Installation Organizer

Websense Web Security Solutions
Version 7.7.x

Use the Installation Organizer to gather hardware, network, and deployment planning information prior to installing your Websense Web Security solution.

Warning
Some stages of installation require account passwords. If you note passwords here, **keep this document secure**. Alternatively, write down only account user names in the document, but have the passwords ready when needed during the installation process.

Important
Use this completed organizer as an aid while following instructions in the Deployment and Installation Center. Do not use this organizer in place of the detailed installation instructions.

The Installation Organizer includes the following sections:

Use only the sections that apply to your planned deployment.

1. Hardware Setup

Quick Start Guide	Use the information on the Quick Start Guide, included in the shipping box, to place and connect your appliance.
Internet access	Network interface C and the proxy interface (typically P1) must be able to access a DNS server. Because enforcement components download essential databases through these interfaces, both typically have continuous Internet access. Ensure that interfaces C and P1 can access the download servers at **download.websense.com**. (Some sites configure the P1 interface to download the Websense Master Database and other security updates so that interface C does not require Internet access.) Make sure that the download site is permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the C and P1 interfaces can access.

2. Initial Configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for network interface C and a few other general items. Gather the following information before running the script. Some of this information may have been written down on the Quick Start Guide during hardware setup.

Item	Description or Note	Value
Hostname	Hostname for the appliance	Name:
C network interface	IPv4 address of the interface. (All Websense component IP addresses must be in IPv4 format.)	IP address: _____._____._____._____
	Subnet mask	Mask: _____._____._____._____
	Default gateway *(optional)* If interface C does not have Internet access, you must configure either P1 or P2 to allow Master Database downloads. Configure P1 and P2 in Appliance Manager, and use TRITON - Web Security to configure the proxy for database downloads.	IP address *(optional)*: _____._____._____._____
	Primary DNS server	IP address: _____._____._____._____
	Secondary DNS server *(optional)*	IP address *(optional)*: _____._____._____._____
	Tertiary DNS server *(optional)*	IP address *(optional)*: _____._____._____._____

Item	Description or Note	Value
Unified password	Unified password for Appliance Manager, the TRITON console, and Content Gateway Manager.	Password (8-15 characters, at least 1 letter and 1 number): (Warning: if password noted here, keep this document secure.)

3. Appliance Manager Initial Configuration

Appliance Manager is the Web-based configuration interface for the appliance. After running the firstboot script, use Appliance Manager to configure network interfaces N and P1 (and optionally P2), used for communications by Network Agent and Websense Content Gateway. Appliances also offer expansion interfaces (E1 and E2) that can be bonded with P1 and P2, respectively, for load balancing or standby, if Websense Email Security Gateway is not running on the appliance.

Gather the following information before running Appliance Manager. Some of this information may have been written on the Quick Start Guide during hardware setup.

Item	Description or Note	Value
NTP Server	Primary	Domain:
	Secondary (optional)	Domain:
	Tertiary (optional)	Domain:
P1 and P2 network interfaces Note: If you do not provide access to the Internet for interface C, then you must configure either P1 or P2 to receive Master Database downloads from Websense. This extra step must be done through the Appliance Manager (to configure P1 and P2) and through the TRITON - Web Security console (to configure the proxy for database downloads).	IP address for network interface P1	IP address: _____._____._____._____
	Subnet mask for network interface P1	Mask: _____._____._____._____
	Default gateway for network interfaces P1 (and P2)	IP address: _____._____._____._____
	Primary DNS server for network interfaces P1 (and P2)	IP address: _____._____._____._____
	Secondary DNS server for network interfaces P1 (and P2) *Optional*	IP address: _____._____._____._____
	Tertiary DNS server for network interfaces P1 (and P2); (IP address) *Optional*	IP address: _____._____._____._____
	IP address for network interface P2 *Required only if P2 is enabled*	IP address: _____._____._____._____
	Subnet mask for network interface P2 *Required only if P2 is enabled*	Mask: _____._____._____._____

