

v7.7.3 Release Notes for TRITON Unified Security Center

Topic 55420 / Updated: 22-January-2013

| | |
|--------------------|---|
| Applies To: | Websense TRITON Unified Security Center 7.7.3 |
|--------------------|---|

Use the Release Notes to find information about what's new and improved in Websense TRITON Unified Security Center Version 7.7.3.

Contents

- ◆ [TRITON Unified Security v7.7.3](#)
- ◆ [Hardware requirements](#)
- ◆ [Software support](#)
- ◆ [Installation](#)
- ◆ [Resolved and Known issues](#)

Through the TRITON Unified Security Center, you can manage Web Security, Data Security, and Email Security from the same management application.

The following release notes are available for this release:

- ◆ [Web Filter and Web Security](#)
- ◆ [Websense Content Gateway](#)
- ◆ [Data Security](#)
- ◆ [Email Security Gateway Anywhere](#)
- ◆ [V-Series Appliances](#)

TRITON Unified Security v7.7.3

Topic 55421 / Updated: 18-January-2013

| | |
|--------------------|---|
| Applies To: | Websense TRITON Unified Security Center 7.7.3 |
|--------------------|---|

Version 7.7.3 is a stability release that provides a small number of features and several important corrections for Websense TRITON Enterprise modules. The focus in this release is on responding to customer requests.

Deployment

Installation for Websense TRITON Enterprise and the modules in your subscription is performed with a single installer for the TRITON infrastructure and reporting database. From this installer you can launch the installation of the individual TRITON modules, as required.

An upgrade process for sites using Web Security, Data Security, and Email Security assists with upgrades from versions 7.5 and 7.6.

For more information, see [Installation](#), page 6.

Two-factor authentication for TRITON administrators

Beginning with version 7.7.0, if your organization uses a form of two-factor authentication (for example, Common Access Card authentication), you can configure the TRITON Unified Security Center to allow or require administrators to use two-factor authentication to log on to the TRITON console with Internet Explorer.

- ◆ When two-factor authentication is *allowed*, administrators not identified via two-factor authentication have the option of using password authentication.
- ◆ When two-factor authentication is *required*, password authentication cannot be used. There is one exception: an administrator can use password authentication on the TRITON management server machine to log on using the default admin account.

Enable two-factor authentication for the TRITON console on the **TRITON Settings > Certificate Authentication** page. (The term “certificate authentication” is used because the TRITON console uses client SSL certificate negotiation to enable support for multiple types of two-factor authentication.)

When certificate authentication is enabled for the TRITON console, it can also be enabled for Content Gateway Manager and Appliance Manager, to grant administrators single sign-on access to all three management consoles.

When certificate authentication is enabled, TRITON console password authentication:

- ◆ Is always available in one specific scenario: when an administrator uses the default admin account to log on to the TRITON console from the TRITON management server machine
- ◆ Can be disabled entirely, except for the scenario above
- ◆ Can be enabled for specific administrators as a backup method, in case certificate authentication fails
- ◆ Is supported only with Microsoft Internet Explorer

Using a non-standard port for the reporting database

Beginning with version 7.7.0, if you are using an existing standard or enterprise version of Microsoft SQL Server to host your reporting databases, you can specify a non-standard port for the database connection. You can specify the port:

- ◆ During TRITON Infrastructure installation. In this case, the port information is automatically passed to any key Web, Data, and Email Security reporting components that are installed on the TRITON management server.
- ◆ During custom installation of Web or Email Security Log Server on machines other than the TRITON management server.

Use the following syntax to specify a port during installation:

```
SQL_Server_location/optional_instance_name,port
```

For example:

```
10.15.130.1/websense,9999
```

If no port is specified, the default ODBC port (1433) is used.

It is not possible to use a non-standard SQL Server port if you are using SQL Server Express 2008 R2 (which is installed by the TRITON Unified Installer).

Use an existing encrypted connection for reporting DB

Beginning with v7.7.0, if your existing Microsoft SQL Server installation is configured to use an encrypted connection, you can configure TRITON software to encrypt communication with the reporting database.

- ◆ If you instruct your Websense software to use encryption, but your Microsoft SQL Server installation is **not** already set up to use encryption, the installer displays an error message and cannot proceed until you either deselect the encryption option or configure encryption within SQL Server.
- ◆ If your SQL Server installation supports both modes, the Websense installer always falls back to the un-encrypted mode (only during installation), even if you checked the 'encrypt connection' option.

After installation, TRITON components do work in encrypted mode. Only the initial communication between the installer and the SQL Server instance is not encrypted (even though you checked 'encrypt connection' during installation, and only with a SQL Server instance that supports both modes).

Hardware requirements

Topic 55422 / Updated: 18-January-2013

| | |
|--------------------|---|
| Applies To: | Websense TRITON Unified Security Center 7.7.3 |
|--------------------|---|

The following hardware is required for the TRITON Management Server machine, depending on the modules in your subscription:

| TRITON module(s) | Minimum requirements |
|---|---|
| Web Security | 4 CPU cores (2.5 GHz), 4 GB RAM, 7 GB disk space |
| Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 140 GB disk space |
| Web Security and Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB disk space |
| Email Security and Data Security | 4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB disk space |
| Web Security, Data Security, and Email Security | 8 CPU cores (2.5 GHz), 16 GB RAM, 146 GB disk space |

It is recommended you allocate more disk space than the minimum specified above, to allow for scaling with use.

