目新增至檔案：  
`IgnoreDollarSign=true`
  4. 儲存並關閉檔案。
  5. 重新啓動 DC Agent (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。

## 手動變更 DC Agent 與 User Service 權限

在執行網域控制站的電腦上：

1. 建立使用者帳戶，例如 **Websense**。您可以使用現有的帳戶，不過 **Websense** 帳戶比較好，因為密碼可以設為不過期。無需特殊權限。  
將密碼設為永不過期。此帳戶僅提供存取目錄物件的安全內容。  
請記下您為此帳戶建立的使用者名稱和密碼，因為在步驟 6 和 7 必須輸入。
2. 在每個 Websense DC Agent 電腦上開啓「Windows 服務」對話方塊 (前往 **開始 > 程式集 > 系統管理工具 > 服務**)。
3. 選取 **Websense DC Agent** 項目，然後按一下 **停止**。
4. 連按兩下 **Websense DC Agent** 項目。
5. 在 **登入** 標籤上，選取 **這個帳戶** 選項。
6. 輸入步驟 1 中建立的 Websense DC Agent 帳戶的使用者名稱。例如：  
**DomainName\websense**。
7. 輸入並確認這個帳戶的 Windows 密碼。
8. 按一下 **確定** 以關閉對話方塊。
9. 在「服務」對話方塊中選取 **Websense DC Agent** 項目，然後按一下 **啓動**。
10. 針對 Websense User Service 的每個實例，重複此程序。

## 疑難排解 Logon Agent

如果因為 Logon Agent 無法識別您網路中的部分使用者，而使用**預設**政策來篩選他們：

- ◆ 請確認「Windows 群組原則物件 (GPO)」已正確套用到這些使用者的電腦 (請參閱[群組原則物件](#)，第 318 頁)。
- ◆ 如果 User Service 是安裝在 Linux 電腦上，而且您正在使用 Windows Active Directory (原生模式)，請檢查您的目錄服務配置 (請參閱[在 Linux 上執行 User Service](#)，第 319 頁)。
- ◆ 確認用戶端電腦可以與正在執行登入指令碼的網域控制站通訊 (請參閱[網域控制站能見度](#)，第 319 頁)。
- ◆ 確認用戶端電腦上已啟用 NetBIOS (請參閱[NetBIOS](#)，第 319 頁)。
- ◆ 確認用戶端電腦上的使用者設定檔沒有損毀 (請參閱[使用者設定檔問題](#)，第 320 頁)。

### 群組原則物件

驗證您的環境符合 Websense 軟體 *安裝手冊* 中所述的必要條件之後，請確認已正確套用「群組原則物件」：

1. 在 Active Directory 電腦上，開啓「Windows 控制台」並前往**系統管理工具 > Active Directory 使用者及電腦**。
2. 以滑鼠右鍵按一下網域項目，然後選取**內容**。
3. 按一下**群組原則**標籤，然後從「群組網域原則物件連結」清單選擇網域政策。
4. 按一下**編輯**然後展開目錄樹狀結構中的「使用者設定」節點。
5. 展開「Windows 設定」節點，然後選取**指令碼**。
6. 在右側窗格中，連按兩下**登入**，然後確認「登入內容」對話方塊有列出 **logon.bat**。

用戶端 Logon Application 需要這個指令碼。

- 如果指令碼中沒有 **logon.bat**，請參考 Websense 軟體 *安裝手冊* 的**初始設定**一章。
- 如果指令碼中的確有 **logon.bat**，但 Logon Agent 沒有運作，請使用本節中的其他疑難排解步驟，確認沒有網路連線問題，或請參考「[Websense 知識庫](#)」。

## 在 Linux 上執行 User Service

當您使用 Logon Agent 進行使用者的無障礙識別，而且 User Service 是安裝在 Linux 電腦上時，您必須暫時設定 Websense 軟體以「混合模式」與 Active Directory 通訊。

1. 在 Websense Manager 中，前往**設定 > 目錄服務**。
2. 記下您目前的目錄設定。
3. 在「目錄」下，選取 **Windows NT Directory / Active Directory (混合模式)**。
4. 按一下**確定**快取變更，然後按一下**全部儲存**。
5. 在「目錄」下，選取 **Active Directory (原生模式)**。如果沒有顯示您原始的配置，使用步驟 2 中所記的記錄重新建立目錄設定。如需詳細指示，請參閱 [Windows Active Directory \(原生模式\)](#)，第 57 頁。
6. 完成變更配置後，按一下**確定**，然後按一下**全部儲存**。

## 網域控制站能見度

若要驗證用戶端電腦是否可以與網域控制站通訊：

1. 嘗試將用戶端電腦上的磁碟機對應到網域控制站的根共用磁碟機。此位置是登入指令碼通常執行的地方，也是存放 **LogonApp.exe** 的地方。
2. 在用戶端電腦上，開啓 Windows 命令提示字元並執行下列指令：

```
net view /domain:<網域名稱>
```

如果這些測試中的任一項失敗，請參閱您的 Windows 作業系統文件，以獲得可能的解決方案。有一個與 Websense 軟體無關的網路連線問題。

## NetBIOS

「NetBIOS for TCP/IP」必須啓用，而且 TCP/IP NetBIOS Helper 服務必須執行，以便 Websense 登入程式碼可以在使用者的電腦上執行。

若要確認用戶端電腦上已啓用「NetBIOS for TCP/IP」：

1. 以滑鼠右鍵按一下**網路上的芳鄰**，然後選取**內容**。
2. 以滑鼠右鍵按一下**區域連線**，然後選取**內容**。
3. 選擇 **Internet Protocol (TCP/IP)**，然後按一下**內容**。
4. 按一下**進階**。
5. 選取 **WINS** 標籤，然後確認已設定正確的 NetBIOS 選項。
6. 如果您執行變更，按一下**確定**，然後再按兩次**確定**，關閉不同的「內容」對話方塊並儲存變更。

如果不需要任何變更，按一下**取消**以關閉每個對話方塊，而不做變更。

使用「Windows 服務」對話方塊來確認 **TCP/IP NetBIOS Helper** 服務是否正在用戶端電腦上執行 (請參閱 [「Windows 服務」對話方塊](#)，第 340 頁)。TCP/IP NetBIOS Helper 服務可在 Windows 2000、Windows XP、Windows Server 2003，以及 Windows NT 上執行。

## 使用者設定檔問題

如果用戶端電腦上的使用者設定檔已損毀，Websense 登入指令碼 (及 Windows GPO 設定) 就無法執行。此問題可以藉由重新建立使用者設定檔獲得解決。

當您重新建立使用者設定檔時，使用者現有的「我的文件」資料夾、「我的最愛」及其他自訂資料與設定並不會自動傳送到新的設定檔。先確認新的設定檔已解決問題，並且將使用者現有的資料複製到新設定檔之後，再行刪除現有已損毀的設定檔。

若要重新建立使用者設定檔：

1. 以本機管理員身份登入用戶端電腦。
2. 將包含使用者設定檔的目錄重新命名：  
C:\Documents and Settings\<使用者名稱>
3. 重新啟動電腦。
4. 以受篩選使用者身份登入電腦。接著會自動建立新使用者設定檔。
5. 檢查以確認使用者如預期地受到篩選。
6. 將自訂資料 (例如「我的文件」資料夾的內容) 從舊設定檔複製到新設定檔。不要使用「檔案及設定轉移精靈」，因為此精靈可能會將損毀情況也轉移到新設定檔。

## 疑難排解 eDirectory Agent

相關主題：

- ◆ [啟用 eDirectory Agent 診斷](#)，第 321 頁
- ◆ [eDirectory Agent 對 eDirectory Server 連線的計數錯誤](#)，第 322 頁
- ◆ [以主控台模式執行 eDirectory Agent](#)，第 322 頁

如果使用者名稱沒有傳送到 eDirectory Agent，可能無法正確篩選使用者。如果使用者沒有登入 Novell eDirectory 伺服器，eDirectory Agent 就無法偵測到登入。此情況發生的原因如下：

- ◆ 使用者登入的網域不包括在 eDirectory 使用者登入工作階段的預設根環境中。此根環境是在安裝期間指定的，而且應該符合 Novell eDirectory 在**設定 > 目錄服務**頁面上指定的根環境。
- ◆ 使用者試圖略過登入提示以規避 Websense 篩選。
- ◆ 使用者在 eDirectory 伺服器中沒有設定帳戶。

如果使用者沒有登入 eDirectory 伺服器，那麼特定於使用者的政策就無法套用到該使用者。相反，發生作用的是**預設**政策。如果您的網路中有共用的工作站，而且使用者可以在該處匿名登入，請針對那些特定電腦設定篩選政策。



若要判斷 eDirectory Agent 是否正在接收使用者名稱並識別該使用者：

1. 啟動 eDirectory Agent 記錄，如 [啟用 eDirectory Agent 診斷](#)，第 321 頁所述。
2. 在文字編輯器中開啓您已指定的記錄檔。
3. 搜尋與沒有正確篩選的使用者相對應的項目。
4. 如有類似下列所述的項目，表示 eDirectory Agent 已識別了使用者：

```
WsUserData::WsUserData()
User: cn=Admin,o=novell (10.202.4.78)
WsUserData::~~WsUserData()
```

在上述範例中，使用者 **Admin** 登入 eDirectory 伺服器，並且已經得到成功識別。

5. 如果使用者已經識別，但依然未如預期地受到篩選，請檢查您的政策配置，以確認是否有適當的政策套用到該使用者，以及 Websense Manager 中的使用者名稱是否與 Novell eDirectory 中的使用者名稱對應。

如果使用者未被識別，則確認下列事項：

- 使用者具有 Novell eDirectory 帳戶。
- 使用者登入的網域已包括在 eDirectory 使用者登入的預設根環境中。
- 使用者並未略過登入提示。

## 啟用 eDirectory Agent 診斷

eDirectory Agent 具有內建的診斷功能，但這些功能預設並未啟動。您可以在安裝期間或其他任何時間，啟用記錄與除錯。

1. 停止 eDirectory Agent (請參閱 [停止和啟動 Websense 服務](#)，第 245 頁)。
2. 在 eDirectory Agent 電腦上，前往 eDirectory Agent 安裝目錄。
3. 在文字編輯器中開啓 **wsedir.ini** 檔案。
4. 找到 **[eDirAgent]** 區段。
5. 若要啟用記錄與除錯，將 **DebugMode** 的值變更為 **On**：

```
DebugMode=On
```

6. 若要指定記錄的細節等級，修改下列行：

```
DebugLevel=<N>
```

**N** 值可以為 0-3，其中 3 表示最詳細。

7. 修改 **LogFile** 行以指定記錄輸出檔案的名稱：

```
LogFile=filename.txt
```

根據預設，記錄輸出會傳送到 eDirectory Agent 主控台。如果您是以主控台模式執行代理程式 (請參閱 [以主控台模式執行 eDirectory Agent](#)，第 322 頁)，則可以維持預設值。

8. 儲存並關閉 **wsedir.ini** 檔案。
9. 啟動 eDirectory Agent 服務 (請參閱 [停止和啟動 Websense 服務](#)，第 245 頁)。

## eDirectory Agent 對 eDirectory Server 連線的計數錯誤

如果 eDirectory Agent 監控您網路中超過 1000 個使用者，但顯示與 Novell eDirectory 伺服器僅有 1000 個連線，這可能是負責將資訊從 eDirectory 伺服器傳遞到 Websense eDirectory Agent 之 Windows API 的限制。這個狀況極少發生。

若要避開這個限制，在準確計數伺服器連線的 **wseidir.ini** 檔案中新增一個參數 (僅適用於 Windows)：

1. 停止 Websense eDirectory Agent 服務 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。
2. 前往 Websense **bin** 目錄 (預設為 **C:\Program Files\Websense\bin**)。
3. 在文字編輯器中開啓 **wseidir.ini** 檔案。
4. 插入空行，然後輸入：

```
MaxConnNumber = <NNNN>
```

其中，<NNNN> 是與 Novell eDirectory 伺服器可能連線的上限數目。例如，如果您的網路有 1,950 個使用者，您可以輸入 2000 作為上限數目。