Item	Description or Note	Value
Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic.	Can be either the C or N network interface.	Choose one: ☐ Interface C ☐ Interface N
Bidirectional span port if N interface is used	If the N network interface transports blocking information, it must be connected to a bidirectional span port.	(N/A)
N network interface	IP address for network interface N	IP address: _____._____._____._____
	Subnet mask for network interface N	Mask: _____._____._____._____
	Default gateway for network interface N *Required only if network interface N carries blocking information*	IP address: _____._____._____._____
	Primary DNS server for network interface N	IP address: _____._____._____._____
	Secondary DNS server for network interface N *Optional*	IP address: _____._____._____._____
	Tertiary DNS server for network interface N *Optional*	IP address: _____._____._____._____
Bond expansion interface E1 to P1? *Optional (not applicable when Web and Email Security solutions are on the appliance)*		☐ Yes ☐ No If Yes (choose one): ☐ Active/standby ☐ Load balancing
Bond expansion interface E2 to P2? *Optional (not applicable when Web and Email Security solutions are on the appliance)*		☐ Yes ☐ No If Yes (choose one): ☐ Active/standby ☐ Load balancing
Policy Source IP address	If this is the full policy source appliance, leave this blank. Specify a policy source IP address if: ◆ This is a user directory and filtering appliance ◆ This is a filtering only appliance	IP address: _____._____._____._____

Item	Description or Note	Value
TRITON - Web Security (user interface for Websense Web Security)	If TRITON - Web Security runs on another machine (recommended), enter its IP address here. If TRITON - Web Security runs on this appliance, leave this blank.	IP address: _____._____._____._____

4. Directory Service

If your network includes one of the supported directory services listed below, you can apply Web filtering to individual users, groups, and domains (OUs). Additionally, you can install an optional transparent identification agent to ensure clients in a supported directory service are filtered without being prompted to log on when they open a browser. (If no directory service is installed, Websense Web Security uses IP addresses to apply filtering policies.)

For organizations where multiple administrators may access the TRITON console, administrators with accounts in most supported directory services can log on with their network credentials.

Microsoft Active Directory 2003 or 2008	Specific permissions need to be granted to Websense Logon Agent to run with 2008.
Novell eDirectory 8.7 or later	NMAS authentication is supported.
Other LDAP-based service	
RADIUS server	Most standard RADIUS servers. The following RADIUS servers have been tested: ◆ Livingston (Lucent) 2.x ◆ Cistron RADIUS server ◆ Merit AAA ◆ Microsoft IAS

5. Subscription Key

After installation, enter a valid subscription or evaluation key in TRITON - Web Security.	Key:

6. Additional Machines for Reporting, Hybrid Security, and Data Security Linking Components

Web Security Log Server, Sync Service, and Linking Service do not run on the appliance.

Item	Description or Note	Value
Log Server	Enter the IP address of the machine on which Log Server will be installed.	IP address: _____._____._____._____
Sync Service	Enter the IP address of the machine on which Sync Service will be installed.	IP address: _____._____._____._____
Linking Service	Enter the IP address of the machine on which Linking Service will be installed.	IP address: _____._____._____._____

1. Required Software and Integration Details

Item	Description or Note	Value
Integration product	Make sure any **third-party** firewall, proxy, or network appliance that you plan to integrate with Websense software is installed and running before you install Websense software. This does not apply if you plan to integrate with Websense Content Gateway. Check the Deployment and Installation Center for supported integration products and versions and information about standalone deployments.	Integration product: _____ Version:_____
Directory service	If you plan to use a directory service, such as Windows® Active Directory®, to identify users, the directory service must be installed and configured.	(N/A)

2. Network

Item	Description or Note
Internet access	To download the Master Database (required), each Filtering Service machine must be able to access the following URLs: ◆ download.websense.com ◆ ddsdom.websense.com ◆ ddsint.websense.com ◆ my.websense.com
Websense Filtering Service	Filtering Service machines must be able to communicate with the integration product (if any) and Websense Network Agent (if installed).
Websense Network Agent	If Network Agent is used, it must be deployed where it can see all internal Internet traffic for the network segment that it is assigned to monitor.
Websense User Service	User Service must be able to communicate with the directory service to enable user- and group-based filtering.

