

v7.6 Release Notes for TRITON Unified Security Center

Topic 45014 / Updated: 13-Apr-2011

Applies To:	Websense TRITON Unified Security Center 7.6
--------------------	---

Contents

- ◆ [Key features in this release](#)
- ◆ [Hardware requirements](#)
- ◆ [Software support](#)
- ◆ [Installation](#)
- ◆ [Known issues](#)

Through the TRITON Unified Security Center, you can manage Web Security, Data Security, and Email Security from the same management application. Click the links below to see the release notes for each TRITON module:

- ◆ [v7.6 Release Notes for Websense Web Security](#)
- ◆ [v7.6 Release Notes for Websense Data Security](#)
- ◆ [v7.6 Release Notes for Websense Email Security Gateway](#)

Click the links below to see the release notes for Websense Content Gateway and the V-Series appliance

- ◆ [v7.6 Release Notes for Websense Content Gateway](#)
- ◆ [v7.6 Release Notes for Websense V-Series Appliances](#)

Key features in this release

Topic 45015 / Updated: 13-Apr-2011

Applies To:	Websense TRITON Unified Security Center 7.6
--------------------	---

Version 7.6 is a major release of Websense TRITON Enterprise with the introduction of Websense Email Security Gateway and Email Security Gateway Anywhere. It

offers enhanced integration across the Websense product line and a significantly improved unified management experience.

Simplified deployment

It is faster and easier to deploy Websense TRITON Enterprise and the modules in your subscription in this version. The installation is performed using 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 is available for Web Security and Data Security version 7.1 and 7.5 users.

For more information, see [Installation](#), page 5.

Improved module integration

When you log on to the TRITON Unified Security Center, you no longer need to log onto individual modules (i.e. TRITON - Data Security and TRITON - Web Security) as well. A single logon applies to the TRITON Unified Security Center and all modules that you have access to.

In the TRITON Unified Security Center, the TRITON toolbar indicates the status of each module:

- ◆ Yellow represents the module that is currently active
- ◆ Blue represents a module that is installed, but not currently active
- ◆ Grey represents a module that is not installed

Enhanced administrator management

Administrator accounts (both local and network) are now managed on the TRITON Settings > Administrators page. The following types of administrator account are available:

- ◆ Global Security Administrators have full SuperAdministrator access to TRITON Settings and all TRITON Unified Security Center modules (Data Security, Email Security, and Web Security). Global Security Administrators can create administrator accounts and grant the accounts permission to access one or more TRITON modules.
- ◆ TRITON administrators have permission to access one or more TRITON modules with a single logon, and can optionally manage other administrators within those modules. A TRITON administrator is given default access rights for each module, and depending on the module and access granted, those access rights can

be modified by a SuperAdministrator within the module – for example, assigned to a delegated administration role in TRITON - Web Security.

The default administrator account created during installation is now “admin”. This account has Global Security Administrator permissions. The account password is defined during the installation process.

To create network accounts, you must set up a supported directory service on the TRITON Settings > User Directory page.

You can send notification emails to new administrators, administrators whose account details have changed, and administrators who have forgotten the TRITON Unified Security Center logon password. To do this, configure SMTP settings during installation, or on the TRITON Settings > Notifications page.



Note

The SMTP settings you configure for TRITON administrators are not propagated into TRITON modules. You must set these up separately for each module if required.

Appliance management

You can now view details of and access your V-Series appliance(s) from a central location, on the Appliances page of the TRITON Unified Security Center.

Appliances installed as part of the TRITON Enterprise installation appear on this page automatically. You can add further appliances by entering the C interface IP address to retrieve the appliance details.

Hardware requirements

Topic 45016 / Updated: 13-Apr-2011

Applies To:	Websense TRITON Unified Security Center 7.6
--------------------	---

The following hardware is required for the TRITON Management Server machine with a remote database, 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, 52 GB disk space

TRITON module(s)	Minimum requirements
Email Security and Data Security	4 CPU cores (2.5 GHz), 8 GB RAM, 52 GB disk space
Web Security, Data Security, and Email Security	8 CPU cores (2.5 GHz), 16 GB RAM, 110 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 45017 / Updated: 13-Apr-2011

Applies To:	Websense TRITON Unified Security Center 7.6
--------------------	---

TRITON Management Server

- ◆ Windows Server 2008 R2, 64 bit
Required to run more than one module in the TRITON Unified Security Center.
- ◆ Windows Server 2003 Standard/R2, 32 bit
This server is supported only for installation or upgrade of a single TRITON module (Data Security or Web Security).

Supported browsers

- ◆ Internet Explorer 7
- ◆ Internet Explorer 8
- ◆ Internet Explorer 9
- ◆ Firefox 3.5.x
- ◆ Firefox 3.6.x
- ◆ Firefox 4

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



Important

Internet Explorer 8 Compatibility View is **not** supported with the TRITON console. If you experience odd behavior or page layouts in Internet Explorer 8, make sure that Compatibility View button (between the URL and the Refresh button in the browser address bar) is not selected.

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. This replaces MSDE which is not supported in version 7.6.

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

Applies To:	Websense TRITON Unified Security Center 7.6
--------------------	---

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 the TRITON Unified Security Center:

1. Download and launch the Websense installer.
2. Accept the subscription agreement.
3. Select **TRITON Unified Security Center** as the **Installation Type** screen, and click Next.
4. Follow the instructions to install TRITON Infrastructure and the modules in your subscription.

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

Known issues

Applies To:	Websense TRITON Unified Security Center 7.6
--------------------	---

A [list of known issues](#) in this release of Websense TRITON Unified Security Center is available.

If you are not currently logged in to MyWebsense, the link above may cause a login prompt to display. Log in to view the list.