Disaster Recovery

Websense® Web Security
Web Security Gateway

v7.6

©1996–2011, Websense, Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2011

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense, Inc.

Every effort has been made to ensure the accuracy of this paper. However, Websense, Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense, Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (**http://www.apache.org**).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

Chapter 1 **Policy Broker on box 5**

Chapter 2 **Policy Broker off box 7**

Chapter 3 **Back up Processes. 9**

WSWPBBU – Back up the WS Policy Database on a Windows Policy Broker . .9
EIPBU – Back up the EIP database on a Windows TRITON 10
DSMGRBU – Back up Data Security 11

Chapter 4 **Restore Processes 15**

EIPRES – Restore EIP 15
WSWPBRES – Restore WS Policy – Windows Policy Broker. 20
WSVPOLSRC – Redirecting a V10K G2 to a different Policy source 24
WSWDBSET – Modify the ODBC data source on a Windows Log Server 28
WSVPOLBU – Back up the policy from a Policy source on V10K G2 33
WSPSLSCFG – Configure a Policy Server to use an active Log Server. 35
WSVPOLRES – Restore the backed up policy to an alternate V10K G2 36
DSMGRRES – Restore Data Security policies and forensics 41
DSSVRREG – Re-register a DSS server with a new TRITON server. 45
DSWCGREG – Re-register a WCG server with a new TRITON server. 48
DSMGRDEP – Deploy settings for all re-registered components. 50
WSRFSCFG – Reconfigure Remote Filtering Servers to point to active server .52

1 Policy Broker on box

This is the procedure for Disaster Recovery (DR) Scenario preparation, recovery, and restoration in an environment where the Policy source is on a V10K G2 appliance. The Policy source machine runs Policy Broker and Policy Database, in addition to other Web Filtering components. The procedure refers to the backup and restore processes from chapters 3 and 4.

Preparation:

1. Backup the EIP Infrastructure and the policy on the V10K G2 appliance by following procedures EIPBU and WSVPOLBU.
2. Designate a V10K G2 appliance to be used as the Policy source in the DR Data Centre for use during a DR Scenario.
3. Install an additional TRITON server with a Log Server on a machine in the DR Data Centre that is configured to use the designated Policy source appliance. Use a dummy SQL Server for this setup and do not log on to the DR TRITON.
4. Shut down the DR TRITON server and stop all Websense services (all services that start with Websense).
5. Then, uninstall/delete the dummy SQL Server.

Disaster Recovery:

1. Follow procedure WSVPOLRES to restore the backup to the designated DR Policy source appliance.
2. Start the DR TRITON server and all Websense services. The Log Server will fail to start.
3. Follow procedure EIPRES to restore the EIP settings to the TRITON server.
4. Follow procedure WSWDBSET to modify the ODBC data source on the TRITON server to point to the non-DR Policy source.
5. Follow procedure WSVPOLSRC to redirect all surviving appliances to use the designated DR Policy source appliance. Complete this procedure for each surviving appliance.
6. Follow procedure WSPSLSCFG to redirect all Policy Servers to the local Log Server. Complete this procedure for each Policy Server.
7. Verify that the system is working as expected.

8. Follow procedures WSVPOLBU and EIPBU on the DR environment when case changes are made or the DR scenario lasts for a long period of time.

Restoration:

1. Follow procedure WSVPOLRES to restore the policy to the original Policy source.
2. Stop the DR TRITON server and all Websense Services.
3. Reinstall the non-DR TRITON if needed. Reinstall using a dummy database server. Then, follow procedure WSWDBSET.
4. Follow procedure EIPRES on the TRITON server if TRITON had to be reinstalled or the EIP settings have changed.
5. Follow procedure WSVPOLSRC to point all appliances back to the non-DR Policy source. Complete this procedure on each appliance.
6. Follow procedure WSPSLSCFG to redirect all Policy Servers to the non-DR Log Server. Complete this procedure for each Policy Server.
7. Verify the system is working as expected.