3. Websense Filtering Service

Enter the following information for the machine that will host Filtering Service. If you will have multiple Filtering Service machines, make separate note of the same items for each additional machine

Item	Description or Note	Value
Machine name	Hostname for the Filtering Service machine	Name:
IP address	IP address of this machine. If there are multiple NICs, enter the IP address of the one chosen for Websense-software communication (see below).	IP address: _____._____._____._____
Domain/User name	Log in as a user with domain and local administration privileges to install Websense software	Domain/user: Password: (Warning: if password noted here, keep this document secure.)
Communication port	Port used by Filtering Service to communicate with other Websense components (default 15868)	Port:
Communication NIC (only if multiple NICs)	If there are multiple network interface cards (NICs), you must choose which one is used by Websense software for communication. Enter a description (e.g., device name) and the IP address of the NIC to be used for this purpose.	Description: IP address: _____._____._____._____

4. Websense Policy Broker and Policy Server

Enter the following information for the machine that will host Policy Broker and Policy Server. Additional instances of Policy Server may be deployed on other machines, if needed.

Item	Description or Note	Value
Machine name	Hostname of the Policy Broker machine	Name:
IP address	IP address of this machine. If there are multiple NICs, enter the IP address of the one chosen for Websense-software communication (see below).	IP address: _____._____._____._____
Domain/user name	Log in as a user with domain and local administration privileges to install Websense software	Domain/user: Password: (Warning: if password noted here, keep this document secure.)

Item	Description or Note	Value
Communication port for Policy Broker	Port used by Policy Broker to communicate with other Websense components (default 55880)	Port:
Communication port for Policy Server	Port used by Policy Server to communicate with other Websense components (default 55806)	Port:
Communication NIC (only if multiple NICs)	If there are multiple network interface cards (NICs), you must choose which one is used by Websense software for communication. Enter a description (e.g., device name) and the IP address of the NIC to be used for this purpose.	Description: IP address: _____._____._____._____

5. Network Agent (optional)

Enter the following information for the machine that will host Network Agent. In some cases, Network Agent is installed on the same machine as Filtering Service. If you will deploy multiple instances of Network Agent, make separate note of the same items for each additional machine. In a multiple-Network-Agent deployment, each instance is assigned a particular segment of the network to monitor. See the Network Agent Quick Start for configuration instructions.

Item	Description or Note	Value
Machine name	Hostname of the Network Agent machine	Name:
IP address	IP address of this machine. If there are multiple NICs, enter the IP address of the one chosen for Websense-software communication (see below).	IP address: _____._____._____._____
Domain/user name	Log in as a user with domain and local administration privileges to install Websense software	Domain/user: Password: (Warning: if password noted here, keep this document secure.)

Item	Description or Note	Value
Communication NIC (only if multiple NICs)	If there are multiple NICs, you must choose which one is used by Websense software for communication. Enter a description (e.g., device name) and the IP address of the NIC to be used for this purpose.	Description: IP address: _____._____._____._____
Monitoring NIC (only if multiple NICs)	You must also choose which NIC or NICs will be used by Network Agent for monitoring traffic. This can be the same as the communication NIC. Enter a description and the IP address of each of the NICs to be used for this purpose. If more than one, note this information separately for each additional NIC. Note: NICs used by Network Agent for monitoring must support **promiscuous** mode.	Description: IP address: _____._____._____._____ Description: IP address: _____._____._____._____

6. Database Location

The Websense Log Database is maintained on Microsoft SQL Server or SQL Server Express (see the Deployment and Installation Center for supported versions).

Item	Description or Note	Value
Machine IP address or hostname	Enter the IP address or hostname of the machine on which Microsoft SQL Server is running.	IP address: _____._____._____._____ (or) Hostname:
Path to database files	Enter the path to the directory in which Log Database files should be stored. If the database engine is on the installation machine, the default path is **C:\Program Files (x86)\Websense\Web Security**. If the database engine is on another machine, the default location is **C:\Program Files\Microsoft SQL Server** on that machine.	Path: (Note: the path you specify must already exist.)

7. Database Access

A Windows trusted connection or Microsoft SQL Server database account can be used to create and access the Websense Log Database.

Item	Description or Note	Value
Trusted user	If a Windows trusted connection will be used to access the Log Database, log onto the installation machine with an account that is also a trusted user on the database engine machine. The account must have proper privileges to access the Log Database (see the requirements below).	Domain/user: Password: (Warning: if password noted here, keep this document secure.)
Database account	The account must be a member of all of the following roles: ◆ dbcreator server role ◆ db_owner on msdb ◆ one of the following on msdb: ■ SQLAgentOperatorRole ■ SQLAgentReaderRole ■ SQLAgentUserRole	User: Password: (Warning: if password noted here, keep this document secure.)