If you plan to use SQL Server 2008 R2 Express on the TRITON management server, an additional 100 GB minimum disk space is required.

Software support

Topic 55423 / Updated: 18-January-2013

| | |
|--------------------|---|
| Applies To: | Websense TRITON Unified Security Center 7.7.3 |
|--------------------|---|

TRITON Management Server

Windows Server 2008 R2, 64 bit, is required to run the TRITON Unified Security Center. The Web Filter and Web Security management console (by itself) can instead be run on Windows Server 2008 32-bit.

Please note that Windows Server 2003 is not supported, except for Data Security secondary servers and Data Security standalone agents.

Supported browsers for servers

- ◆ Microsoft Internet Explorer 8
- ◆ Microsoft Internet Explorer 9
- ◆ Mozilla Firefox versions 4.x, 5.x, and 6.x
- ◆ Chrome 13

If you have another browser or version, the management interface may behave in unexpected ways or report an error.

TRITON database

The following databases are required for TRITON Enterprise:

- ◆ TRITON Settings Database
This is a Postgres database that contains TRITON configuration and infrastructure data. It is always installed on the TRITON Management Server machine.
- ◆ TRITON Reporting Database
This is a Microsoft SQL Server Database that contains reporting and logging data for all installed TRITON modules. It also holds Data Security policy, fingerprint, and forensics data.
In smaller networks, the reporting database (Microsoft SQL Server Express only) can be installed on the TRITON Management Server machine. You make this choice during installation.

As a free database management option for small deployments, SQL Server 2008 R2 Express is provided with TRITON Enterprise.

Supported directory services

TRITON Unified Security Center supports the following directory services for setting up network administrators:

- ◆ Microsoft Active Directory
- ◆ Novell eDirectory
- ◆ Lotus Notes
- ◆ Oracle Directory Server
- ◆ Generic LDAP directories

Installation

Topic 55424 / Updated: 18-January-2013

| | |
|--------------------|---|
| Applies To: | Websense TRITON Unified Security Center 7.7.3 |
|--------------------|---|

The following components are installed on the TRITON Management Server machine:

- ◆ TRITON Infrastructure. This is the framework required by the TRITON Unified Security Center and the TRITON modules.
- ◆ The TRITON modules that you select:
 - TRITON - Web Security
 - TRITON - Data Security
 - TRITON - Email Security
- ◆ SQL Server 2008 R2 Express (optional)
- ◆ Web Security Log Server (optional; may be installed on another machine)
- ◆ Email Security Log Server (optional; may be installed on another machine)
- ◆ Real-Time monitor (optional; may be installed on another machine)
- ◆ Sync Service (optional; may be installed on another machine)
- ◆ Linking Service (optional; may be installed on another machine)

To install or upgrade the TRITON Unified Security Center:

1. If you are already using Virtual Machines (VMs) for the TRITON console or for Microsoft SQL Server, take a snapshot of the VMs before you start a TRITON upgrade.
2. If you are using Websense Data Security, launch the TRITON console and choose Data Security. Then navigate to **Scheduled Tasks** and disable the DSS Watchdog service. This prevents it from restarting stopped services in the middle of the upgrade.
3. Download and launch the Websense TRITON installer, available on the **Support > Downloads** page under any Websense product:
(WebsenseTRITON773Setup.exe).
4. Accept the subscription agreement.
5. Select **TRITON Unified Security Center** as the **Installation Type** screen, and click **Next**.
6. Follow the instructions to install TRITON Infrastructure and the modules in your subscription.

NOTE: While you are going through the TRITON Infrastructure upgrade, you'll see a window telling you that some services are running and have files open. Be sure to choose "Do not close applications (requires reboot)."

- ◆ After the TRITON Infrastructure update is completed, you are prompted to reboot. Be sure to complete the requested reboot.

- ◆ After the TRITON software reboots, log in and make sure that Websense services are running.
- ◆ Then go to Start > Programs > Websense > Websense TRITON Setup.
- ◆ The upgrade will automatically continue.

Any time you receive a pop-up message notifying you that some services have files open that need to be upgraded, always select “Do not close applications (requires reboot),” and then reboot immediately after that section of the 7.7.3 upgrade completes.

See the Release Notes for each TRITON module for additional information.

Resolved and Known issues

Topic 55425 / Updated: 18-January-2013

| | |
|--------------------|---|
| Applies To: | Websense TRITON Unified Security Center 7.7.3 |
|--------------------|---|

- ◆ If you create a new administrator from LDAP by clicking **Administrators > Add Network Account**, the new administrator will be unable to change the TRITON console Help system language from English (to Chinese or Japanese) on the ‘My Account’ page.
- ◆ An unnecessary warning message may pop up during upgrade of the TRITON infrastructure from v7.7 to v7.7.3: “You need to modify DSS/ESG/WSG installations as well, in order for changes to take effect.” You can safely ignore this message. Simply click **OK** to continue with the upgrade.
- ◆ Data Security endpoint clients and Web Security endpoint clients are not yet supported on Firefox 18. This support is planned for the near future.

For Resolved and Known Issues for individual modules, please see the separate Release Notes.