2 Policy Broker off box

This is the procedure for Disaster Recovery (DR) Scenario preparation, recovery, and restoration in an environment where the Policy source is off a V10K G2 appliance. The Policy source machine runs Policy Broker and Policy Database, in addition to other Web Filtering components. The procedure refers to the backup and restore processes from chapters 3 and 4.

Preparation:

1. Back up the EIP Infrastructure, the off-box WWS policy, and the DS policy by following procedures WSWPBBU, EIPBU, and DSMGRBU. Set up scheduled tasks to periodically perform these procedures.
2. Install an additional TRITON server with a Log Server on a machine in the DR Data Centre with a local Policy source and Policy Broker. Use a dummy SQL Server for this setup and do not log on to the DR TRITON.
3. Shut down the additional TRITON server and stop all Websense services (all services that start with Websense).
4. Uninstall/delete the dummy SQL Server.

Disaster Recovery:

1. Start the DR TRITON server and Websense services. The Log Server will fail to start.
2. Follow procedure EIPRES to restore the EIP settings on the TRITON server.
3. Follow procedure WSWDBSET to modify the ODBC data source on the TRITON server to point to the non-DR Policy source.
4. Follow procedure WSWPBRES to restore the off-box policy to the Policy Broker.
5. Follow procedure WSVPOLSRC to redirect all surviving appliances to use the new off-box Policy source. Complete this procedure on each surviving appliance.
6. Follow procedure WSPSLSCFG to redirect all Policy Servers to the local Log Server. Complete this procedure for each Policy Server.
7. Follow procedure DSMGRRES to restore the Data Security setup, policies, and forensics.
8. Follow procedure DSSVRREG on all surviving DSS Servers to re-register with the new TRITON.

9. Follow procedure DSWCGREG on all surviving appliances' WCG (P1 ports) to re-register with the new TRITON.
10. Follow procedure DSMGRDEP to deploy the DS policy to all surviving DS components. Components that did not survive the DR Scenario will fail.
11. Verify that the system is working as expected.
12. Follow procedures WSVPOLBU, DSMGRBU, and EIPBU on the DR environment when case changes are made in the DR environment or the DR scenario lasts for a long period of time.

Restoration:

1. Follow procedure WSVPOLRES to restore the policy to the original Policy source.
2. Stop the DR TRITON server and all Websense Services.
3. Reinstall the non-DR TRITON server if needed. Reinstall using a "dummy" server, then follow procedure WSWDBSET.
4. Follow procedure EIPRES on the TRITON server.
5. Follow procedure DSMGRRES on the TRITON server.
6. Follow Disaster Recover steps 5-12 on the DR Scenario targeting the non-DR TRITON.

3 Back up Processes

WSWPBBU – Back up the WS Policy Database on a Windows Policy Broker

Purpose: Export the Policy Database to a flat file to be transferred to the destination machine. Extract the Policy Broker token from the configuration file.

Perform on: Source Windows Policy Broker.

Perform when: Periodically (back up).

Steps How:

1. **Export.** Run the command: “C:\Program Files (x86)\Websense\Web Security\bin\PgSetup.exe” and save as C:\Temp\policy.dmp. Copy the policy.dmp file to a backup location in the DR site.
2. **Extract token.** Run the command: find “Token” < “C:\Program Files (x86)\Websense\Web Security\bin\config.xml” > token.txt. Copy the token.txt file to a backup location in the DR site.
3. **Results.** The token file should contain the token element from the configuration file.

```
c:\Temp>find "Token" < "c:\Program Files (x86)\Websense\Web Security\bin\config.
xml" > token.txt

c:\Temp>type token.txt
                        <data name="Token">0542A478BC2AB7773AE226F8471E4DD12E7AB
78DEFF21A3A151621EFBF5A98552E76E8DD044AAAC1B5CB94B27BFC896C0435D33EF0502A517D21D
9573EAE5CBA51C8B246EF9CE4D3D27D502D7F9F21DEDF71D228CB3A5A58D7CE4EAFAE6561C19A61D
56A92A8E96AD7F682C0BCA6DB9069C1E89DF258FFE90E22C0EECBC3908892998E8EABA96C409C4F4
01815FAD21BD427175DBD1B06B28465CC20C41AD452DE2B7798A71CF17E</data>

c:\Temp>
```

EIPBU – Back up the EIP database on a Windows TRITON

Purpose: Back up the EIP database containing the EIP settings.