8. Global Security Administrator

Item	Description or Note	Value
admin user	**admin** is the built-in Global Security Administrator for the TRITON Unified Security Center. During installation, you create a password for this user. It is a best practice to enter a password that is **very strong** (at least 8-characters long, containing all of the following: uppercase characters, lowercase characters, numbers, and symbols)	Password: (Warning: if password noted here, keep this document secure.)

9. Subscription Key

After installation, enter a valid subscription or evaluation key in TRITON - Web Security to download the Master Database and start filtering.	Key:

10. Windows Directory Service Access

Item	Description or Note	Value
Domain Admin user	Websense User Service, DC Agent, and Logon Agent query a domain controller to identify users. If you install any of these components, you must supply the domain/user name and password for a **domain admin** user on the domain controller for the users you wish to identify.	Domain/user: Password: (Warning: if password noted here, keep this document secure.)

11. Installation Location

Item	Description or Note	Value
Installation directory	By default, Websense software is installed in: ◆ **C:\Program Files (x86)\Websense\ Web Security** (Windows) ◆ **/opt/Websense** (Linux) If you want to install elsewhere, enter the location here.	Installation directory:

Make sure an administrator is available during the deployment to help resolve any connectivity and access issues.

Websense Content Gateway is a high-performance Web proxy that provides real-time threat protection and Web data loss prevention (DLP) support for Web Security Gateway and Gateway Anywhere. It can be deployed on 1 or more V-Series appliances or dedicated servers.

Use this organizer if Content Gateway is being installed on a dedicated Linux server. See *V-Series Appliance* if Content Gateway is being deployed on a Websense appliance.

1. Deployment preparation

Item	Description	Value
Rollout plan	Is there a phased plan for installing, configuring, testing, and moving into full production with Content Gateway? A phased approach is highly recommended and produces the best results.	☐
System security: Outside intrusion	How will you secure the Content Gateway host system? ◆ IPTables ◆ External firewall ◆ Other Who needs to know about this activity? Who needs to assist in this activity?	☐ ☐ ☐
Network configuration: Client request routing	How will client requests be routed to Content Gateway? **Explicitly** ◆ What browsers will be used? ◆ Who will prepare the PAC file? ◆ What must be in the PAC file? ◆ How will the PAC file be distributed to clients? See PAC File Best Practices. **Transparently** ◆ What network devices are effected? ◆ How must they be changed? ◆ Who will make the changes?	☐ ☐
Content Gateway configuration: proxy clusters	Will multiple Content Gateway servers be deployed in a cluster? All nodes in the cluster share a common name. What is the name?	☐ Name:
Content Gateway configuration: proxy cache	Will Content Gateway cache content? Are the cache disks properly sized and formatted? 148GB max; raw device (created with mknod)	☐ ☐

Item	Description	Value
Content Gateway configuration: Protocols handled	What traffic will Content Gateway proxy? ◆ HTTP requests ◆ HTTPS requests ◆ FTP requests ◆ DNS requests ◆ PUTS and POSTS through TRITON - Data Security to perform Web DLP	☐ ☐ ☐ ☐ ☐
Content Gateway configuration: user authentication	How will users be authenticated or identified? ◆ Integrated Windows Authentication ◆ NTLM ◆ LDAP ◆ RADIUS ◆ Multiple Realm Authentication ◆ Websense transparent identification agents	☐ ☐ ☐ ☐ ☐ ☐

2. Access (Physical and Logical)

Item	Description	Value
In preparation of Content Gateway software installation, are all systems powered and running?	Content Gateway Linux servers (see the Deployment and Installation Center for hardware and software requirements). TRITON Unified Security Center machine	☐ ☐
Cisco routers and switches	If you are using Cisco devices for transparent routing, they must have IOS version 12.x or later. You should also visit the Cisco support site to view their list of known problems and to acquire and apply needed patches.	http://www.cisco.com/en/US/products/hw/switches/
Content Gateway system **hostname**	Name of Content Gateway host system. It is very important that the hostname be properly entered in the **/etc/hosts** file. See the Installation Guide.	Hostname:
Content Gateway **admin** account password	The administrator password, set during installation (software) or the firstboot process (appliance). 8-15 characters.	Password: (Warning: if password noted here, keep this document secure.)
Network: base attributes	Identify network attributes. DNS IP address should be included in **/etc/resolv.config**.	Net mask: ____.____.____.____ Default Gateway: ____.____.____.____ DNS: ____.____.____.____

