Deployment Planner Checklist and Worksheet

Websense® X10G™ Security Chassis and X10G™ Security Blades

Use this document to plan X10G Blade Chassis and X10G Security Blade deployments.

- Preparation (checklists)
- Hardware setup
- Software setup
- Post-installation verification

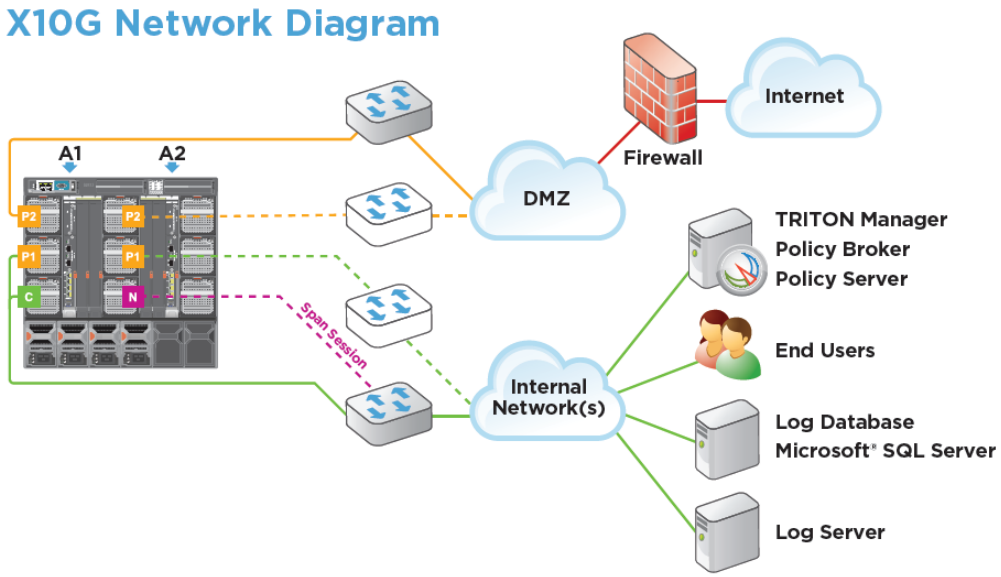
The Deployment Planner assumes a basic deployment done by skilled network technicians.

Values and choices for your system may be different. For deployment of additional components in more complex installations, please see the online ***Deployment and Installation Center***.

- Install an instance of Microsoft SQL Server 2005 or 2008 off-chassis in your network. The Log Database of reporting data is stored on that machine. Ensure that SQL Server is running.

- A few Websense components (such as the TRITON management console and reporting Log Server) also run off the chassis on Windows servers and must be installed separately. For best performance, Log Server should run on its own server (not combined with TRITON console). Use the TRITON Unified Installer to install all off-chassis Websense components.

- One off-chassis server must host Websense Policy Broker and one copy of Policy Server for your network (also stores your Policy Database). This server is known as the *policy source*. The same server that is used for the TRITON console is frequently used as the *policy source*.



Checklists

Hardware:

- ☐ Network Rack with 10U clearance (for X10G Chassis).
- ☐ Adequate power supply (208 - 240 volt AC input).
- ☐ External switch or router with:
    - 1G port for X10G Control Interface (C).
    - 1G port for Chassis Management Controller (CMC).
    - 10G port for Proxy interface 1 (P1) on leftmost chassis switch A1 (A1.P1).
    - 1G port for N Interface (N), optional. Filters mirrored data.
    - 10G ports for additional, optional proxy interfaces A1.P2, A2.P1, and A2.P2.

  Note "external switch" refers to your network switch or router, not the X10G chassis switches.

- ☐ Cat 5E or Cat 6 network cable to run from CMC to external (network) switch.
- ☐ X10G chassis, blades, and installation kit (cables, DVD, setup poster).
- ☐ Optical transceiver kit, if ordered. Required only if you plan to use fiber optic cable.
- ☐ Fiber optic cable (you provide this, if desired). Use OM3 or OM4, with a subscriber connector (SC) on one end, for connection to chassis. Other end needs appropriate connector for your external (network) switch.
- ☐ Separate Windows Server for running TRITON management console, Websense Policy Broker, and Policy Server. Should be running and accessible to all security blades. Blades will need to reference the machine running Policy Broker.
- ☐ Microsoft SQL Server (set up and running). *
- ☐ Separate Windows Server for running Websense Log Server.

  *See the *Deployment and Installation Center* guide for specific software versions.