5. 儲存檔案。
6. 重新啓動 eDirectory Agent。

## 以主控台模式執行 eDirectory Agent

1. 執行下列其中之一：
  - 在 Windows 命令提示字元 (開始 > 執行 > **cmd**) 中，輸入下列指令：  
`eDirectoryAgent.exe -c`
  - 在 Linux command shell 中輸入下列指令：  
`eDirectoryAgent -c`
2. 當您準備好停止代理程式時，按下 **Enter**。代理程式停止執行可能需要數秒鐘。

## 疑難排解 RADIUS Agent

RADIUS Agent 具有內建的診斷功能，但這些功能預設並未啓動。若要啓動 RADIUS Agent 記錄與除錯：

1. 停止 RADIUS Agent 服務 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。
2. 在 RADIUS Agent 電腦上，前往代理程式安裝目錄 (預設為 **Websense\bin**)。
3. 在文字編輯器中開啓 **wsradius.ini** 檔案。
4. 找到 **[RADIUSAgent]** 區段。
5. 若要啓用記錄與除錯，將 **DebugMode** 的值變更為 **On**：

```
DebugMode=On
```

6. 若要指定記錄的細節等級，修改下列行：

```
DebugLevel=<N>
```

**N** 值可以為 0-3，其中 3 表示最詳細。

7. 修改 **LogFile** 行以指示輸出檔案的名稱：

```
LogFile=filename.txt
```

根據預設，記錄輸出會傳送到 RADIUS Agent 主控台。如果您是以主控台模式執行代理程式（請參閱[以主控台模式執行 RADIUS Agent](#)，第 323 頁），則可以選擇維持預設值。

8. 儲存並關閉 **wsradius.ini** 檔案。  
9. 啟動 RADIUS Agent 服務（請參閱[停止和啟動 Websense 服務](#)，第 245 頁）。

如果未如預期地識別及篩選遠端使用者，原因可能是 RADIUS Agent 與您的 RADIUS 伺服器之間的通訊問題。查看 RADIUS Agent 記錄中的錯誤，以判斷原因。

## 以主控台模式執行 RADIUS Agent

若要以主控台模式啟動 RADIUS Agent（當作應用程式），輸入下列指令：

- ◆ 在 Windows 命令提示字元中輸入：

```
RadiusAgent.exe -c
```

- ◆ 在 Linux shell 提示中輸入：

```
./RadiusAgent -c
```

若要在任何時間停止代理程式，再次按下 **Enter**。代理程式停止執行可能需要數秒鐘。

RADIUS Agent 接受下列命令行參數：



### 注意

在 Linux 上，Websense, Inc. 建議使用提供的指令碼來啟動或停止 Websense RADIUS Agent (**WsRADIUSAgent start|stop**)，而不要使用 **-r** 與 **-s** 參數。

參數	說明
-i	安裝 RADIUS Agent 服務/精靈。
-r	執行 RADIUS Agent 服務/精靈。
-s	停止 RADIUS Agent 服務/精靈。
-c	執行 RADIUS Agent 作為應用程式程序，而不是作為服務或精靈。在主控台模式時，RADIUS Agent 可以設定為將記錄輸出傳送到主控台或文字檔。

參數	說明
-v	顯示 RADIUS Agent 的版本編號。
-? -h -help <無選項>	在指令行顯示使用資訊。列出並說明所有可能的指令行參數。

## 遠端使用者沒有獲得進行手動驗證的提示

如果您已設定遠端使用者在存取網際網路時要手動驗證，有時可能會發生個別使用者沒有獲得驗證提示的情形。當有些網路內 IP 位址已經設定略過手動驗證時，就可能發生此狀況。

當遠端使用者存取網路時，Websense 軟體會讀取電腦的「媒體存取控制」(MAC) 位址的最後部分。如果它符合已設定為略過手動驗證的網路內 IP 位址，當遠端使用者存取網際網路時，就不會獲得手動驗證的提示。

一種解決方案是將網路內 IP 位址設定為使用手動驗證。另一種解決方案是針對受影響的遠端使用者停用手動驗證需求。

## 遠端使用者沒有獲得正確篩選

如果遠端使用者沒有經過篩選，或沒有經過指派給它們的特定政策篩選，查看 RADIUS Agent 記錄中的訊息 **Error receiving from server: 10060** (Windows) 或 **Error receiving from server: 0** (Linux)。

這通常在 RADIUS 伺服器未將 RADIUS Agent 識別為用戶端 (RADIUS 要求的來源) 的情況下發生。請確保您的 RADIUS 伺服器已正確設定 (請參閱 [設定 RADIUS 環境](#)，第 191 頁)。

您可以使用 RADIUS Agent 的內建診斷工具來疑難排解篩選問題 (請參閱 [疑難排解 RADIUS Agent](#)，第 322 頁)。

當您已執行 Remote Filtering 功能 (請參閱 [篩選遠端用戶端](#)，第 137 頁) 時，如果 Remote Filtering Client 無法與網路內的 Remote Filtering Server 通訊，就無法篩選遠端使用者。

如需有關設定 Remote Filtering 的指示，請參閱 *Remote Filtering* 技術報告。

## 封鎖訊息問題

- ◆ [封鎖檔案類型沒有顯示封鎖頁面](#)，第 325 頁
- ◆ [使用者收到瀏覽器錯誤而不是封鎖頁面](#)，第 325 頁
- ◆ [顯示空白頁面而不是封鎖頁面](#)，第 326 頁
- ◆ [通訊協定封鎖訊息未如預期地顯示](#)，第 326 頁
- ◆ [顯示通訊協定封鎖訊息而不是封鎖頁面](#)，第 326 頁

## 封鎖檔案類型沒有顯示封鎖頁面

使用檔案類型封鎖時，使用者可能並不是每次都看到封鎖訊息。例如，當可下載的檔案包含在允許之網站的內部框架 (IFRAME) 中時，傳送到該框架的封鎖訊息就會看不見，因為框架大小為零。

這只是顯示問題；使用者還是無法存取或下載封鎖檔案。

## 使用者收到瀏覽器錯誤而不是封鎖頁面

如果使用者收到錯誤訊息，而不是收到封鎖頁面，最可能的原因有 2 個：

- ◆ 使用者的瀏覽器設定為使用外部代理。在大多數的瀏覽器中，有設定可以啓用使用外部代理。請確認瀏覽器未設定使用外部代理。
- ◆ 識別 Filtering Service 電腦或與之通訊時發生問題。

如果使用者的瀏覽器設定是正確的，請確認 **eimserver.ini** 檔案中正確列出 Filtering Service 電腦的 IP 位址。

1. 停止 **Websense Filtering Service** (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。
2. 瀏覽至 Websense **bin** 目錄 (預設為 C:\Program Files\Websense\bin 或 /opt/Websense/bin)。
3. 在文字編輯器中開啓 **eimserver.ini** 檔案。
4. 在 [WebsenseServer] 下，新增空行並輸入下列內容：

```
BlockMsgServerName = <Filtering Service IP 位址>
```

例如，如果 Filtering Service IP 位址是 10.201.72.15，請輸入：

```
BlockMsgServerName = 10.201.72.15
```

5. 儲存並關閉檔案。
6. 重新啓動 Filtering Service。

如果 Filtering Service 電腦有一個以上的網路卡，而且在編輯 **eimserver.ini** 檔案之後，封鎖頁面依然沒有正確顯示，請在 **BlockMsgServerName** 參數中嘗試其他網路卡的 IP 位址。

如果封鎖頁面依然沒有顯示，請確認該使用者對於下列 Websense 封鎖頁面目錄中的檔案有讀取權限：

- ◆ Websense\BlockPages\en\Default
- ◆ Websense\BlockPages\en\Custom

如果封鎖頁面問題依然存在，請參閱「Websense [知識庫](#)」以獲得其他疑難排解提示。

## 顯示空白頁面而不是封鎖頁面

當封鎖廣告時，或者瀏覽器未正確偵測封鎖頁面的相關編碼時，使用者可能收到空白頁面，而不是封鎖頁面。此狀況的原因如下：

- ◆ 當「廣告」類別被封鎖時，Websense 軟體有時會將圖形檔案要求解譯為廣告要求，而顯示空白影像，而不是封鎖頁面 (這是封鎖廣告的一般方法)。如果要求的 URL 結尾為 .gif 或類似的結尾，請使用者重新輸入該 URL，但不要輸入 \*.gif 部分。
- ◆ 有些較舊的瀏覽器可能無法偵測封鎖頁面的編碼。若要啟動合適的偵測，設定您的瀏覽器顯示適當的字元集 (法文、德文、義大利文、西班牙文、巴西葡萄牙文、簡體中文、繁體中文或韓文使用 UTF-8；日文使用 Shift\_JIS)。請參閱瀏覽器的文件以取得指示，或將瀏覽器升級為更新版本。

## 通訊協定封鎖訊息未如預期地顯示

通訊協定封鎖訊息沒有顯示，或在延遲後顯示，可能是因為下列原因之一：

- ◆ User Service 必須安裝在 Windows 電腦上，才能正確顯示通訊協定封鎖訊息。如需詳細資訊，請參閱 *安裝手冊*。
- ◆ 如果 Network Agent 是安裝在具有多個網路介面卡 (NIC) 的電腦上，而且有一個網路卡監控與 Filtering Service 不一樣的網路區段，那麼通訊協定封鎖訊息可能無法傳送到用戶端電腦。確認 Filtering Service 電腦具有 NetBIOS 並且「伺服器訊息塊通訊協定」可存取用戶端電腦，而且連接埠 15871 沒有封鎖。
- ◆ 當 Network Agent 設定為監控傳送到內部電腦的要求時，通訊協定封鎖訊息可能會有些許延遲，或顯示在產生要求之通訊協定資料的內部電腦 (而不是顯示在用戶端電腦上)。
- ◆ 如果受篩選用戶端或 Websense 篩選電腦執行的是 Windows 200x，必須執行 Windows Messenger 服務才能顯示通訊協定封鎖訊息。使用用戶端或伺服器電腦上的「Windows 服務」對話方塊查看 Messenger 服務是否正在執行 (請參閱「[Windows 服務](#)」對話方塊，第 340 頁)。即使封鎖訊息沒有顯示，依然會封鎖通訊協定要求。

## 顯示通訊協定封鎖訊息而不是封鎖頁面

如果您的整合產品沒有傳送 HTTPS 資訊到 Websense 軟體，或者如果 Websense 軟體是以單機模式執行，那麼 Network Agent 可能會將經由類別設定而封鎖的 HTTPS 網站要求解譯為通訊協定要求。因此，就不會顯示通訊協定封鎖訊息。HTTPS 要求也會被記錄為通訊協定要求。

## 記錄、狀態訊息及警示問題

- ◆ [我在哪裡可以找到 Websense 元件的錯誤訊息？](#)，第 327 頁
- ◆ [Websense 健全度警示](#)，第 327 頁
- ◆ [單一要求產生了兩個 Log 記錄](#)，第 328 頁

### 我在哪裡可以找到 Websense 元件的錯誤訊息？

如果 Websense 核心元件有相關的錯誤或警告，會有簡短的警示訊息顯示在 Websense Manager 的 **狀態 > 今天** 頁面頂端的 **健全度警示摘要** 清單中 (請參閱 [Websense 健全度警示](#)，第 327 頁)。

- ◆ 在 **狀態 > 警示** 頁面上按一下警示訊息，檢視更多詳細資訊。
- ◆ 在「狀態」>「警示」頁面上，按一下訊息旁的 **解決方案** 以獲得疑難排解協助。

來自 Websense 軟體元件的錯誤、警告及訊息，以及資料庫下載狀態訊息，會記錄在 **websense.log** 檔案，此檔案位於 Websense **bin** 目錄 (預設為 C:\Program Files\Websense\bin 或 /opt/Websense/bin)。請參閱 [Websense 記錄檔](#)，第 341 頁。

對於安裝在 Windows 電腦上的 Websense 軟體元件，您也可以查看「Windows 事件檢視器」。請參閱 [Windows 事件檢視器](#)，第 340 頁。