Item	Description	Value
Network IP addresses: network segments	Specify internal IP address ranges to be monitored	Internal networks:
IP address: Management interface (MGMT_NIC)	The physical interface used by the system administrator to manage the computer.	IP address: ____.____.____.____
IP address: Client-facing interface (CLIENT_NIC)	The physical interface used by clients to request data from the proxy.	IP address: ____.____.____.____
IP address: Internet-facing interface (WAN_NIC)	The physical interface used to request pages from the Internet (usually the most secure interface).	IP address: ____.____.____.____
IP address: Cluster interface (CLUSTER_NIC)	The physical interface used by the proxy to communicate with members of the cluster.	IP address: ____.____.____.____
TRITON - Web Security Policy Server IP address and mask	The IP address of the TRITON - Web Security Policy Server interface.	IP address: ____.____.____.____
TRITON - Web Security Filtering Service IP address and mask	The IP address of the TRITON - Web Security Filtering Service interface. May be the same as the Policy Server IP address.	IP address: ____.____.____.____
TRITON console user name and password	The default Global Security Administrator account is **admin**. This account cannot be deleted or renamed. Additional Web or Data Security Super Administrator accounts can be created as needed.	User name: _____ Password: _____ (Warning: if password noted here, keep this document secure.)
IP address of TRITON Unified Security Center machine	Used to register with Web DLP to register Content Gateway with TRITON - Data Security.	IP address: ____.____.____.____
Web Security Gateway Anywhere subscription key	Content Gateway typically receives key information automatically from Policy Server, if a key has been entered in the TRITON console.	Key:
Sites with special requirements	Prepare a list of hosts and Web sites that have special requirements, such as access control lists (ACLs) and security key fobs.	

Item	Description	Value
Internal networks that should bypass Content Gateway	Prepare a list of any internal networks that should not go through the proxy. It is highly recommended that all intranet traffic bypass the proxy.	

3. Corporate

Item	Description	Value
Web and Data security team members	Who in my organization is involved in this rollout? Who are my contacts at Websense?	
Change control	Is there a change control process, and has it been followed?	☐
End-user communication	Have communiques been prepared for end users prior to rollout?	☐
Helpdesk procedure and incident escalation	Has Helpdesk (or equiv) been notified and properly prepared for incident management?	☐

4. Environmental

Item	Description	Value
Contingency plan	Is there a plan in place for fallback?	☐
Backup / recovery third-party agents	Do you have a backup and recovery plan?	☐

Make sure an administrator is available during the deployment to help resolve any connectivity and access issues.

Data Security components are installed on the TRITON management server and offer Web DLP capabilities for Websense Web Security Gateway Anywhere.

1. Access (Physical and Logical)

Item	Description	Value
Are all system modules powered on and running?	Web Security Gateway machines, including, V-Series appliances (if used).	☐
TRITON Unified Security Center password	Credentials for the **admin** account.	Password: _____ (Warning: if password noted here, keep this document secure.)
User directory service account	Does the application have a service account in Active Directory or other user directory service?	☐
Directory service access account	Required to import users and groups into TRITON - Data Security	User name: _____ Password: _____ (Warning: if password noted here, keep this document secure.)
User names and passwords for administrators of the Microsoft SQL Server database	SQL Server is used for the Data Security fingerprint database and incident and configuration database. Note user names and passwords for administrators who may need access to the database.	User name: _____ Password:_ _____ (Warning: if passwords noted here, keep this document secure.)
IP address of the Data Security Management Server machine	This is also the TRITON management server (on which all TRITON console components reside.	IP address: _____

2. Corporate

Item	Description	Value
Players	Do I know who will be involved?	☐
Change control	Is there a change control process, and has it been followed?	☐
End-user communication	Has a communication been prepared for end users prior to implementation?	☐
Helpdesk procedure and incident escalation	Has Helpdesk (or equiv) been notified and properly prepared for incident management?	☐

3. Environmental

Item	Description	Value
Contingency plan	Is there a plan in place for fail back?	☐
Backup / recovery third-party agents	Do you have a backup and recovery plan?	☐
Network	Identify network attributes	Net mask: ____.____.____.____ Gateway: ____.____.____.____ DNS: ____.____.____.____
Network IP addresses	Specify internal IP address ranges to be monitored	Internal networks:

Make sure an administrator is available during the deployment to help resolve any connectivity and access issues.