Perform on: Source TRITON server.

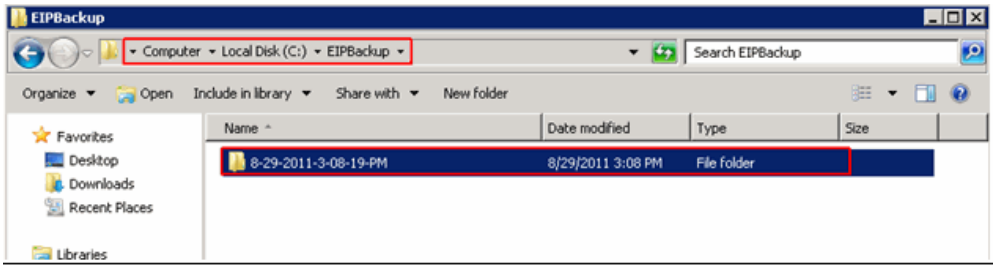
Perform when: Periodically (back up).

Steps How:

1. **Configure.** Modify the backup configuration in:

   "C:\Program Files (x86)\Websense\EIP Infra\EIPBackup.xml".

   Without modifications, the backup will be saved to C:\
2. **Extract token.** Run the command: cscript "C:\Program Files (x86)\Websense\EIP Infra\EIPBackup.vbs". Copy the token.txt file to a backup location in the DR site.
3. **Results.** The backup is stored in the folder EIPBackup under the folder configured in step 1.



DSMGRBU – Back up Data Security

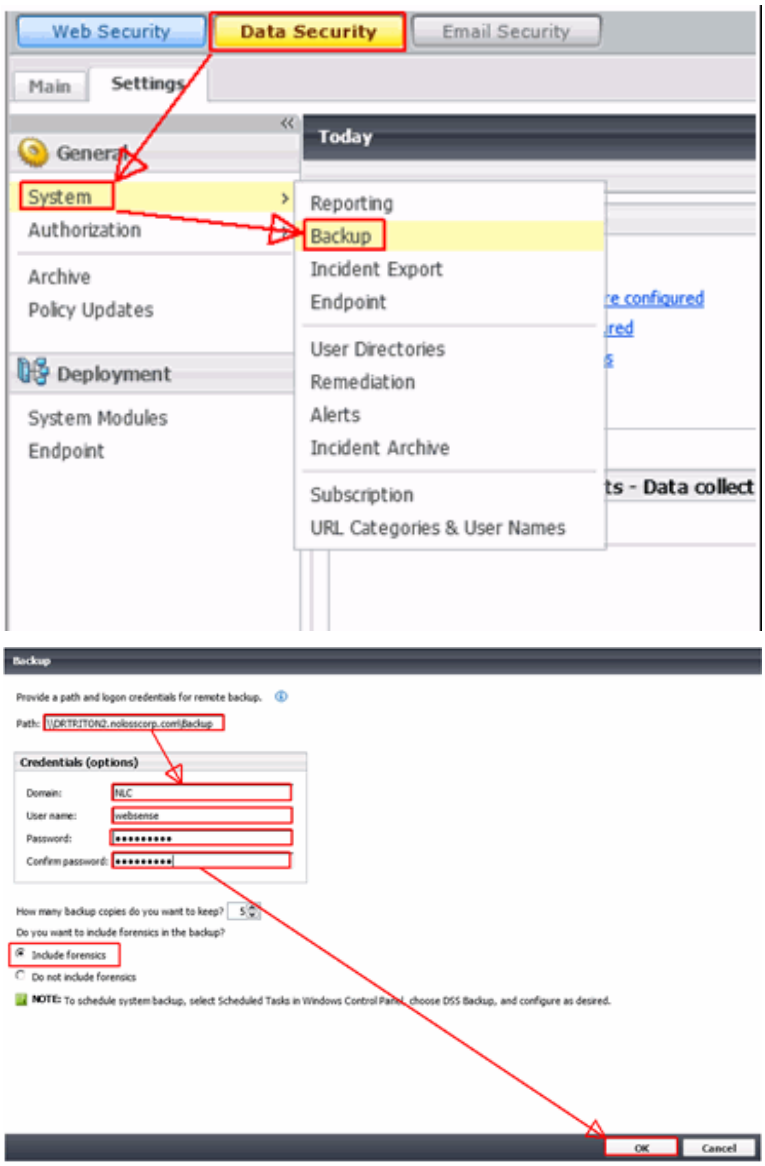
Purpose: Back up Data Security settings, policies, forensics, and database.