### Websense 健全度警示

「Websense 健全度警示摘要」會列出 Websense 軟體之受監控元件會碰到的潛在問題。包括：

- ◆ Filtering Service 沒有執行
- ◆ 無法使用 User Service
- ◆ Log Server 沒有執行
- ◆ 沒有為 Policy Server 設定 Log Server
- ◆ 記錄資料庫無法使用
- ◆ Network Agent 沒有執行
- ◆ 沒有為 Policy Server 設定 Network Agent
- ◆ Network Agent 未設定監控網路卡
- ◆ Network Agent 未設定 Filtering Service
- ◆ 初始篩選資料庫正在使用中
- ◆ 首次下載 Master Database
- ◆ Master Database 已更新
- ◆ Master Database 已超過 1 星期沒有更新
- ◆ Master Database 未下載成功
- ◆ 未啓用 WebCatcher

- ◆ 訂閱有問題
- ◆ 訂閱密碼即將到期
- ◆ 尚未輸入任何訂閱密碼

「警示」頁面會提供有關所有錯誤或警告情況的基本資訊。如需有關解決問題的資訊，按一下[解決方案](#)。

某些情況下，如果您收到有關未使用或已停用的元件的錯誤或狀態訊息，可以選擇隱藏警示訊息。如需詳細資訊，請參閱[檢閱目前的系統狀態](#)，第 252 頁。

## 單一要求產生了兩個 Log 記錄

如果 Windows QoS Packet Scheduler 與 Network Agent 安裝在同一部電腦上，那麼針對 Network Agent 電腦所執行的每個單一 HTTP 或通訊協定要求都會記錄 2 個要求 (您網路中的用戶端電腦所執行的要求並不會發生這樣的重複情況)。

若要修復此問題，停用 Network Agent 電腦上的 Windows QoS Packet Scheduler。

如果您使用 Network Agent 執行所有記錄，就不會發生此問題。如需詳細資訊，請參閱[設定網路卡設定](#)，第 298 頁。

## Policy Server 與 Policy Database 問題

---

- ◆ [忘記密碼](#)，第 328 頁
- ◆ [無法登入 Policy Server](#)，第 329 頁
- ◆ [Websense Policy Database 服務無法啟動](#)，第 329 頁

## 忘記密碼

如果您是透過 Websense Manager 使用 Websense 使用者帳戶登入 Policy Server 的「超級管理員」或委派管理員，任何無條件「超級管理員」都可以重設密碼。

- ◆ 您可在[設定 > 帳戶](#)頁面上設定 WebsenseAdministrator 密碼。
- ◆ 其他管理員帳戶密碼則可以在[委派管理 > 管理 Websense 使用者帳戶](#)頁面上設定。

如果您不是使用委派管理員，而且忘記 WebsenseAdministrator 密碼，可以登入 MyWebsense 來重設密碼。

- ◆ 與 MyWebsense 帳戶相關聯的訂閱密碼必須與您目前的 Websense Web Security 或 Websense Web Filter 訂閱密碼相符。
- ◆ 如果您有多個訂閱密碼，則必須選擇適當的 Websense Web Security 或 Websense Web Filter 密碼，密碼重設程序才會成功。
- ◆ 您必須存取 Websense Manager 電腦，以便完成重設程序。



## 無法登入 Policy Server

確認所選的 Policy Server IP 位址是正確的。如果因為新增 Policy Server 到 Websense Manager 而使 Policy Server 電腦的位址變更，您必須登入其他的 Policy Server，從 Websense Manager 移除舊的 IP 位址，然後新增新的 Policy Server IP 位址。請參閱 [新增及編輯 Policy Server 實例](#)，第 239 頁。

如果 Websense Manager 突然停止，或是透過 kill (Linux) 或 End Task (Windows) 指令而停止，請稍候幾分鐘，然後再次登入。Websense 軟體會在 3 分鐘內偵測並關閉終止的工作階段。

## Websense Policy Database 服務無法啟動

Websense Policy Database 是以特殊帳戶執行的：**WebsenseDBUser**。如果這個帳戶發生登入問題，Policy Database 將無法啟動。

若要解決此問題，請變更 WebsenseDBUser 密碼。

1. 以本機管理員身份登入 Policy Database 電腦。
2. 前往 **開始 > 程式集 > 系統管理工具 > 電腦管理**。
3. 在瀏覽窗格的「系統工具」下，展開**本機使用者及群組**，然後選取**使用者**。使用者資訊會顯示在內容窗格中。
4. 以滑鼠右鍵按一下 **WebsenseDBUser** 並選取**設定密碼**。
5. 輸入並確認這個使用者帳戶的新密碼，然後按一下**確定**。
6. 關閉「電腦管理」對話方塊。
7. 前往 **開始 > 程式集 > 系統管理工具 > 服務**。
8. 以滑鼠右鍵按一下 **Websense Policy Database** 並選取**內容**。
9. 在「內容」對話方塊的「登入」標籤上，輸入新的 WebsenseDBUser 密碼資訊，然後按一下**確定**。
10. 再次以滑鼠右鍵按一下 Websense Policy Database，然後選取**啟動**。  
當服務啟動之後，關閉「服務」對話方塊。

## 委派管理問題

- ◆ [無法從角色刪除受管理的用戶端](#)，第 330 頁
- ◆ [登入錯誤顯示有其他人已登入我的電腦](#)，第 330 頁
- ◆ [有些使用者無法存取「未篩選的 URL」清單上的網站](#)，第 330 頁
- ◆ [已重新分類的網站根據錯誤的類別篩選](#)，第 330 頁
- ◆ [我無法建立自訂通訊協定](#)，第 330 頁

## 無法從角色刪除受管理的用戶端

在下列情況中，無法從「委派管理」>「編輯角色」頁面上的受管理的用戶端清單直接刪除用戶端：

- ◆ 管理員已套用政策至用戶端
- ◆ 管理員已套用政策至網路、群組、網域或組織單位的一或多個成員

若「超級管理員」在登入 Websense Manager 時，選擇不是與包含要刪除之用戶端的目錄服務通訊的 Policy Server，也可能會發生問題。在此情況下，目前的 Policy Server 和目錄服務將無法辨識用戶端。

如需有關刪除受管理用戶端的協助，請參閱 [刪除受管理的用戶端](#)，第 228 頁。

## 登入錯誤顯示有其他人已登入我的電腦

當您嘗試登入 Websense Manager 時，有時可能會收到錯誤「登入失敗。角色 <角色名稱> 已經被 <用戶名稱> 使用，自 <日期，時間> 起，在電腦 127.0.0.1 上。」IP 位址 127.0.0.1 又稱為回送位址，通常指的是本機電腦。

此訊息表示有人已使用您要求的相同角色登入 Websense Manager 安裝電腦。您可以選擇其他角色（如果您管理多個角色的話）、只登入執行報告，或等候另一個管理員登出。

## 有些使用者無法存取「未篩選的 URL」清單上的網站

「未篩選的 URL」只會影響已在其中新增 URL 之角色所管理的用戶端。例如，如果「超級管理員」新增了未篩選的 URL，委派管理角色所管理的用戶端並未被授予存取那些網站的權限。

若要使網站可以讓其他角色中用戶端存取，「超級管理員」可以切換到每個角色並將相關網站新增到該角色的未篩選 URL 清單。

## 已重新分類的網站根據錯誤的類別篩選

「已重新分類的 URL」只會影響已在其中新增 URL 之角色所管理的用戶端。例如，當「超級管理員」重新分類 URL 時，委派管理角色所管理的用戶端卻繼續根據那些網站的 Master Database 類別來篩選。

若要將重新分類套用到其他角色的用戶端，「超級管理員」可以切換到每個角色，並重新分類該角色的網站。

## 我無法建立自訂通訊協定

只有「超級管理員」可以建立自訂通訊協定。不過，委派管理員可以設定自訂通訊協定的篩選動作。

當「超級管理員」建立自訂通訊協定時，應該針對大多數的用戶端設定適當的預設動作。然後，通知委派管理員有新的通訊協定，讓他們可以視需要更新他們角色的篩選器。

## 報告問題

- ◆ *Log Server* 沒有執行，第 331 頁
- ◆ 沒有為 *Policy Server* 安裝 *Log Server*，第 332 頁
- ◆ 記錄資料庫未建立，第 333 頁
- ◆ 記錄資料庫無法使用，第 333 頁
- ◆ 記錄資料庫大小，第 334 頁
- ◆ *Log Server* 沒有在記錄資料庫中記錄資料，第 334 頁
- ◆ 更新 *Log Server* 連線密碼，第 335 頁
- ◆ 設定 *Microsoft SQL Server 2005* 的使用者權限，第 335 頁
- ◆ *Log Server* 無法連接到目錄服務，第 336 頁
- ◆ 網際網路瀏覽時間報告中的資料不準確，第 336 頁
- ◆ 頻寬比預期的更大，第 336 頁
- ◆ 有些通訊協定要求沒有記錄，第 337 頁
- ◆ 所有報告都是空的，第 337 頁
- ◆ 「今天」或「記錄」頁面上沒有顯示圖表，第 338 頁
- ◆ 無法存取某些報告功能，第 338 頁
- ◆ *Microsoft Excel* 輸出缺少某些報告資料，第 339 頁
- ◆ 將簡報報告輸出儲存為 *HTML*，第 339 頁
- ◆ 調查報告搜尋問題，第 339 頁
- ◆ 一般調查報告問題，第 340 頁

### Log Server 沒有執行

如果 *Log Server* 沒有執行，或者其他 *Websense* 元件無法與 *Log Server* 通訊，則不會儲存網際網路使用資訊，而且您也無法產生網際網路使用報告。

在下列狀況中，*Log Server* 可能無法使用：

- ◆ *Log Server* 電腦上的磁碟空間不足。
- ◆ 您變更了 *Microsoft SQL Server* 或 *MSDE* 密碼，但沒有更新 *ODBC* 或 *Log Server* 配置。
- ◆ 自從 *Master Database* 成功下載之後已超過 14 天。
- ◆ 找不到 *logserver.ini* 檔案或該檔案已損毀。
- ◆ 您已停止 *Log Server* 以避免記錄網際網路使用資訊。

若要疑難排解此問題：

- ◆ 確認可用磁碟空間容量，並視需要移除無關的檔案。
- ◆ 如果您確信密碼變更是造成此問題的原因，請參閱 [更新 Log Server 連線密碼](#)，第 335 頁。
- ◆ 瀏覽至 Websense **bin** 目錄 (預設為 C:\Program Files\WebSense\bin)，並確認您可以在文字編輯器中開啓 **logserver.ini**。如果此檔案已經損毀，請以備份檔案取代它。
- ◆ 查看「Windows 服務」對話方塊以確認 Log Server 已經啓動，若有必要請重新啓動服務 (請參閱 [停止和啓動 Websense 服務](#)，第 245 頁)。
- ◆ 查看「Windows 事件檢視器」及 **websense.log** 檔案中來自 Log Server 的錯誤訊息 (請參閱 [疑難排解工具](#)，第 340 頁)。

## 沒有為 Policy Server 安裝 Log Server

Websense Log Server 會收集網際網路使用資訊並儲存在記錄資料庫，以便用於調查報告、簡報報告及 Websense Manager 中「今天」與「記錄」頁面上的圖表和摘要。

您必須安裝 Log Server 才能執行報告。

如果發生下列狀況，就可能看到此訊息：

- ◆ Log Server 安裝在與 Policy Server 不同的電腦上，而且在 Websense Manager 中，Log Server IP 位址錯誤設為 localhost。
- ◆ Log Server 安裝在 Linux 電腦上。
- ◆ 您沒有使用 Websense 報告工具。

若要驗證 Websense Manager 中設定的 Log Server IP 位址是否正確：

1. 選擇左側瀏覽窗格的**設定**標籤，然後前往**一般 > 記錄**。
2. 在 **Log Server IP 位址或名稱**欄位中輸入 Log Server 電腦的 IP 位址。
3. 按一下**確定**來快取您的變更，然後按一下**全部儲存**。