Software:

- ☐ Websense TRITON Unified Installer for Windows. Download the executable from mywebsense.com. Use WebsenseTRITON763Setup.exe for all Windows components.

- ☐ Data Security Suite **Policy Engine** v7.6.3 for Linux. Your Websense Support professional will provide this rpm file and will SSH into each blade to install the latest Web DLP Policy Engine.

Access:

- ☐ Synchronized clock source (NTP) or reliable time source for time synchronization. Important! Time must be consistent across all servers used for Websense Web Security Gateway modules.
- ☐ Optional laptop with browser access to network of CMC IP address (recommended) for verifying connectivity.

Passwords:

Default user name and password shown in parentheses. Keep a record of changed passwords. Note and keep handy all passwords for the following devices.

- ☐ CMC (root/calvin):
- ☐ Dell Remote Access Control (iDRAC) to slots (root/calvin):
- ☐ firstboot shared password:
- ☐ TRITON console:

Accounts:

- ☐ Windows Service Account:
- ☐ SQL Server Account:

Subscription Key:

- ☐ X10G security blade Websense subscription key:

Miscellaneous:

- ☐ Consistent time source. (Up to 3 time servers. Provide hostnames or IP addresses):

Network planning and IP addresses:

Sequential IP address assignment for related X10G interfaces is recommended. Examples provided for guidance only.

- ☐ 3 Windows servers – need IP addresses:
  - TRITON console with policy source (Policy Broker and Policy Server):
  - Log Server:
  - MS SQL Server:
- ☐ Reserve IP address ranges for X10G interfaces, within distinct subnets.
  - A1.P1 and A1.P2 should be within different subnets.
  - CMC port, blade iDRAC ports, and switch management ports should be within a separate subnet.
- ☐ IP address for CMC: x.x.x.100
- ☐ Sequential IP addresses for iDRAC to each chassis slot: (such as .101 to .116)
- ☐ IP address of chassis switch A1: x.x.x.117
- ☐ IP address of chassis switch A2: x.x.x.118
- ☐ Sequential range for C interfaces on blades (typically on separate management subnet)
  - IPs: x.x.x.201 – x.x.x.216
- ☐ IP address for N interface on blade in slot 16 (if Network Agent is used)
  - IP: x.x.x.137 (This one IP address is not currently used, but it must be assigned.)
- ☐ Sequential range of IP addresses for A1.P1 interface on each blade, recommended in subnet different from subnet with C interfaces.
- ☐ Sequential range of IP addresses for optional A1.P2 interface on each blade (if used for failover), required to be in subnet different from subnet with A1.P1 interfaces.

X10G Security Blade Configuration Worksheet

Slot # _____ *(Slot 1 must always have a blade in it.)*

Use this form to plan and record information needed for each blade. Use the data for software setup steps.

Firstboot information	
Hostname:	DNS Primary:
C IP:	DNS Secondary:*
Subnet Mask:	DNS Tertiary:*
Default Gateway:*	Password:
System Time and Date	
NTP Primary:	NTP Secondary:*
Websense Content Gateway Interfaces	
A1.P1 IP :	A1.P2 IP:*
A1.P1 Subnet mask:	A1.P2 Subnet mask:*
Default Gateway:	Primary DNS:
Secondary DNS: *	Tertiary DNS: *
Network Agent Interface (slot 16 only)*	
N IP:	Subnet:
Default Gateway:	Primary DNS:
Secondary DNS: *	Tertiary DNS: *
Is this blade the policy source? *(Best practice is to install policy source off-chassis.)*	
☐ Full policy source *(not best practice)* ☐ User directory and filtering ☐ Filtering Only	
Policy source IP address (typically on Windows):	

* Optional

TRITON Unified Security Center	
Websense Web Security	**Microsoft SQL Server**
Policy source IP:	IP address:
Log Server IP:	User name:
Subscription Key:	Password:

Hardware Setup

Refer to the Websense Quick Start Poster and Getting Started Guide for hardware setup details.