Perform on: Source TRITON server.

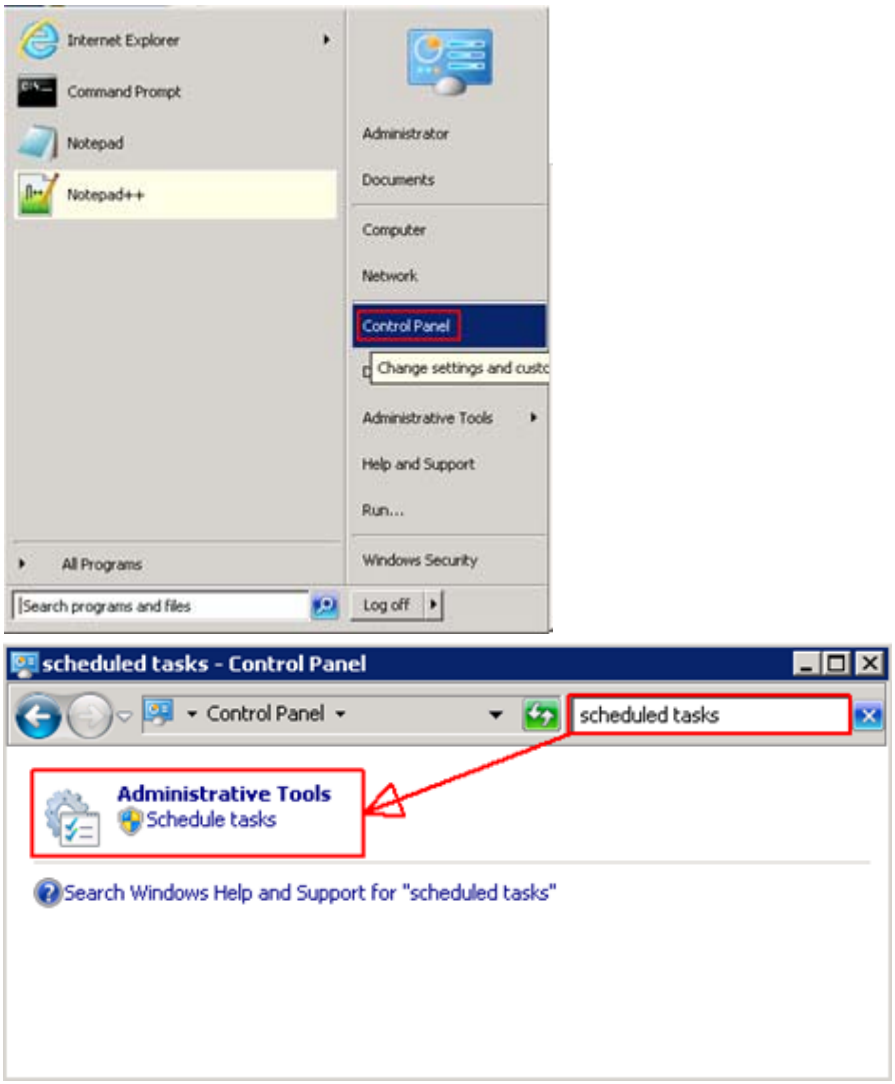
Perform when: Periodically (back up).