如果 Log Server 安裝在 Linux 電腦上，或者如果您沒有使用 Websense 報告工具，則可以隱藏 Websense Manager 中的警示訊息。

1. 在左側瀏覽窗格的「主要」標籤上，前往**狀態 > 警示**。
2. 在「使用中的警示」下，按一下**進階**。
3. 針對「未安裝任何 Log Server」訊息勾選**隱藏此警示**。
4. 按一下**立即儲存**。接著會立即執行變更。

## 記錄資料庫未建立

安裝程式有時無法建立記錄資料庫。下列清單說明最常見的原因及解決方案。

**問題：** 有檔案使用了 Websense 軟體針對記錄資料庫 (wslogdb70 及 wslogdb70\_1) 所使用的名稱，但那些檔案並未正確連接至資料庫引擎，因此 Websense 安裝程式無法使用它們。

**解決方案：** 移除或重新命名現有檔案，然後再次執行安裝程式。

**問題：** 用來登入以進行安裝的帳戶，對正在安裝資料庫的磁碟機沒有足夠的權限。

**解決方案：** 更新登入帳戶使其具有安裝位置的讀寫權限，或以另一個已具有這些權限的帳戶登入。然後，再次執行安裝程式。

**問題：** 指定位置上沒有足夠磁碟空間可建立與維護記錄資料庫。

**解決方案：** 在所選的磁碟上清理出足夠的空間，以便安裝與維護記錄資料庫。然後，再次執行安裝程式。或者，選擇其他位置。

**問題：** 用來登入以進行安裝的帳戶沒有足夠的 SQL Server 權限以便建立資料庫。

**解決方案：** 更新登入帳戶，或以已經具有必要權限的帳戶登入。然後，再次執行安裝程式。

需要的權限取決於 Microsoft SQL Server 的版本：

- SQL Server 2000 或 MSDE：必須有 **dbo** (資料庫擁有者) 權限
- SQL Server 2005：必須有 **dbo** 及 **SQLServerAgentReader** 權限

## 記錄資料庫無法使用

Websense Log Database 會儲存網際網路使用資訊以使用於簡報報告、調查報告及 Websense Manager 中「今天」與「記錄」頁面上的圖表和摘要。

如果 Websense 軟體無法連線到記錄資料庫，首先確認資料庫引擎 (Microsoft SQL Server 或 Microsoft SQL Server Desktop Engine [MSDE]) 是在記錄資料庫電腦上執行。

1. 開啓「Windows 服務」對話方塊 (請參閱 [「Windows 服務」對話方塊](#)，第 340 頁) 並確認下列服務正在執行中：
  - Microsoft SQL Server：
    - MSSQLSERVER
    - SQLSERVERAGENT
  - Microsoft SQL Desktop Engine (MSDE)：
    - MSSQL\$WEBSSENSE (如果您從 Websense, Inc. 取得 MSDE)
    - SQLAgent\$WEBSSENSE

2. 如果其中有服務已停止，以滑鼠右鍵按一下該服務名稱，然後按一下**啓動**。如果服務沒有重新啓動，查看「Windows 事件檢視器」(請參閱[Windows 事件檢視器](#)，第 340 頁)中的 Microsoft SQL Server 或 MSDE 錯誤與警告。

如果資料庫引擎已在執行中：

- ◆ 確認 SQL Server Agent 是在執行資料庫引擎的電腦上執行。
- ◆ 使用「Windows 服務」對話方塊確認 **Websense Log Server** 服務正在執行中。
- ◆ 如果 Log Server 與記錄資料庫位於不同電腦上，確認兩台電腦都在執行，而且兩台電腦之間的網路連線沒有受損。
- ◆ 確認記錄資料庫電腦上有足夠的可用空間，而且記錄資料庫已分配了足夠的磁碟空間容量 (請參閱[Log Server 沒有在記錄資料庫中記錄資料](#)，第 334 頁)。
- ◆ 確認 Microsoft SQL Server 或 MSDE 密碼並未變更。如果密碼變更，您必須更新 Log Server 用來連線到資料庫的密碼資訊。請參閱[更新 Log Server 連線密碼](#)，第 335 頁。

## 記錄資料庫大小

記錄資料庫大小一直是很重要的考量。如果您已成功產生 Websense 報告並發現報告需要較長時間才會顯示，或者是從網頁瀏覽器收到逾時訊息，請考慮停用部分資料庫分割區。

1. 在 Websense Manager 中，前往**設定 > 報告 > 記錄資料庫**。
2. 找到頁面上的**可用的分割區**區段。
3. 對於目前報告作業不需要的所有分割區，清除其**啓動**核取方塊。
4. 按一下**立即儲存**以執行變更。

## Log Server 沒有在記錄資料庫中記錄資料

一般而言，當 Log Server 無法寫入資料到記錄資料庫時，表示資料庫分配的磁碟空間已經不足。當磁碟機已滿，或在使用 Microsoft SQL Server 的情況下設定了資料庫可增加的上限時，就會發生此問題。

如果儲存記錄資料庫的磁碟機已滿，您必須增加電腦的磁碟空間，以便恢復記錄。

如果您的「SQL Server 資料庫管理員」已針對 Microsoft SQL Server 中個別資料庫可增加的大小設定了上限，請執行下列其中一項操作：

- ◆ 聯絡「SQL Server 資料庫管理員」提高上限。
- ◆ 找出大小上限，並前往**設定 > 報告 > 記錄資料庫**以設定記錄資料庫，使其達到約 90% 的大小上限時進行變換。請參閱[設定變換選項](#)，第 280 頁。

如果您的「資訊科技」部門建立了 SQL Server 作業的磁碟空間上限，請聯絡他們以取得協助。

## 更新 Log Server 連線密碼

如果您變更 Websense 軟體用來連線到記錄資料庫的帳戶之密碼，也必須更新 Log Server 以使用新密碼。

1. 在 Log Server 電腦上，前往**開始 > 程式集 > Websense > 公用程式 > Log Server Configuration**。Log Server Configuration 公用程式隨即開啓。
2. 按一下**資料庫**標籤，然後驗證「ODBC 資料來源名稱 (DSN)」欄位中是否顯示正確的資料庫 (預設為 **wslogdb70**)。
3. 按一下**連接**。接著會開啓「選擇資料來源」對話方塊。
4. 按一下**電腦資料來源**標籤，然後連按兩下 **wslogdb70** (或您的記錄資料庫名稱)。接著會開啓「SQL Server 登入」對話方塊。
5. 確認「LoginID」欄位中含有正確的帳戶名稱 (通常是 **sa**)，然後輸入新密碼。
6. 按一下**確定**，然後，在「Log Server 配置」對話方塊中，按一下**套用**。
7. 按一下**連接**標籤，然後停止並重新啓動 Log Server。
8. 當 Log Server 再次執行時，按一下**確定**以關閉公用程式。

## 設定 Microsoft SQL Server 2005 的使用者權限

Microsoft SQL Server 2005 定義了 SQL Server Agent 角色，該角色控管工作架構的可存取性。SQL Server 2005 的 SQL Server Agent 工作儲存於 SQL Server msdb 資料庫中。

若要成功安裝 Websense Log Server，擁有 Websense 資料庫的使用者帳戶必須具有 msdb 資料庫中的下列其中一個角色的成員資格：

- ◆ SQLAgentUser 角色
- ◆ SQLAgentReader 角色
- ◆ SQLAgentOperator 角色



### 注意

SQL 使用者帳戶也必須是 **DBCreator** 固定伺服器角色的成員。

請至 Microsoft SQL Server 2005 以授予 SQL Server 使用者帳戶必要的權限，以成功安裝 Websense 報告元件。

1. 在 SQL Server 電腦上，前往**開始 > 程式集 > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio**。
2. 選取**物件總管**樹狀結構。
3. 選取**安全性 > 登入**。
4. 選取要在安裝期間使用的登入帳戶。
5. 以滑鼠右鍵按一下登入帳戶，然後選取此使用者的**內容**。

6. 選取**使用者對應**，並執行下列動作：
  - a. 在資料庫對應中選取 **msdb**。
  - b. 將成員資格授予下列其中一個角色：
    - SQLAgentUser 角色
    - SQLAgentReader 角色
    - SQLAgentOperator 角色
  - c. 按一下**確定**以儲存。
7. 選取**伺服器角色**，然後選取 **dbcreator**。dbcreator 角色隨即建立。
8. 按一下**確定**以儲存。

## Log Server 無法連接到目錄服務

如果發生下列錯誤，Log Server 將無法存取目錄服務；而存取目錄服務是針對報告更新使用者與群組對應所必需的。這些錯誤會顯示在「Windows 事件檢視器」中（請參閱 [Windows 事件檢視器](#)，第 340 頁）。

- ◆ EVENT ID: 4096 - 無法初始化目錄服務 Websense Server 可能失敗或無法連線。
- ◆ EVENT ID: 4096 - 無法連接到目錄服務。目前將不會解析這個使用者的群組。請確認此程序可以存取目錄服務。

最常見的原因是，Websense Log Server 與 Websense User Service 位於限制存取的防火牆的兩邊。

若要解決此問題，設定防火牆以允許透過那些電腦用來彼此通訊之連接埠所進行的存取。

## 網際網路瀏覽時間報告中的資料不準確

請注意，合併可能會使網際網路瀏覽時間報告的資料不準確。這些報告會顯示使用者存取網際網路所花的時間，並包含在每個網站所花時間的詳細資料。網際網路瀏覽時間是使用特殊演算法計算的，啟用合併可能會影響這些報告的計算準確性。

## 頻寬比預期的更大

許多 Websense 整合 (但不是全部) 會提供頻寬資訊。如果您的整合不提供頻寬資訊，可以設定 Network Agent 執行記錄，以便包含頻寬資料。

當使用者要求允許的檔案下載時，整合產品或 Network Agent 會傳送完整檔案大小，而 Websense 軟體會將該大小記錄為已接收的位元組。

如果使用者後來取消了實際的下載，或檔案未完全下載，那麼記錄資料庫中的已接收位元組值依然會顯示完整檔案大小。在這些情況下，報告的已接收位元組將會大於實際接收的位元組數量。

這也會影響報告的頻寬值，因為頻寬值顯示的是已接收位元組與已傳送位元組的組合。



## 有些通訊協定要求沒有記錄

少數的通訊協定 (例如 ICQ 與 AOL 使用的通訊協定) 會提示使用者使用一個 IP 位址登入伺服器，然後傳送不同的識別 IP 位址與連接埠號碼到用戶端，以供訊息傳送之用。在此情況下，所有傳送與接收的訊息可能都不受 Websense Network Agent 監控與記錄，因為在訊息交換時，訊息伺服器是未知的。

因此，所記錄的要求數可能與實際傳送的要求數不相符。這會影響 Websense 報告工具所產生之報告的準確性。

## 所有報告都是空的

如果您的報告中沒有任何資料，請確認下列事項：

- ◆ 已啓用的資料庫分割區含有報告所含資料的資訊。請參閱[資料庫分割區](#)，第 337 頁。
- ◆ 在 Microsoft SQL Server 或 MSDET 中啓動了 SQL Server Agent 工作。請參閱[SQL Server Agent 工作](#)，第 337 頁。
- ◆ 已正確設定 Log Server 以便從 Filtering Service 接收記錄資訊。請參閱[Log Server 配置](#)，第 338 頁。

## 資料庫分割區

Websense 的 Log 記錄儲存在資料庫中的分割區。視您的資料庫引擎與配置而定，可以根據大小或日期來建立新的分割區。

您可以啓動或停用 Websense Manager 中的個別分割區。如果您嘗試根據儲存在已停用之分割區上的資訊來產生報告，就會找不到資訊，且報告會空白。

若要確認適當的資料庫分割區已啓動：

1. 前往**設定 > 報告 > 記錄資料庫**。
2. 向下捲動到**可用的分割區**區段。
3. 針對其中包含報告要包括之資料的每個分割區，標記它們的**啓動**核取方塊。
4. 按一下**立即儲存**以執行變更。