1) Insert the security blades into the chassis. The first slot (slot 1) must always have a blade inserted. Top blades slide smoothly when hanging from top rail. Do not force them.
2) Connect proxy A1.P1 and optional A1.P2 cabling. Use the SFP+ copper cables provided. If you ordered the optional optical transceiver kit, follow the kit instructions and connect the appropriate fiber optic cables. Connect the SC end of the fiber optic cable to the chassis side.
3) Connect remaining network cabling per Websense Quick Start Poster.
4) Connect 4 power cables to power packs on back of chassis.
5) Connect a Cat 5E or Cat 6 cable from the leftmost CMC network port to a switch on the network for the CMC and iDRAC remote management.
6) Power on the chassis and blades.
7) Set the CMC IP address, using the small LCD screen at the lower left at the front of the chassis.
8) Access the CMC with a browser using its IP address as the URL.
9) Assign the blade slot iDRAC addresses using the **Server Overview**, **QuickDeploy** option.
10) Follow the instructions in the next section to do a base configuration using the *firstboot* script.

Software Setup

For all blade servers: X10G Security Blade ***firstboot*** script (base configuration) is required:

1) Power on chassis and security blades, if not already on.
2) Using the IP address of the CMC as its URL, access the CMC from a browser that has connectivity to that network.
3) Log on to the CMC console.
4) Select "SLOT-N" from the list on the left, where "N" is the blade you wish to configure.
5) Click **Launch Remote Console** for this security blade.
6) The **Remote Console** (CLI) opens.
7) Accept the subscription agreement.
8) Type **yes** to run the ***firstboot*** script.
9) Blade in Slot 16 only: select the option to run Network Agent if you want to use Network Agent to scan protocol traffic (recommended). If Network Agent is not chosen, switch A2 can be reconfigured to support (optional) proxy failover for this blade. See the *Getting Started* Guide for details.
10) Enter the security blade's desired hostname (such as: chassis1_blade1.yourcompany.com).
11) Enter C interface IP address.
12) Enter the Subnet mask.
13) Enter the Default Gateway IP address.
14) Enter the Primary/Secondary/Tertiary DNS IP addresses.
15) Enter the password to be used for the security blade. This password will be used later for: Security Blade Manager, Content Gateway Manager, and the on-blade TRITON - Web Security manager (demo use only).
16) Verify the information on the Initial Configuration Summary, and select **Yes** if satisfied with settings.

The ***firstboot*** script needs approximately 5 to 10 minutes to complete the initial configuration. Repeat ***firstboot*** steps for next blade, or move to the following section of this Checklist when all blades have been booted.

Important!

After ***firstboot***, before configuring the proxy interfaces on the blades, ensure that a *full policy source* machine is set up and running.

Best practice is to set up a *full policy source* machine on an off-chassis Windows server (recommended).

For off-chassis *full policy source* on Windows:

1. Make sure SQL Server 2005 or 2008 is already installed and running in the network. You need the IP address for that machine and the SQL Server credentials.

2. The TRITON Windows installer will guide you through the installation. [For assistance with off-chassis installation steps, see the online topic listed below.] You need the Websense Web Security installer for Windows.

   The filename is WebsenseTRITON763Setup.exe.

   .

   Download it from the Downloads page at mywebsense.com.

   Run the TRITON Windows installer. On the Subscription Agreement screen, select *I accept this agreement* and then click **Next**. Choose to install only the Web Security module. (If your site uses Data Security components, that module may also be installed at this time.) When you reach the **Installation Type** screen, select **Custom** and choose these 2 components: **Policy Broker**, **Policy Server**. (Other optional components include transparent identification agents such as **DC Agent** and **Logon Agent**.) Follow the prompts to complete the installation. For additional details:

   http://www.websense.com/content/support/library/deployctr/v76/wwf_wws_sw_install.aspx

After ***firstboot*** has been run on a blade, use these steps to update the Policy Engine for Web DLP and configure proxy settings, time/date, and other options for the blade:

1) Ask your Websense Support professional to SSH into the security blade and install the v7.6.3 Policy Engine for Web DLP. This requires an rpm file provided by Websense support staff.
2) Next, open a browser and enter: http://*ip_address_C_interface* (for the selected blade).
3) Log on to the Security Blade Manager with user name ***admin*** and the password you created during ***firstboot***. You will now configure additional, initial settings for this one blade server.
4) In the left navigation pane, click **Configuration > System**.
5) Under **Time and Date**, set the time zone and the time and date. Click **Save**.
6) In the left navigation pane, click **Configuration > Network Interfaces**.
7) Enter the information from the configuration Worksheet for this blade (see prior section) into (a) the **Network Interfaces** page, then (b) the **Routing** page, and (c) the **Web Security Components** page. **Save** as you go.