Steps How:

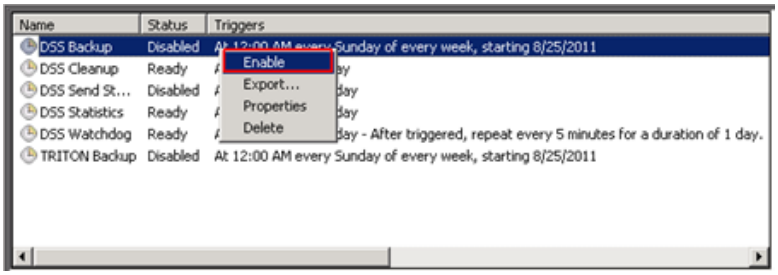
1. **Configure.** Log on to the TRITON console and go to the Data Security configuration screen. Enter the location of the backup, the credentials, and the number of copies. This needs to be done only once or on an as-needed basis**.**



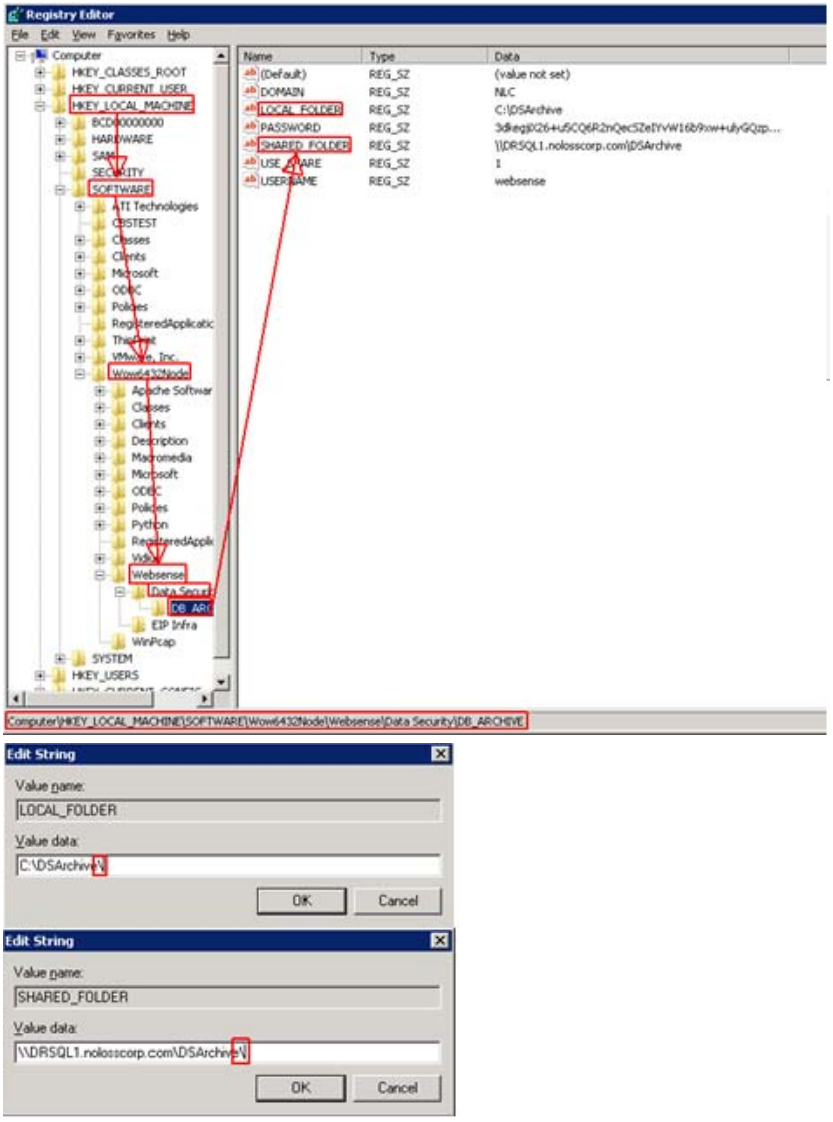
2. **Configure scheduled task.** Go to the DSS Backup scheduled task. Configure if necessary.