## SQL Server Agent 工作

有可能 SQL Server Agent 資料庫工作已停用。爲了讓 ETL 資料庫工作可以將 Log 記錄處理到資料庫中，此工作必須執行。

如果您是使用 MSDE 執行：

1. 前往**開始 > 系統管理工具 > 服務**。
2. 請確定 SQL Server 和 SQL Server Agent 兩者都已啓動。如果您是從 Websense, Inc. 取得 MSDE，這些服務的名稱是 MSSQL\$WEBSSENSE 和 SQLAgent\$WEBSSENSE。

如果您執行的是完整 Microsoft SQL Server，請詢問「資料庫管理員」以確認 SQL Server Agent 工作是否正在執行中。

## Log Server 配置

Websense Manager 與 Log Server 中的配置設定必須正確，才能確保 Log Server 會收到來自 Filtering Service 的記錄資訊。否則，記錄資料絕不會處理到記錄資料庫中。

首先，確認 Websense Manager 已成功連接到 Log Server。

1. 使用無條件「超級管理員」權限登入 Websense Manager。
2. 前往**設定 > 一般 > 記錄**。
3. 輸入 Log Server 所在位置的**電腦名稱**或**IP 位址**。
4. 輸入 Log Server 正在監聽的**連接埠** (預設值為 55805)。
5. 按一下**檢查狀態**來判斷 Websense Manager 是否能夠與指定的 Log Server 進行通訊。

此時會出現一個訊息來表示是否通過連接測試。如有需要，可更新 IP 位址或電腦名稱和連接埠，直到測試成功。

6. 完成之後，按一下**確定**來快取您的變更。按一下**全部儲存**才能使變更生效。

下一步，確認「Log Server Configuration」公用程式中的設定。

1. 在執行 Log Server 的電腦上，前往**開始 > 程式集 > Websense > 公用程式 > Log Server Configuration**。
2. 在**連接**標籤上，確認「連接埠」與 Websense Manager 中輸入的值相符。
3. 按一下**確定**來儲存任何變更。
4. 使用**連接**標籤上的按鈕來停止然後重新啟動 Log Server。
5. 按一下**退出**以關閉 Log Server Configuration 公用程式。

## 「今天」或「記錄」頁面上沒有顯示圖表

在使用委派管理的組織內，檢閱委派管理角色的報告權限。如果沒有選擇**檢視「今天」與「記錄」頁面上的報告**，那麼針對該角色中的委派管理員，這些圖表就不會顯示。

在使用多個 Policy Servers 的環境中，安裝的 Log Server 只會與單一個 Policy Server 通訊。您必須登入該 Policy Server 才能檢視「今天」與「記錄」頁面上的圖表，或存取其他報告功能。

## 無法存取某些報告功能

如果您的網頁瀏覽器以嚴格的設定執行快顯封鎖功能，它可能會封鎖某些報告功能。若要使用那些功能，您必須降低封鎖等級或整個停用快顯封鎖。

## Microsoft Excel 輸出缺少某些報告資料

Microsoft Excel 工作表中可開啓的最大列數為 65,536。如果您將具有 65,536 列以上記錄的報告匯出到 Microsoft Excel 格式，那麼工作表中會看不到第 65,537 列及之後的所有記錄。

爲了確保可在匯出的報告中存取所有資料，執行下列其中一項：

- 針對簡報報告，編輯報告篩選器以定義較小的報告，您可以設定較短的資料範圍、選擇較少的使用者與群組，或選擇較少的動作。
- 針對調查報告，向下查看資料，以定義較小的報告。
- 選擇其他匯出格式。

## 將簡報報告輸出儲存爲 HTML

如果您直接從「報告」>「簡報報告」頁面產生報告，有 3 種顯示格式可以選擇：HTML、PDF 及 XLS。如果您選擇 HTML 顯示格式，可以在 Websense Manager 視窗中檢視報告。

不建議從瀏覽器列印與儲存簡報報告。列印輸出會包括整個瀏覽器視窗，而且開啓已儲存的檔案會啓動 Websense Manager。

若要更有效地列印或儲存報告，請選擇 PDF 或 XLS 做爲輸出格式。如果本機電腦上已安裝了檢視軟體 (Adobe Reader 或 Microsoft Excel)，您就可以立即開啓這些檔案類型。您也可以將檔案儲存到磁碟 (如果沒有適當的檢視軟體可用，這是唯一的選項)。

當您在 Adobe Reader 或 Microsoft Excel 中開啓報告之後，可使用該程式的列印與儲存選項來產生需要的最終輸出。

## 調查報告搜尋問題

與搜尋調查報告有關的潛在問題有兩個。

- ◆ 無法輸入延伸 ASCII 字元
- ◆ 可能找不到搜尋模式

### 延伸 ASCII 字元

在主要調查報告頁面上的橫條圖上方的「搜尋」欄位，可讓您在所選的圖表要素中搜尋特定詞或字串。

如果您是在 Linux 伺服器上使用 Mozilla Firefox 來存取 Websense Manager，就無法在這些欄位中輸入延伸 ASCII 字元。這是 Linux 上之 Firefox 的已知限制。

如果您必須在調查報告中搜尋包含延伸 ASCII 字元的字串，請從 Windows 伺服器使用任何支援的瀏覽器來存取 Websense Manager。

### 找不到搜尋模式

針對主要調查報告頁面上「搜尋」欄位中輸入的模式，調查報告有時會找不到與該模式相關聯的 URL。如果發生此狀況，而且您非常確信該模式存在於報告的 URL 中，請嘗試輸入另一個也可以找到想要的 URL 的模式。

## 一般調查報告問題

- ◆ 有些查詢需要很長的時間。您可能會看到空白畫面或表示查詢已逾時的訊息。發生此情況的可能原因如下：
  - Web 伺服器逾時
  - MSDE 或 Microsoft SQL Server 逾時
  - 代理或快取伺服器逾時您可能必須手動增加這些元件的逾時限制。
- ◆ 如果使用者不在任何群組中，他們也不會出現在網域中。「群組」及「網域」兩個選擇將會沒有作用。
- ◆ 即使 Log Server 記錄的是造訪次數而不是點選次數，調查報告仍會將此資訊的標籤設為**點選次數**。

## 疑難排解工具

---

- ◆ [「Windows 服務」對話方塊](#)，第 340 頁
- ◆ [Windows 事件檢視器](#)，第 340 頁
- ◆ [Websense 記錄檔](#)，第 341 頁

### 「Windows 服務」對話方塊

在 Microsoft Windows 電腦上，Filtering Service、Network Agent、Policy Server、User Service，以及所有 Websense 無障礙識別代理程式都會以服務方式執行。您可以使用「Windows 服務」對話方塊來檢查這些服務的狀態。

1. 在「Windows 控制台」中，開啓**系統管理工具**資料夾。
2. 連按兩下**服務**。
3. 捲動服務清單，找到您要疑難排解的服務。

服務項目包括服務名稱、簡短的服務說明、服務狀態 (已啓動或已停止)、服務如何啓動，以及服務用來執行其工作的帳戶。

4. 連按兩下服務名稱可以開啓內容對話方塊，其中有關於該服務的更多詳細資訊。

### Windows 事件檢視器

「Windows 事件檢視器」會記錄有關 Windows 事件 (包括服務活動) 的錯誤訊息。這些訊息可協助您識別可能導致網際網路篩選或使用者識別問題的網路或服務錯誤。

1. 在「Windows 控制台」中，開啓**系統管理工具**資料夾。
2. 連按兩下**事件檢視器**。

3. 在「事件檢視器」中，按一下**應用程式**，取得錯誤訊息、警告及資訊訊息的清單。
4. 捲動清單，找到來自 Websense 服務的錯誤或警告。

## Websense 記錄檔

Websense 軟體會將錯誤訊息寫入 **websense.log** 檔案，此檔案位於 Websense **bin** 目錄 (預設為 C:\Program Files\WebSense\bin 或 /opt/WebSense/bin)。

此檔案中的資訊可比得上「Windows 事件檢視器」中的資訊。在 Windows 環境中，「事件檢視器」是以對使用者更友善的格式來顯示訊息。不過，**websense.log** 檔案可在 Linux 系統中檢視，而且如果您需要協助疑難排解問題，也可以傳送到「Websense 技術支援部」。



# 索引

## A

- Active Directory
  - 原生模式，57
- ActiveX 內容
  - 移除，132
- Applet
  - 配額時間，41
- ASCII 字元，延伸
  - 搜尋調查報告，339

## B

- BCP，269
- BrandWatcher，27

## C

- Content Gateway，236

## D

- DC Agent，185，237
  - 設定，186
  - 疑難排解，316
- DMZ，139，140

## E

- eDirectory，58
- eDirectory Agent，194，238
  - 主控台模式，322
  - 設定，196
  - 診斷，321
  - 疑難排解，320
- eDirectory 伺服器複本
  - 設定，197
- ETL 工作，278
- Excel 格式
  - 報告不完整，339
  - 稽核記錄，244
  - 調查報告，103，121
  - 簡報報告，87，96，100
- Explorer for Linux，83，263

## F

- Filtering Service，235
  - IP 位址變更，314
  - 更新 UID，315
  - 詳細資料頁面，243
  - 資料庫下載，243
  - 摘要圖表，22
  - 說明，242

## H

- HTML 格式
  - 儲存簡報報告，339
  - 簡報報告，87
- HTML 格式，簡報報告，96
- HTTP Post，275

## I

- IP 位址變更
  - Policy Server，240

## J

- JavaScript 內容
  - 移除，132

## L

- LDAP
  - 字元集，59
  - 自訂群組，60
- Linux 報告，83，263
- Log Server，237，261
  - 未安裝，332
  - 更新使用者 / 群組資訊，268
  - 使用代理伺服器，276
  - 配置，338
  - 配置公用程式，262，263，267
  - 停止，267，268，276
  - 啟動，267，268，276
  - 連接到目錄服務，336
  - 與記錄資料庫的連接，270

驗證, 275, 276  
Log 記錄, 134  
Logon Agent, 187, 238  
    設定, 188  
    疑難排解, 318

**M**  
Master Database, 29, 235  
    下載, 29  
    下載狀態, 243  
    下載問題, 305  
    下載排程, 30  
    加強, 274  
    即時安全性更新, 30  
    即時更新, 29  
    通訊協定, 34  
    類別, 34  
    繼續下載, 244  
Microsoft Excel  
    報告不完整, 339  
Microsoft SQL Server, 261  
Microsoft SQL Server Desktop Engine, 261  
MSDE, 261  
MyWebsense 入口網站, 26

**N**  
NetBIOS  
    啟用, 319  
Network Agent, 235, 293  
    本機設定, 297  
    全域設定, 296  
    和 Remote Filtering, 138  
    封鎖網路卡, 299  
    硬體配置, 294  
    超過 2 個網路卡, 314  
    監控網路卡, 298  
    網路卡配置, 298  
    與 Filtering Service 通訊, 314  
Novell eDirectory, 58

**O**  
ODBC, 269

**P**  
PDF 格式  
    調查報告, 103, 121, 123  
    簡報報告, 87, 95, 100  
Policy Broker, 235  
    和 Policy Database, 238  
Policy Database, 235, 238  
Policy Server, 235, 239  
    多個實例, 240  
    多個實例, 設定記錄, 265  
    和 Policy Database, 238  
    和 Websense Manager, 239  
    從 Websense Manager 中移除, 239  
    新增至 Websense Manager, 239  
    變更 IP 位址, 240

**R**  
RADIUS Agent, 190, 238  
    設定, 192  
Remote Filtering, 137  
    Client, 236  
    DMZ, 139, 140  
    Server, 236  
    VPN 支援, 142  
    支援的通訊協定, 137, 138  
    失敗則關閉, 142, 143  
    失敗則關閉逾時, 142, 143  
    和 Network Agent, 138  
    活動訊號, 139, 140  
    記錄檔, 140, 144  
    設定, 143  
    通訊, 141  
    無法開啓, 141  
    網路內部, 139  
    網路外部, 140  
    頻寬篩選, 137  
Remote Filtering Client, 138  
Remote Filtering Server, 137

