v7.6.0.1 Release Notes for TRITON Unified Security Center

Topic 45032 / Updated: 10-August-2011

Applies To:	Websense TRITON Unified Security Center 7.6

Contents

This internal release note covers the changes in the Websense TRITON Unified Installer for version 7.6.0.1. This installer is a replacement for the 7.6.0 installer, and should be used for new 7.6 customers only. It cannot be installed over the top of the 7.6.0 installation.

Note that the hardware requirements and software support information have not changed from those listed in the Websense TRITON Unified Security Center 7.6 Release Notes.

Key features in this release

Topic 45033 / Updated: 29-July-2011

Applies To:	Websense TRITON Unified Security Center 7.6

Version 7.6.0.1 is a minor release of the Websense TRITON Unified Installer. It fixes a number of issues that were encountered during version 7.6 deployments.

TRITON EIP changes

Installation failure due to port conflict

[CR 45528] After installing Websense TRITON components, one of the following occurred:

- On deployments with Microsoft ISA Server, users cannot browse through ISA on port 8080.
- A 404 error is displayed when trying to access the TRITON Unified Security Center.
- The following is displayed: Error 1920. Service “Websense Triton Unified Security Center” (EIPManager) failed to start. Verify that you have sufficient privilege to start system.

This was because Websense EIP components were listening on port 8080. This conflicted with the default ports for some other network components, for example ISA Server.

The default port for Websense EIP components has now been changed to 19448.

Upgrade paths clarified

[CR 45487] Upgrade to version 7.6 is only permitted from the latest 7.5.x or 7.1.x version. If a customer tries to upgrade from any other version, they will have to install the latest 7.5 or 7.1 version first.

File not encrypted when TRITON installed on non-default drive

[CR 45524] The WebsenseResume.txt file, which contains username and password information, is created during upgrade and should be encrypted due to its contents. The file was not encrypted when the TRITON Management Server was installed on a non-default drive (for example, D: or E:).

Installation failed on a localized operating system

[CR 45525] Installation failed on any localized operating system with Error 1720. This was because the word “Users” was hardcoded in a script, and this word was translated on the localized system (for example “utilisateurs” in French). Note that version 7.6 supports only installation paths that contain ASCII characters.

Clear text passwords in installation logs

[CR 45526] Installer log files contained passwords in clear text rather than being encrypted.

Installation failed when TRITON Management Server deployed by GPO within a domain

[CR 45527] When the TRITON Unified Security was distributed via GPO to a server within a domain, the installation failed because both local users and postgres_eip were not allowed to log on as a service.

Existing SQL server is not detected

[CR 45533] When installing the TRITON Management Server, the installer did not allow the selection of an existing local SQL server.

Data Security changes

The following issues have been fixed for Data Security deployments.

Printer Agent mode changed after upgrade

[CR 42015] When upgrading Data Security from version 7.1.8 to version 7.6, Printer Agent was in monitor mode after the upgrade, when previously it had been in blocking mode.

SQL error during upgrade

[CR 45044] During upgrade from 7.5 to 7.6, a 'Violation or Primary Key constraint' SQL error appeared. Clicking OK would enable the installation to proceed without problems; however, this error no longer appears in the updated installer.

Installation errors when using remote SQL and Windows authentication

[CR 45521] Data Security installation failed in the following circumstances:

- The Data Security management server is on Windows 2008 and is a member of the domain
- Remote SQL 2008 R2 is deployed
- During installation, Windows authentication was specified on the SQL connection settings page

Errors appeared during the installation but the process completed. However, it was not possible to log on to TRITON - Data Security.

Missing text when setting up temporary folder for archiving in Modify mode

[CR 45534] When the installer was run in Modify mode to set up a temporary folder for Data Security archiving, the Temporary Folder for Archiving page had missing text.

Export tool fix

[CR 45536] The upgrade export tool has been updated to allow the upgrade of very large DiscoveryJobs folders.

Web Security Gateway changes

The following issues have been fixed for Web Security Gateway deployments.

Log Server 7.6 upgrade caused logging to fail with existing MSDE

[CR 45501] After a 7.6 upgrade, logging no longer worked if an existing MSDE SQL DB engine was being used. This occurred if the previous version of Log Server was connected to an unsupported MSDE SQL server during the upgrade. The issue has been fixed so that logging continues post-upgrade.

WSG Manager has upgrade and remove options

[CR 45529] The 7.6 installer offered the option to upgrade or remove WSG manager. This has been changed so that the manager is always upgraded.

Merging administrators can cause logon issues

[CR 45740] When merging administrators from Web Security Gateway to TRITON, an administrator with the same name but a different email address was merged, but required confirmation in the TRITON console from a super administrator before they could log on.This caused an issue when it was the super administrator who required confirmation.

Known issues

Topic 45034 / Updated: 10-Aug-2011

Applies To:	Websense TRITON Unified Security Center 7.6

Reboots occurring during installation

If you are installing SQL Server 2008 R2 Express on a Windows 2003 machine, and the operating system does not have all current updates installed, 2 reboots occur during installation, with no messages displayed. This is due to local SQL Server prerequisites.

When you log on after reboot, the Websense installer launches automatically from the point where it was suspended, and proceeds with the installation.