Then, enable the scheduled task by right-clicking the task:



3. **Registry modification.** Add a trailing slash to the registry entry of the archive folder setting:



4. **Result.** When the scheduled task runs, it creates a DSSBackup folder under the folder defined in step 1. The folder has a dated folder name.

4 Restore Processes

EIPRES – Restore EIP

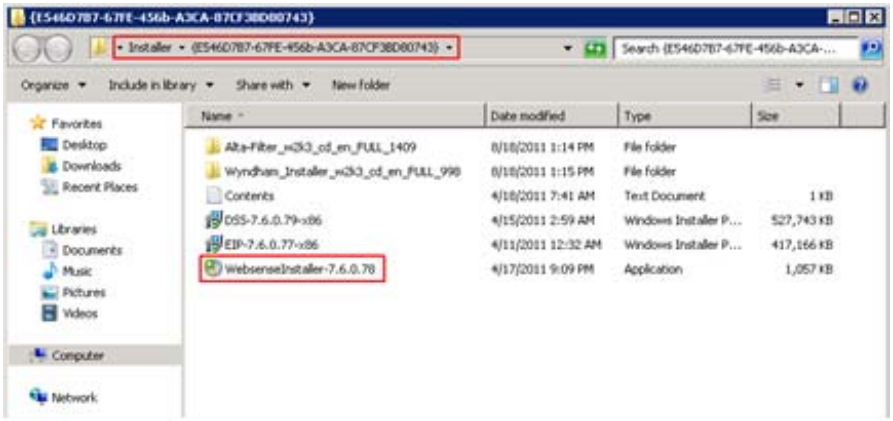
Purpose: Restore the EIP settings including user directories on the target TRITON server to enable user authentication.

Perform on: Target TRITON server.

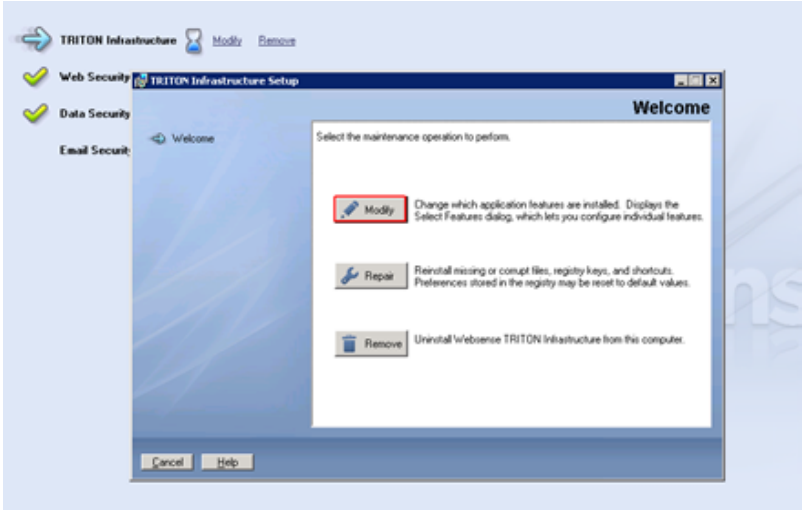
Perform when: In a DR Scenario.