**S**  
Security Gateway, 236  
SiteWatcher, 27  
SNMP 警示, 249  
SQL Server



- 權限, 333
- SQL Server Agent
  - 工作, 337
- Sun Java System Directory, 58
- T**
- TCP 和 UDP 支援, 47
- ThreatWatcher, 27
- Trap 伺服器
  - SNMP 警示通知, 249
- U**
- Usage Monitor, 236
- User Service, 56, 237
- V**
- VPN
  - Remote Filtering, 142
  - 分割通道, 142
- W**
- WebCatcher, 274
- Websense Explorer for Linux, 83, 263
- Websense Manager, 17, 235
  - Websense 標題, 19
  - 工作階段逾時, 18
  - 使用 Websense 使用者帳戶存取, 218
  - 使用網路帳戶存取, 217
  - 停用逾時, 22
  - 啟動, 17
  - 登入, 17
  - 管理員同時存取, 228
  - 管理員存取, 216
  - 瀏覽, 19
- Websense Master Database, 29
- Websense Web Protection Services, 27
- Websense 使用者帳戶, 208, 218
  - WebsenseAdministrator, 17
  - 密碼, 208
  - 新增, 219
  - 管理, 220
- Websense 狀態, 252
  - 今天, 21
  - 記錄, 23
  - 稽核記錄, 244
  - 警示, 252
- Websense 配置資訊, 238
- Websense 軟體
  - 元件, 234
- websense.log, 341
- WebsenseAdministrator, 17, 207
  - 刪除, 206
  - 使用者, 205, 206
  - 密碼, 207
- WebsenseAdministrator 密碼
  - 重設遺失, 26
- Windows
  - 事件檢視器, 340
  - 服務對話方塊, 340
- Windows Active Directory (原生模式), 57
- Windows NT Directory / Active Directory (混合模式), 57
- X**
- XLS 格式
  - 稽核記錄, 244
  - 調查報告, 103, 123
  - 簡報報告, 87, 96
- 符號**
- 「URL 存取」工具, 173
- 「URL 類別」工具, 172
- 「測試篩選」工具, 172
- 「編輯通訊協定」按鈕, 151
- 「編輯類別」按鈕, 151
- 「調查使用者」工具, 173
- 「檢查政策」工具, 172
- 三畫**
- 大量複製工具程式 (BCP), 269
- 工作
  - ETL, 278
  - IBT, 278
  - SQL Server Agent, 337
  - 記錄資料庫, 278
  - 記錄資料庫 維護, 278
  - 排程的調查報告, 120, 122
  - 排程的簡報報告, 96, 100

- 工作佇列
  - 調查報告, 102, 122
  - 簡報報告, 88
- 工作階段, 瀏覽, 282
- 工作階段逾時, 18
- 工具
  - URL 存取, 173
  - URL 類別, 172
  - 尋找使用者選項, 173
  - 測試篩選, 172
  - 調查使用者, 173
  - 檢查政策, 172
- 工具箱, 171
- 已快取的變更, 19
- 已封鎖且已鎖定, 230
  - 通訊協定, 231
  - 檔案類型, 231
  - 關鍵字, 230
  - 類別, 230
- 已封鎖的要求, 已記錄的頻寬, 111
- 已重新分類的 URL, 158
  - 已說明, 151
  - 未套用, 330
  - 新增, 160
  - 編輯, 160
- 已記錄的頻寬, 已封鎖的要求, 111
- 四畫**
  - 今天的值圖表, 21
  - 今天頁面, 21
    - 自訂, 22
    - 健全度警示摘要, 21
    - 圖表, 21
  - 元件, 234
    - DC Agent, 237
    - eDirectory Agent, 238
    - Filtering Service, 235
    - Log Server, 237
    - Logon Agent, 238
    - Master Database, 235
    - Network Agent, 235
    - Policy Broker, 235
    - Policy Database, 235
    - Policy Server, 235
    - RADIUS Agent, 238
    - Remote Filtering Client, 138, 236
    - Remote Filtering Server, 137, 236
    - Usage Monitor, 236
    - User Service, 237
    - Websense Content Gateway, 236
    - Websense Manager, 235
    - Websense Security Gateway, 236
    - 記錄資料庫, 237
- 允許, 39
- 允許所有使用者存取的 URL, 159
- 內容
  - 分類, 129
  - 掃描, 127, 130
- 內容抽除, 132
- 公用程式
  - Log Server Configuration, 267
- 分割區
  - 刪除, 262, 286
  - 建立, 284
  - 記錄資料庫, 277
  - 針對報告選取, 285
  - 變換選項, 280
- 分類內容, 129
- 切換角色, 208
- 升級
  - 找不到使用者, 304
- 手動驗證, 177
  - 啓用, 178
- 日期範圍
  - 調查報告排程工作, 121
  - 簡報報告排程工作, 99
- 五畫**
  - 主要標籤, 19
  - 主動式內容
    - 移除, 132
  - 主控台模式
    - eDirectory Agent, 322
  - 代理伺服器
    - Log Server 使用, 276
    - 資料庫下載配置, 31
  - 代理設定
    - 資料庫下載, 307
    - 驗證, 307

- 加強記錄, 270
- 失敗批次檔, 284
- 失敗則關閉
  - Remote Filtering, 142, 143
  - 逾時, 142, 143
- 未篩選的 URL, 151, 158
  - 未套用, 330
  - 定義, 159
- 正規表示式, 151, 170
  - 在限制存取篩選器中, 148
  - 和未篩選的 URL, 159
  - 重新分類 URL, 153
- 永不掃描清單, 129
  - 刪除項目, 133
  - 新增網站, 133
- 永遠掃描清單
  - 刪除項目, 133
  - 新增網站, 133
- 用戶端, 53
  - 使用者, 53, 56
  - 指派政策, 69, 70
  - 套用政策, 53
  - 移至角色, 63
  - 新增, 61
  - 群組, 56
  - 電腦, 53, 55
  - 管理, 54
  - 網路, 53, 55
  - 編輯, 62
  - 選取簡報報告, 90
- 用戶端, 受管理, 206
  - 在角色中新增, 211
  - 具有多個角色, 214, 225
  - 指派給角色, 214, 222, 225
  - 重疊的角色, 226
  - 套用政策, 216
  - 從角色中刪除, 222, 228
  - 移至角色, 210
- 目前的篩選負載圖表, 21
- 目錄
  - 報告, 86
  - 資料庫, 277
- 目錄服務
  - Log Server 連接至, 336
  - Windows NT Directory / Active Directory (混合模式), 57
    - 為 Websense Manager 登入設定, 217
    - 設定, 56
    - 搜尋, 62
  - 目錄設定
    - 進階, 59
- 六畫
  - 全域目錄, 57
  - 全部允許篩選器, 48
    - 和管理角色, 211
    - 與篩選優先權, 72
  - 全部封鎖篩選器, 48
    - 與篩選優先權, 72
  - 全部儲存, 19
  - 列印
    - 今天頁面, 22, 253
    - 記錄頁面, 24
    - 調查報告, 124
    - 簡報報告, 96
  - 向下查看, 標準報告, 104
  - 合併
    - Log 記錄, 262, 273
    - 與完整 URL 記錄, 281
    - 與網際網路瀏覽時間, 336
  - 多個 Policy Server, 240
  - 多個角色, 權限, 209
  - 多個政策
    - 篩選優先權, 53
  - 多個群組政策, 71
  - 字元集
    - MBCS, 304
    - 搭配 LDAP 使用, 59
  - 存取 Websense Manager, 17, 212
  - 安全性通訊協定群組, 39
  - 安全性類別, 36
  - 安全封鎖頁面, 264
  - 有條件政策權限, 207
  - 有條件超級管理員, 207
  - 自行報告, 124, 226
    - 啟用, 265
    - 設定, 291
    - 通知使用者, 291

- 自訂
  - 今天頁面，22
  - 封鎖訊息，77
  - 記錄頁面，24，25
- 自訂 LDAP 群組，60
  - 新增，60
  - 管理，220
  - 編輯，60
- 自訂 URL
  - 已定義，158
  - 篩選優先權，158
- 自訂封鎖訊息，77
- 自訂通訊協定，160
  - 建立，164
  - 重新命名，163
  - 無法建立，330
  - 編輯，162
  - 識別碼，162
- 自訂標誌
  - 封鎖頁面，79
  - 簡報報告，89，93
- 自訂類別，152
  - 建立，151
  - 重新命名，154
  - 新增，155
  - 編輯，152
- 七畫**
- 估計
  - 時間節省，25
  - 頻寬節省，25
- 刪除永遠掃描或永不掃描清單的項目，134
- 刪除受管理的用戶端，330
- 即時安全性更新，30，253
- 即時掃描，127
  - 設定，129
  - 概覽，128
  - 資料庫更新，128
- 即時資料庫更新，29，253
- 即時選項，130，134
  - 分類內容，129
  - 抽除內容，132
  - 報告，134
  - 儲存變更，133
  - 檔案掃描，131
- 完整 URL 記錄，262，274，281
- 快取檔案
  - 記錄，271
- 快速入門教學課程，18
  - 啟動，18
- 快顯封鎖
  - 報告存取，338
- 我的最愛
  - 調查報告，102，118，119，120
  - 簡報報告，84，86，87，93，94
- 技術支援，32
- 找不到使用者
  - 升級之後，304
- 更新即時掃描資料庫，128
- 系統警示，246
  - 設定，249
- 角色
  - 切換，208
  - 用戶端位於多個，226
  - 全部允許篩選器於，211
  - 名稱，220
  - 刪除，220
  - 刪除，影響，227
  - 刪除用戶端，222
  - 刪除超級管理員，206，227
  - 刪除管理員，222
  - 建立政策，215
  - 建立篩選器，215
  - 重疊的用戶端，214
  - 套用政策，211，216
  - 超級管理員，205，206，207
  - 新增，220，221
  - 新增受管理的用戶端，211，214，222，225
  - 新增管理員，222，224
  - 管理，206
  - 管理員具有多個，224
  - 編輯，221
  - 編輯政策，215
  - 編輯篩選器，215
  - 篩選器鎖定，影響，229
  - 優先順序，220，227
  - 檢視定義，214

- 鎖定通訊協定，231
- 鎖定類別，230
- 防火牆設定
  - 資料庫下載，307
- 八畫**
- 事件檢視器，340
- 使用自訂篩選器，59
- 使用更為嚴格的封鎖，146
  - 使用限制存取篩選器，146
- 使用者，53，56
  - 手動驗證，177
  - 無障礙識別，175
  - 識別，175
  - 識別遠端，141
- 使用者每日 / 每月活動細節報告，102，111
- 使用者每日活動細節報告，112
  - 類別對應，114
- 使用者每月活動細節報告，113
- 使用者帳戶
  - Websense，208，218
  - WebsenseAdministrator，205，206，207
  - 密碼，208
  - 新增 Websense，219
- 使用者設定檔
  - 登入指令碼問題，320
- 使用者搜尋，62
- 使用者資訊，記錄，265
- 使用者識別
  - 手動，177
  - 無障礙，175
  - 疑難排解，315
  - 遠端使用者，176
- 使用者識別頁面，177
- 使用配額時間，40
  - 封鎖頁面按鈕，40
- 使用警示，247
  - 記錄類別，265
  - 通訊協定，設定，251
  - 通訊協定，新增，252
  - 類別，設定，250
  - 類別，新增，251
- 取得支援，32
- 受管理的用戶端，206
  - 在角色中新增，211
  - 指派給角色，222，225
  - 從角色中刪除，222，228
  - 移至角色，210
- 委派管理
  - 存取 Websense Manager，216
  - 刪除角色，220
  - 刪除角色，影響，227
  - 快速入門，210
  - 角色衝突，226
  - 使用，220
  - 政策權限，207
  - 套用政策，211
  - 從角色刪除用戶端，228
  - 設定，210
  - 通知管理員，212
  - 報告存取，262
  - 報告權限，207
  - 新增角色，220，221
  - 新增管理員，224
  - 概覽，205
  - 編輯角色，221
  - 篩選器鎖定，229
- 委派管理員，208
- 延伸 ASCII 字元
  - 在 DC Agent 電腦名稱中，186
  - 在 eDirectory Agent 電腦名稱中，196
  - 在 Logon Agent 電腦名稱中，188
  - 在 RADIUS Agent 電腦名稱中，192
  - 搜尋調查報告，339
- 延伸的防護，36
- 抽除主動式內容，132
- 服務
  - 停止和啓動，245
- 服務對話方塊，340
- 狀態
  - 今天，21
  - 記錄，23
  - 稽核記錄，244
  - 警示，252
- 初始資料庫，29
- 九畫**
- 信任連接，271