8) Under **Web Security Components > Policy Source**, select either **User directory and filtering** or **Filtering only**. Enter the IP address of the off-chassis policy source machine. Click **Save**.
   Note: Do not proceed to do this same step on another blade until the communication between this blade and the off-chassis Policy Broker has had time to establish itself. Wait 5 to 10 minutes and watch for on-screen notification that the policy source has been set.
9) Ensure that the demo copy of the TRITON-Web Security console on the blade is disabled, as shown below:

10) Click **Save**.
11) Click **Log Off** at the top right when you have completed the configuration for this blade.
12) Set up the next blade by returning to Step 1 in this list.
13) If all blades have been set up and configured, finish installing off-chassis components (see following sections).

TRITON Unified Security Center Installation

After all blades have been set up and configured, finish installing additional off-chassis components. Install the TRITON console on a Windows server, separate from the X10G chassis and blades. This server can be the same server where you installed Policy Broker and Policy Server earlier.

NOTE: In large installations, Log Server (required) is best installed on a separate Windows server. See the *Deployment and Installation Center* for various deployment options.

Checklist

- ☐ Windows Server
- ☐ Static IP address for the Windows Server
- ☐ Websense Web Security installer for Windows.
  Obtain WebsenseTRITON763Setup.exe from the Downloads page at mywebsense.com.
- ☐ Windows Server joined to the domain (if using Windows Active Directory)
- ☐ Microsoft SQL Server should be installed and running.
- ☐ Microsoft SQL Server authentication credentials must be available.
- ☐ SMTP server to be used for system notifications must be identifiable.

1) Log on to the installation machine (Windows server) and copy or download WebsenseTRITON763Setup.exe from mywebsense.com.
2) Double-click the downloaded installer to launch the Websense TRITON installer.
3) On the welcome screen, click **Start**.
4) On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
5) On the **Installation Type** screen select **TRITON Unified Security Center** and the **Web Security** component, then click **Next**.
6) TRITON Infrastructure Setup is launched.
7) On the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
8) On the Installation Directory screen, specify the location where you want TRITON Infrastructure to be installed, and then click **Next**.
9) On the **SQL Server** screen, specify the location of your database engine and how you want to connect to it.
10) On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Unified Security Center.
11) On the **admin Account** screen, enter an email address and password for the default administration account for TRITON Unified Security Center, and then click **Next**.
12) On the **Email Settings** screen, enter information about the SMTP server to be used for system notifications, and then click **Next**.
13) On the **Pre-Installation Summary** screen, verify the information shown, and then click **Next** to begin the installation. The Installation screen appears. Wait until all files have been installed.
14) On the **Installation Complete** screen, click **Finish**.
15) Continue to the next section to set up the remaining off-chassis components.

Log Server and DC Agent Installation

Use these instructions to install and configure two important components off-chassis for a basic deployment: Web Security Log Server and DC Agent.

- DC Agent is a Websense transparent identification agent used in networks to authenticate users with a Windows directory service.
- Log Server receives records of Internet filtering activity and sends them to the Log Database, from which reports are prepared.

These components should be installed on a Windows server, separate from the X10G chassis. For larger installations, install them on a Windows server that is different from the server running the TRITON console. (See Step 13 below.)

Note: The Windows server must be joined to the domain, if you plan to install DC Agent. You must log on as the domain administrator.

See the *Deployment and Installation Center* for other deployment options.

1) Log on to the installation machine (Windows server) as domain administrator and copy or download WebsenseTRITON763Setup.exe from mywebsense.com.
2) Double-click the downloaded installer to launch the Websense installer.
3) On the **Welcome** screen, click **Start**.
4) On the **Subscription Agreement** screen, select **I accept this agreement**, and then click **Next**.
5) On the **Installation Type** screen, select **Custom.**
6) When returned to the Custom Installation screen, select **Install** to the right of Web Security.
7) On the Select Components screen, select **Log Server** and **DC Agent.** Click **Next**.
8) Follow the on-screen instructions and fill out the fields.
9) On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.
10) On the Pre-Installation Summary screen, verify the information shown.
11) Click **Next** to start the installation. An Installing progress screen is displayed. Wait for the installation to complete.
12) On the Installation Complete screen, click **Done**.

13) Log Server must be configured to use the same Policy Server instance as the one used by the TRITON – Web Security console. To set this up after installation on the Log Server machine:
    a. From the Windows Start menu, select Programs > Websense > Web Security > Web Security Log Server Configuration.
    b. The Log Server Configuration utility opens with the Connections tab selected.
    c. Use this tab to point Log Server to the Policy Server instance on the TRITON manager machine. Save your changes.