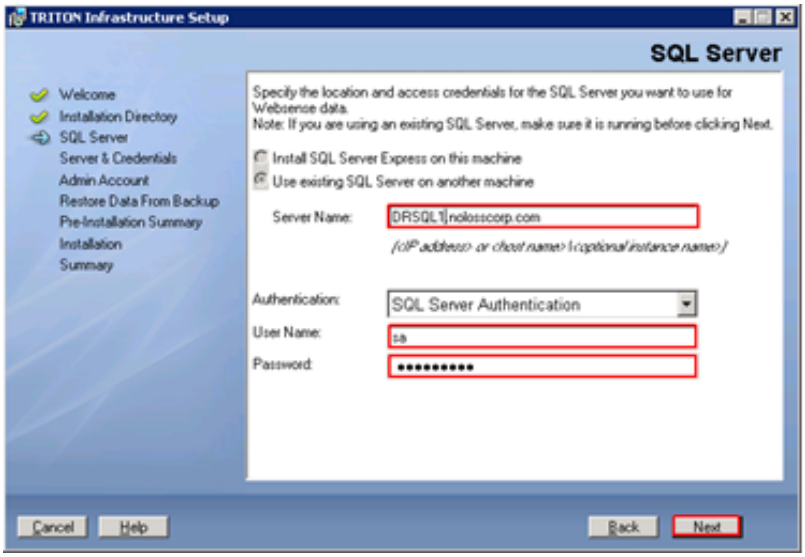
Steps How:

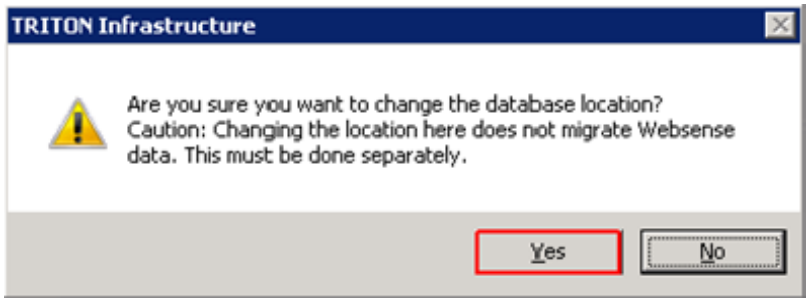
1. **Run the installer.** Assuming the TRITON universal installer files have been kept, run the TRITON Universal Installer WebsenseInstaller-7.6.0.78.exe from C:\Windows\Installer\{E546D7B7-67FE-456b-A3CA-87CF3BD80743}. Then click Modify.



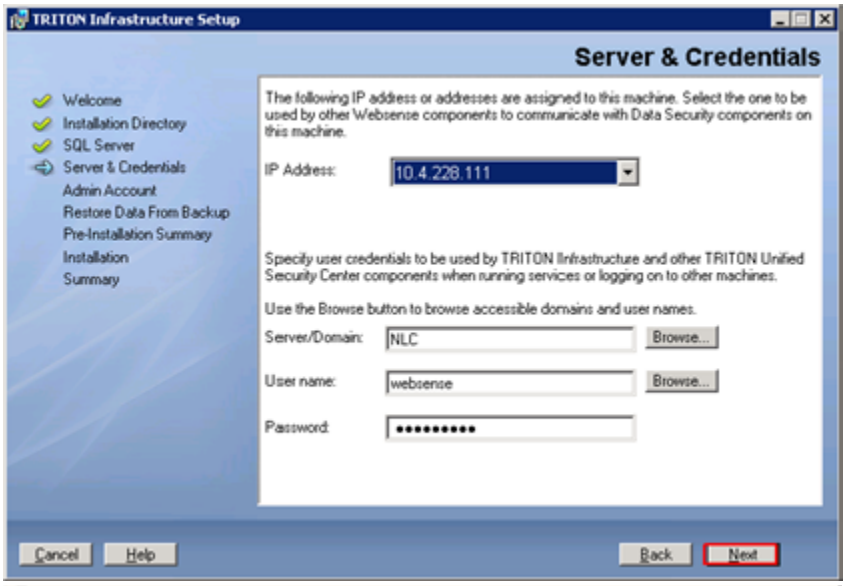
2. **Reconfigure the database.** Click Modify in the installer and progress to the dialog. Modify the database to the active database if necessary.