- 信譽篩選，36
- 威脅
  - 在網頁中，130
  - 在檔案中，131
  - 掃描，130
- 威脅掃描，130
- 封鎖，39
  - 根據關鍵字，157
  - 通訊協定，161
  - 檔案類型，40，168
  - 關鍵字，40
- 封鎖的要求
  - 記錄的頻寬，104
- 封鎖頁面，75
  - 內容變數，79
  - 使用配額時間按鈕，40
  - 來源檔案，77
  - 密碼覆寫，41
  - 還原至預設，81
  - 繼續按鈕，40
  - 變更標誌，79
- 封鎖訊息
  - 自訂，77
  - 建立自訂，77
  - 建立替代，81
  - 針對檔案類型，168
  - 通訊協定，76
  - 變更框架大小，78
- 封鎖網路卡，299
- 建立
  - 政策，68
  - 限制存取篩選器，69
  - 通訊協定篩選器，69
  - 類別篩選器，69
- 政策
  - 已定義，33，65
  - 列印成檔案，67
  - 多個群組，71
  - 決定是否適用，71
  - 重新命名，68
  - 套用至用戶端，69，70
  - 套用至使用者與群組，56
  - 套用至受管理的用戶端，211，216
  - 針對角色建立，215
  - 針對角色編輯，215
  - 強制執行，71
  - 無限制，65
  - 新增，67，68
  - 預設，66
  - 說明，68
  - 範例 - 一般使用者，65
  - 編輯，67，68
  - 複製到角色，67，149，210，211
  - 篩選優先權，72
  - 檢視，67
- 政策定義
  - 排程，69
- 政策配置
  - 還原預設值，49
- 政策權限，207，208
  - 有條件，207
  - 無條件，207
  - 釋放，212
- 流量控制，警示，247
- 活動訊號，Remote Filtering，139，140
- 紅色字體，標準報告，105
- 訂閱，26
  - MyWebsense 入口網站，26
  - 已到期，26
  - 已超出，26
- 訂閱密碼，26
  - 無效或到期，303
  - 輸入，27
  - 驗證，306
- 重設 WebsenseAdministrator 密碼，26
- 重新命名
  - 自訂通訊協定，163
  - 政策，68
  - 限制存取篩選器，148
  - 通訊協定篩選器，46
  - 類別，154
  - 類別篩選器，44
- 重新建立記錄資料庫的索引，283
- 重新整理
  - 記錄資料庫設定，279
- 限制存取篩選器，42，145
  - 正規表示式，148
  - 建立，147

- 重新命名，148
- 新增，69
- 篩選優先權，146
- 風險等級，36，263，264
  - 在報告中，264
  - 安全風險，38
  - 法律責任，37
  - 指派類別，264
  - 商業使用量，37
  - 損失，37，38
  - 網路頻寬損失，37
  - 選取調查報告，110
  - 選取簡報報告，90
- 十畫**
- 修補程式，26
- 原生模式
  - Active Directory，57
- 套用至用戶端，69
- 時間節省
  - 記錄頁面，23，25
- 特殊事件，35
- 記憶體需求
  - 資料庫下載，308
- 記錄
  - Remote Filtering，140
    - 已定義，263
    - 加強，270
    - 合併記錄，273
    - 即時選項，134
    - 即時選項與篩選的比較，135
    - 完整 URL，274，281
    - 使用者資訊，265
    - 匿名，266
    - 設定，265
      - 多個 Policy Server，265
    - 造訪次數，272
    - 插入方式，269
    - 策略，262
    - 稽核，244
    - 選擇性類別，262，266
    - 點選次數，272
    - 類別，265
  - 記錄快取檔案，271
  - 記錄頁面，23
    - 自訂，24，25
    - 圖表，24
  - 記錄通訊協定
    - 針對所有角色，231
  - 記錄插入方法，269
  - 記錄資料庫，237，261，262，263
    - IBT 工作，85，278
    - 大小，334
    - 工作，278
    - 未建立，333
    - 目錄資料庫，277
      - 合併，273
      - 作用中，279
    - 刪除錯誤，284
    - 信任連接，271
    - 建立分割區，284
      - 重新建立索引，283
      - 針對報告選取分割區，285
      - 針對調查報告連接，287
      - 設定，279
      - 無法使用，333
      - 資料庫分割區，277
      - 磁碟空間不足，334
      - 磁碟空間需求，262
      - 管理，263，278
      - 維護工作，278，283
      - 維護配置，283
      - 與 Log Server 的連線，270
      - 檢視錯誤記錄，286
      - 簡介，277
  - 記錄檔，341
    - Remote Filtering，144
  - 追蹤
    - 系統變更，244
    - 網際網路活動，246
  - 配置公用程式
    - Log Server，267
    - 存取，267
  - 配額，40
  - 配額時間，40
    - Applet，41
    - 工作階段，41
    - 在多 Policy Server 環境中，240

- 套用至用戶端，41
- 十一畫
- 停止
  - Log Server，267，268，276
  - Websense 服務，245
- 健全度警示，252
  - 解決方案，328
  - 摘要，21
  - 說明，327
- 偏好設定，報告，265
- 副檔名
  - 針對即時掃描，131
  - 新增到預先定義的檔案類型，169
  - 新增到檔案類型，170
  - 篩選依據，168
  - 屬於預先定義的檔案類型，168
- 動作，39
  - 允許，39
  - 封鎖，39
  - 封鎖檔案類型，40
  - 封鎖關鍵字，40
  - 配額，40
  - 確認，40
  - 選取簡報報告，92
- 動態內容
  - 分類，129
- 匿名記錄，266
- 執行 Websense Manager，17
- 密碼，26
  - Websense 使用者，208，218
  - Websense Administrator，207
  - 針對 Websense 使用者變更，219，220
- 密碼覆寫，41
  - 在多 Policy Server 環境中，240
- 將政策列印成檔案，67
- 將政策套用至用戶端，70
- 將網站移至另一個類別，160
- 帳戶資訊
  - 設定，27
- 掃描內容，127，129
- 掃描應用程式，131
- 掃描檔案，131
- 排程
  - 政策定義，69
  - 排程工作
    - 工作記錄，101
    - 日期範圍，99，121
    - 自訂電子郵件，100，121
    - 刪除，101
    - 停用，101
    - 排程，97，121
    - 啟動，101
    - 報告檔案名稱，86
    - 調查報告，102，120
    - 輸出格式，100
    - 簡報報告，96，98，100
  - 排程工作清單
    - 調查報告，122
    - 簡報報告，88
  - 排程器，簡報報告，96
  - 教學課程
    - 快速入門，18
  - 啟動
    - Log Server，267，268，276
    - Websense 服務，245
  - 啟動 Websense Manager，17
  - 混合模式
    - Active Directory，57
  - 異常值報告，102，122
  - 移至角色，63
    - 用戶端，210
  - 移除
    - VB Script 內容，132
    - 主動式內容，132
    - 永遠掃描或永不掃描清單項目，133
    - 來自 Websense Manager 的 Policy Server 實例，239
  - 細節檢視
    - 更改，108
    - 設定預設值，288
    - 調查報告，107
    - 欄位，109
  - 設定
    - Network Agent，296
    - Policy Server，239
    - Remote Filtering，143
    - 目錄服務，56
    - 即時掃描，129



- 使用者識別, 177
  - 記錄資料庫, 279
  - 帳戶, 27
  - 登入目錄, 217
  - 資料庫下載, 30
  - 篩選, 49
  - 警示與通知, 248
  - 設定即時選項, 129
  - 設定標籤, 19
  - 通訊協定
    - TCP 和 UDP 支援, 47
    - 已定義, 29, 34
    - 已新增至 Master Database, 35
    - 未記錄, 337
    - 安全性通訊協定群組, 39
    - 收集使用資訊, 28
    - 定義, 160
    - 定義自訂, 151
    - 所有清單, 35
    - 封鎖訊息, 76
    - 建立新的, 162
    - 重新命名自訂, 163
    - 修改 Websense 定義, 166
    - 針對所有角色記錄, 231
    - 針對所有角色鎖定, 230, 231
    - 管理, 151
    - 篩選, 46, 161
    - 選取調查報告, 110
    - 選取簡報報告, 91
    - 頻寬使用量, 166
  - 通訊協定使用警示
    - 設定, 251
    - 新增, 252
  - 通訊協定篩選器, 42
    - 已定義, 33
    - 建立, 45
    - 重新命名, 46
    - 新增, 69
    - 範本, 45, 49
    - 編輯, 46
  - 通訊協定識別碼, 162
    - IP 位址, 163
    - 連接埠, 162
  - 造訪次數
    - 已定義, 272
    - 記錄, 262, 272
- ## 十二畫
- 備份 Websense 資料, 253
  - 備份公用程式, 253
  - 報告
    - Linux, 83, 263
    - 不完整, 339
    - 元件, 261
    - 存取, 262
    - 自行報告, 226
    - 即時選項, 134
    - 快顯封鎖, 338
    - 使用, 83
    - 使用者每日活動細節, 112
    - 使用者每月活動細節, 113
    - 空, 337
    - 保留, 86
    - 偏好設定, 265
    - 設定自行報告, 291
    - 設定電子郵件伺服器, 265
    - 設定調查, 287
    - 設定權限, 223
    - 策略, 262
    - 逾時, 334
    - 電子郵件發佈, 265
    - 管理員, 214, 229
    - 管理員限制, 209
    - 調查, 83, 84
    - 簡報, 83
    - 權限, 207, 209, 216, 223
  - 報告目錄, 86
    - 名稱, 92
  - 報告標題, 簡報報告, 93
  - 報告篩選器, 簡報報告, 86, 87, 88
    - 確認, 94
    - 選取用戶端, 90
    - 選取風險等級, 90
    - 選取動作, 92
    - 選取通訊協定, 91
    - 選取類別, 90
  - 尋找產品資訊, 26
  - 替代封鎖訊息, 81

- 測試篩選
  - 尋找使用者，173
- 無法開啓
  - Remote Filtering，141
- 無限制政策，65
- 無條件超級管理員，207，222
- 無障礙使用者識別，175
  - DC Agent，185
  - eDirectory Agent，194
  - Logon Agent，187
  - RADIUS Agent，190
  - 代理程式，175
  - 設定，177
- 登入，17
- 登入目錄
  - 定義，217
- 登入指令碼
  - 使用者設定檔問題，320
  - 啓用 NetBIOS，319
  - 網域控制站能見度問題，319
- 登入錯誤，330
- 評估篩選政策，83
- 診斷
  - eDirectory Agent，321
- 超級管理員
  - WebsenseAdministrator，17
  - 切換角色，208
  - 有條件，207
  - 刪除角色，206，227
  - 角色，205，206，207
  - 將用戶端新增到角色，210
  - 從角色移動用戶端，210，211
  - 無條件，207，222
  - 複製政策，211
  - 複製篩選器，211
  - 篩選器鎖定，影響，229
  - 權限，207
- 開啓資料庫連接 (ODBC)，269
- 順序
  - 篩選，72
- 十三畫**
- 圓形圖，105
- 搜尋
  - 目錄用戶端，62
  - 從網址列，311
  - 調查報告，106，339
- 搜尋模式
  - 調查報告，339
- 新增
  - 永遠掃描或永不掃描清單項目，133
  - 用戶端，61
  - 自訂 LDAP 群組，60
  - 到 Websense 定義的通訊協定，166
  - 政策，68
  - 限制存取篩選器，147
  - 通訊協定篩選器，45
  - 檔案類型，169
  - 關鍵字，157
  - 類別篩選器，43
- 群組，56
- 解除封鎖 URL，159
- 資料庫
  - Master Database，29
  - Policy Database，238
  - 目錄，277
  - 即時安全性更新，30
  - 即時資料庫更新，29
  - 記錄資料庫，277
  - 記錄資料庫工作，278
  - 記錄資料庫分割區，277
  - 針對即時掃描，128
  - 維護工作，283
- 資料庫下載，29
  - 即時安全性更新，30
  - 即時更新，29
  - 即時掃描，128
  - 狀態，243
  - 訂閱問題，306
  - 限制應用程式問題，309
  - 記憶體需求，308
  - 設定，30
  - 透過代理伺服器，31
  - 疑難排解，305
  - 磁碟空間需求，307
  - 繼續，244
  - 驗證網際網路存取，306
- 資料庫工作
  - ETL，278