Windows 2003 installation requires Service Pack 2

If you are installing on Windows 2003 Server R2 and intend to install SQL Server Express locally, you must install Service Pack 2 or later. This is required for SQL Server.

Installation may fail on unpatched Windows 2003 systems

This possible installation failure is due to a Microsoft limitation on large installers in this version. Apply Microsoft KB925336 to fix this.

Domain and user name display in Server & Credentials installer screen

[CR 45885] When installing TRITON Infrastructure, there is a display issue in the **Server & Credentials** screen. If you use the **Browse** button to select a different domain or user name than currently shown, the old user name or domain may continue to be displayed. This is a display issue only; the new value you have selected is actually the one the installer will use. Clicking **Next** and **Back** will show the correct value.

May not be able to connect to existing SQL Server Express during TRITON Unified Security Center installation

You can install SQL Server 2008 R2 Express (SQL Server Express) by itself by performing a custom installation using the Websense installer. During subsequent installation of the TRITON Unified Security Center, if you choose to use the separately installed SQL Server Express, connection to the database may fail. If this occurs, start the SQL Server Browser service on the SQL Server Express machine. Connection to the database should now be successful and you can continue the installation of TRITON Unified Security Center

This is most likely to occur on lower-resourced machines or on virtual machines.

TMG Agent installation always creates Websense folders on C drive

If you choose to install TMG Agent to a non-default installation path, the majority of components are installed to the specified path. However, C:\Program files\Websense (which is empty) and C:\Program files (x86)\Websense are still created. This does not affect the operation of TMG Agent.

Note that the TMG Agent is installed using the 64-bit version of the Data Security component installer (**WebsenseDataSecurity760-x64.msi**).

Cannot edit user name for Windows authentication for SQL Server

By default, the currently logged in user that launched the Websense installer is taken as the Windows account to use to connect to SQL Server when Windows authentication is chosen. You cannot specify a different account in the **SQL Server** screen when installing TRITON Infrastructure.

If you want to use a different account, cancel the installation. Log in to the machine as the user you want used for SQL Server Windows authentication and then restart the Websense installer.

In some organizations, policies are in place where service accounts (i.e., accounts used to run Windows services) cannot be interactive (i.e., used by a user for general login) and interactive accounts cannot be used to run services. In such a case, if possible, allow a service account to be interactive for the duration of installing Websense products. Log in to the machine with the service account, so services are properly installed to run as a service user, and then revoke the interactivity for that account after installation is complete.

Backup and restore

[CR 44646]: If administrators are unable to log on to the TRITON console after a TRITON configuration has been restored, restart the TRITON services.

Problems changing the TRITON Manager host name

Sometimes an error is returned when you are performing the Modify operation on the TRITON Infrastructure module. This may happen when you are following the procedure to change the host name of the TRITON management server. The message returned is “Error 1720.”

If you receive this error, locate a file called “EIPSettings.xml” in the EIP Infra sub-folder of the main installation folder. On Windows Server 2003 systems, the default location of this file is C:\Program Files\Websense\EIP Infra\EIPSettings.xml. On Windows server 2008 R2 systems, the default location is C:\Program Files (x86)\Websense\EIP Infra\EIPSettings.xml.

Edit the **EIPSettings.xml file**. In line 31, locate the user name of the administrative user you have chosen for the Websense installation, in the format “<old-hostname>\<username>”. Change the <old-hostname> to the new host name of the TRITON manager, save the file, and retry the Modify operation.

Account names must use ASCII characters

[CR 45809] The user account specified on the Server & Credentials screen that is used by TRITON Unified Security Center must include only ASCII characters. The account name can include English-based letters, numbers and some special characters such as # and &.

This limitation has also been documented in the Deployment and Installation Center for v7.6.

Schema DB and Partition DB names incorrect after upgrade

[CR 46294] When upgrading from version 7.1 of Web Filter to version 7.6 with an MSDE SQL server, and installing SQL Server 2008 R2 Express as part of the upgrade, the names of the schema DB and partition DB in the database are wslogdb76 and wslogdb76_1 respectively. The names should be wslogdb70 and wslogdb70_1.

To work around this issue, after the installation of SQL Server 2008 R2 Express and before the Web Security Gateway upgrade starts, restore the wslogdb70 and wslogdb70_1 files from MSDE to SQL Server 2008 R2 Express. Then continue with the upgrade.

Note that this issue does not affect new installations.

Passwords must use standard ASCII characters

[CR 45957] The password specified during installation for access to TRITON Unified Security Center must use only standard ASCII characters (English-based letters, numbers and some special characters such as # and &). Although extended ASCII characters, such as õ and ¦, are accepted by the installer, the user will not be able to log on to the TRITON console with a password containing these characters.

Sender name for email notifications must use standard ASCII characters

[CR 45962] The Sender name specified on the **Email Settings** screen during TRITON Infrastructure installation must use only standard ASCII characters (English-based letters, numbers and some special characters such as # and &). Although extended ASCII characters, such as õ and ¦, are accepted by the installer, a sender name that contains these characters will not be displayed on the **TRITON Settings > Notifications** page in the TRITON console.