Transparent identification agent set up

Use these instructions to set up your transparent identification agent. Transparent identification agents allow Websense software to identify users without prompting them for logon information. This setup assumes you are using DC Agent and Active Directory. The setup for other agents is similar; see the *Deployment and Installation Center* for setting up other agents.

1) Launch the TRITON console by opening a browser and entering:
   http://<*ip_address*>:9443/triton
   where <*ip_address*> is the IP address of the machine on which TRITON Unified Security Center is installed.
2) Go to **TRITON Settings > Directory Services > Select Active Directory (Native Mode) > Add**. Enter the hostname or IP Address of the Global Catalog Server. Select **Full distinguished names** and enter the account information (domain\username and password). Click **OK** twice.
3) Ensure that you can add a Client under: **TRITON Settings > Policy Management > Clients > Add**.
4) Click **Directory Entries**.
   If you can browse the directory structure, you have successfully integrated with Active Directory. If you cannot browse the tree, recheck the account settings in Directory Services.
5) Websense recommends using the IP address of the DC Agent location instead of the hostname. Go to **Settings > User Identification > Transparent Identification Agents**. Select the hostname/server of the DC Agent. Change the hostname of the server to the IP Address of the DC Agent location (IP address of the TRITON console/reporting server).

Register Secondary Policy Servers (blade instances) in the TRITON Unified Security Center

Each blade on the X10G that runs in the mode **User directory and Filtering** is running an instance of **Policy Server**. Each instance of **Policy Server** running on a blade should be configured as a Secondary **Policy Server**, so that it uses the same subscription key as the Primary **Policy Server** (running on the Windows machine with **Policy Broker**).

1) Launch the TRITON console by opening a browser and entering:

   http://<*ip_address*>:9443/triton

   where <*ip_address*> is the IP address of the machine on which TRITON Unified Security Center is installed.
2) Use the **Settings** > **General** > **Policy Servers** page to associate a new **Policy Server** instance with TRITON - Web Security, or to update configuration information for an existing **Policy Server**.
3) Enter or edit the IP address (or name) and communication Port for the **Policy Server** instance. The default port is 55806.
4) Enter or update the Description of the selected **Policy Server** instance.
5) You cannot change the description for the base **Policy Server**.
6) Indicate whether this is a Primary or Secondary **Policy Server**.
   a. A primary Policy Server has a different subscription key from other Policy Server instances associated with TRITON - Web Security.
   b. A secondary Policy Server uses the same subscription key as another Policy Server that has already been associated with TRITON - Web Security.
7) Because you are registering a secondary **Policy Server**, select the IP address of the primary **Policy Server** from which the secondary should get its key, and then click **OK** to return to the Policy Servers page.
8) Be sure to register all secondary **Policy Servers** running on blades.
9) You must click **OK** on the Policy Servers page to cache your changes.
10) Changes are not implemented until you click **Save All**.

Register X10G blades to the TRITON Unified Security Center

1) Launch the TRITON console by opening a browser and entering:

   http://<*ip_address* >:9443/triton

   where <*ip_address*> is the IP address of the machine on which TRITON Unified Security Center is installed.
2) Log on to the TRITON console.
3) Go to **Appliances > Add**.
4) Enter the IP address of the C interface of a blade you want to register.
5) Click **Finish**.
6) Repeat for all other Websense X10G blade servers that you want to access through this TRITON console.

Deployment test

Perform a simple test to determine if your basic deployment is working correctly:

1) Launch the TRITON console by opening a browser and entering:

   http://<*ip_address* >:9443/triton

   where <*ip_ address*> is the IP address of the machine on which the TRITON console is installed.
2) Under **Main > Policy Management > Policies > Default Policy**, select the Category Filter and Protocol Filter that you wish to test with (such as: Monitor Only, Basic, Basic Security).
3) Modify the categories to the proper dispositions/actions for the testing. Select **OK** and **Save All**.
4) To test a specific user/workstation, configure the browser on that server to proxy to the blade or appliance in explicit mode. To do this:

   Launch **Internet Explorer > Tools > Internet Options > Connections > LAN Settings**. Enable "Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)" and "Bypass proxy server for local addresses" > Advanced. Enter the IP Address of the A1.P1 interface for HTTP using port 8080.
5) Close the browser and reopen. Attempt to browse to sites that should not be allowed, based on the categories you selected earlier.

Websense Technical Support offers a test page for all categories, including any Web sites that require real-time analysis: http://testdatabase.websense.com.