- SQL Server Agent, 337
- 網際網路瀏覽時間 (IBT), 278
  - 維護, 278
- 資料庫分割區
  - 刪除, 283, 286
  - 建立, 284
  - 針對報告選取, 285
  - 變換選項, 280
- 資料庫引擎
  - 支援的, 261
- 資料庫更新, 29
  - 即時, 29, 253
  - 即時安全性, 30, 253
  - 即時掃描, 128
- 逾時
  - 停用 Websense Manager, 22
  - 報告, 334
- 電子郵件
  - 報告發佈, 265
- 電子郵件訊息
  - 自訂調查報告, 121
  - 自訂簡報報告, 100
- 電子郵件警示, 248
- 電腦
  - 用戶端, 53
- 預設使用者, 206, 207
  - 刪除, 206
- 預設政策, 66
  - 套用錯誤, 318
- 十四畫**
- 圖表
  - Filtering Service 摘要, 22
  - 今天的值, 21
  - 今天頁面, 21
  - 目前的篩選負載, 21
  - 記錄頁面, 24
  - 選擇今天頁面, 22
- 摘要報告
  - 多層級, 107
  - 調查報告, 104
- 疑難排解工具
  - websense.log, 341
  - 事件檢視器, 340
  - 服務對話方塊, 340
- 監控網路卡, 298
- 磁碟空間
  - 記錄資料庫需求, 262
  - 資料庫下載需求, 307
  - 簡報報告使用量, 86
- 管理角色, 206
- 管理員, 206
  - Websense 使用者帳戶, 218
  - 同時存取相同的角色, 228
  - 存取 Websense Manager, 217
  - 有條件政策權限, 207
  - 告知職責, 212
  - 具有多個角色, 209, 224, 228
  - 委派, 208
  - 委派的工作, 213
  - 追蹤所做的變更, 244
  - 從角色中刪除, 222
  - 報告, 206, 214, 229
  - 報告權限, 207, 223
  - 無條件政策權限, 207
  - 超級管理員, 207
  - 超級管理員的工作, 210
  - 新增到角色, 222, 224
  - 概覽, 206
  - 篩選器鎖定, 影響, 229
  - 檢視角色定義, 214
  - 權限, 207
  - 權限, 設定, 222, 225
- 網域控制站
  - 測試能見度, 319
- 網路
  - 用戶端, 53
- 網路卡配置, 294
  - 封鎖, 299
  - 設定, 298
  - 監控, 298
- 網路配置, 294
- 網路帳戶
  - 定義登入目錄, 217
- 網路認證
  - 存取 Websense Manager, 217
- 網際網路瀏覽時間 (IBT)
  - 已說明, 85
  - 配置, 282

- 報告, 282
- 資料庫工作, 85
- 與合併, 336
- 閱讀時間, 282, 283
- 維護工作
  - 記錄資料庫, 278, 283
  - 設定, 283
- 遠端使用者, 識別, 141
- 十五畫**
- 彈出式警示, 248
- 標準報告, 調查, 102, 116
- 標誌
  - 簡報報告, 89
  - 變更封鎖頁面, 79
- 標誌, 簡報報告, 93
- 標題, 簡報報告, 93
- 確認, 40
  - 在多 Policy Server 環境中, 240
- 稽核記錄, 244
- 範本, 48
  - 政策, 65
  - 通訊協定篩選器, 45, 49
  - 類別篩選器, 43, 48
- 範例
  - 政策, 65
  - 類別和通訊協定篩選器, 48
- 範例 - 一般使用者政策, 65
- 編輯
  - 用戶端設定, 62
  - 自訂 LDAP 群組, 60
  - 政策, 68
  - 限制存取篩選器, 148
  - 通訊協定篩選器, 46
  - 類別篩選器, 44
- 複製
  - 限制存取篩選器, 43
  - 通訊協定篩選器, 43
  - 簡報報告, 88
  - 類別篩選器, 43
- 複製到角色, 149
  - 政策, 67
  - 篩選器, 43
- 調查報告, 83, 84, 261
- Excel 格式, 103, 121, 123
- PDF 格式, 103, 121, 123
- XLS 格式, 123
- 工作佇列, 102, 122
- 列印, 124
- 多層級摘要, 107
- 存取, 24
- 自行報告, 124, 291
- 自訂電子郵件, 121
- 我的最愛, 102, 118, 119
- 使用者每日活動細節, 112
- 使用者每月活動細節, 113
- 使用者活動, 102
- 紅色字體, 105
- 匿名, 106
- 排程工作, 102, 120
- 異常值, 102, 122
- 細節檢視, 107, 108, 109
- 設定, 287
- 設定排程, 121
- 圓形圖, 105
- 搜尋, 106, 339
- 搜尋模式, 339
- 概覽, 102
- 預設設定, 288
- 摘要, 104
- 標準, 102, 116
- 橫條圖, 105
- 輸出選項, 289
- 選項, 103
- 選擇記錄資料庫, 287
- 儲存我的最愛, 118
- 隱藏使用者名稱, 106
- 顯示選項, 289
- 閱讀時間, 283
- 閱讀時間臨界值, 282
- 十六畫**
- 橫條圖, 105
- 篩選
  - 工具箱, 171
  - 使用關鍵字, 156
  - 動作, 39
  - 通訊協定, 161

- 順序, 71
- 圖表, 72
- 優先權, 72
- 優先權, 自訂 URL, 158
- 檔案類型, 168
- 篩選設定
  - 設定, 49
- 篩選器, 42
  - 全部允許, 211
  - 決定使用, 69
  - 限制存取, 42, 145
  - 針對角色建立, 215
  - 針對角色編輯, 215
  - 通訊協定, 33, 42
  - 編輯作用中, 70
  - 複製到角色, 149, 210, 211
  - 還原預設值, 49
  - 簡報報告, 86, 87
  - 類別, 33, 42
- 篩選器元件, 151
- 篩選器範本, 48
- 篩選器鎖定
  - 建立, 207, 230
  - 記錄通訊協定, 231
  - 設定, 210
  - 影響角色, 208, 215, 229
  - 鎖定通訊協定, 231
  - 鎖定檔案類型, 231
  - 鎖定關鍵字, 230
  - 鎖定類別, 230
- 輸出選項
  - 調查報告, 289
- 選項, 調查報告, 103
- 選擇性類別記錄, 262, 266
- 選擇性驗證, 179
- 遺失 Websense Administrator 密碼, 26
- 錯誤記錄
  - Websense.log, 341
  - 事件檢視器, 340
  - 針對記錄資料庫刪除, 284
  - 針對記錄資料庫檢視, 286
- 頻寬
  - 大於預期, 336
  - 依通訊協定使用, 166
  - 依類別使用, 166
  - 記錄封鎖的要求, 104
  - 設定限制, 167
  - 管理, 166
- 頻寬節省
  - 記錄頁面, 23, 25
- 頻寬類別, 36
- 十七畫**
  - 優先順序, 角色, 220, 227
  - 優先權
    - 委派管理角色, 226
    - 篩選, 72
    - 篩選政策, 53
  - 儲存簡報報告, 96
  - 應用程式掃描, 131
  - 檔案名稱
    - 排程的簡報報告, 86
  - 檔案掃描
    - 副檔名, 131
    - 設定大小上限, 131
  - 檔案掃描的大小上限, 131
  - 檔案類型, 151
    - 封鎖, 40
    - 針對角色鎖定, 231
    - 新增, 169
    - 編輯, 169
  - 檢查政策
    - 尋找使用者, 173
  - 檢視擱置中的變更, 20
  - 聯絡技術支援, 26
  - 還原 Websense 資料, 253
  - 還原公用程式, 253
  - 隱藏使用者名稱
    - 調查報告, 106
  - 點選次數
    - 已定義, 272
    - 記錄, 262
- 十八畫**
  - 擷取、轉換以及載入 (ETL) 工作, 278
  - 瀏覽 Websense Manager, 19
  - 瀏覽工作階段, 282
  - 瀏覽時間
    - 網際網路 (IBT), 85, 282

- 簡報報告, 83, 261
  - Excel 格式, 87, 96, 100
  - HTML 格式, 87, 96
  - PDF 格式, 87, 95, 100
  - XLS 格式, 87, 96
  - 工作佇列, 88, 100
  - 工作記錄, 101
  - 列印, 96
  - 自訂標誌, 89, 93
  - 我的最愛, 84, 86, 87, 93, 94
  - 保留, 86
  - 執行, 95
  - 排程, 88, 96, 97
  - 設定工作的日期範圍, 99
  - 報告目錄, 86
  - 報告目錄名稱, 92
  - 報告篩選器, 86, 87, 88
  - 概覽, 84
  - 磁碟空間使用量, 86
  - 確認報告篩選器, 94
  - 複製, 88
  - 輸出格式, 100
  - 儲存, 96
  - 檔案名稱, 86
- 覆寫動作
  - 通訊協定, 163
  - 類別, 153
- 十九畫**
  - 識別碼
    - 通訊協定, 162
  - 關鍵字, 151, 156
    - 未封鎖, 311
    - 定義, 157
    - 封鎖, 40
    - 針對角色鎖定, 230
  - 關鍵字封鎖
    - 疑難排解, 311
  - 類別, 35
    - 已定義, 29, 34
    - 已新增至 Master Database, 35
    - 安全性, 36
    - 自訂, 152
    - 延伸的防護, 36
    - 所有清單, 34
    - 重新命名自訂, 154
    - 特殊事件, 35
    - 記錄, 265
    - 針對所有角色鎖定, 230
    - 新增自訂, 155
    - 編輯自訂, 152
    - 選取簡報報告, 90
    - 頻寬, 36
    - 頻寬使用量, 166
  - 類別使用警示
    - 刪除, 250
    - 設定, 250
    - 新增, 251
    - 與記錄, 265
  - 類別對應
    - 使用者活動細節報告, 114
  - 類別管理, 151
  - 類別篩選器, 42
    - 已定義, 33
    - 建立, 43
    - 重新命名, 44
    - 新增, 69
    - 範本, 43, 48
    - 編輯, 44
    - 複製, 43
- 二十畫**
  - 繼續按鈕, 40
  - 警示, 252
    - SNMP, 249
    - Websense 健全度, 252
    - 即時安全性更新, 253
    - 即時資料庫更新, 253
  - 系統, 246
    - 系統, 設定, 249
    - 防止過多, 247
    - 健全度摘要, 21
    - 設定方法, 248
    - 設定限制, 248
    - 通訊協定使用, 247
    - 通訊協定使用, 設定, 251
    - 通訊協定使用, 新增, 252
    - 傳送方法, 247

電子郵件，248  
彈出式，248  
類別使用，247  
類別使用，設定，250  
類別使用，新增，251  
釋放政策權限，212

## 二十一畫

欄位  
    針對細節調查報告，109

## 二十二畫

權限，206  
    SQL Server，333  
    多個角色，209  
    安裝磁碟機，333  
    有條件政策，207  
    政策，207，208

設定，222，223，225  
報告，207，209，216  
無條件政策，207  
釋放政策，212

## 二十三畫

變更  
    快取，19  
    儲存，19  
    檢閱，20  
變更 URL 類別，160  
變更角色，208  
變換選項，資料庫分割區，280  
顯示選項  
    調查報告，289  
驗證  
    Log Server，275，276  
    選擇性，179