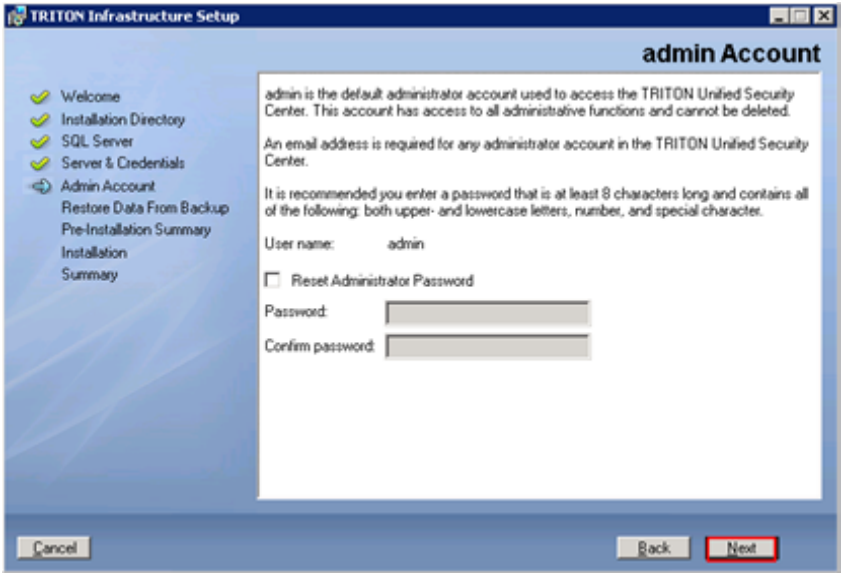




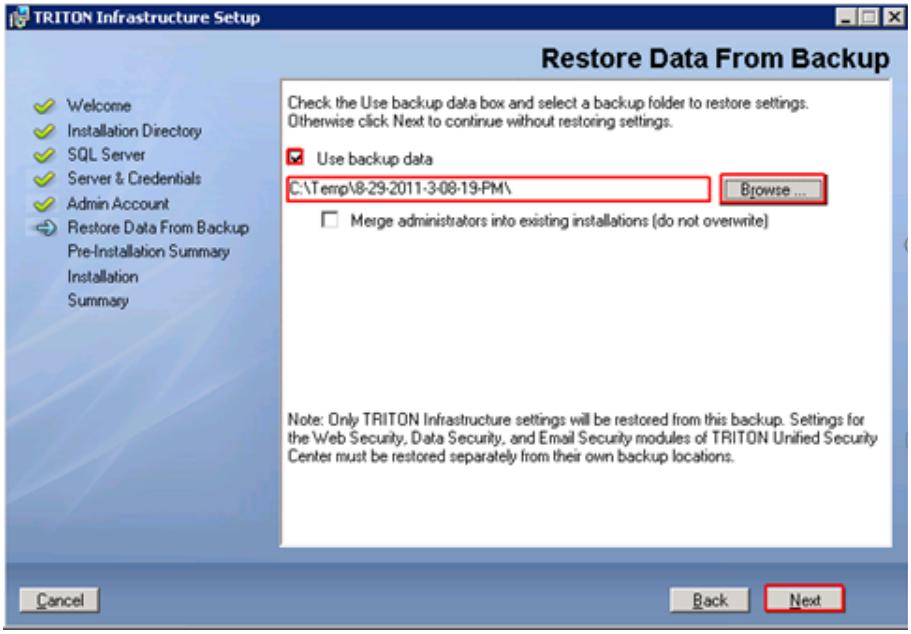


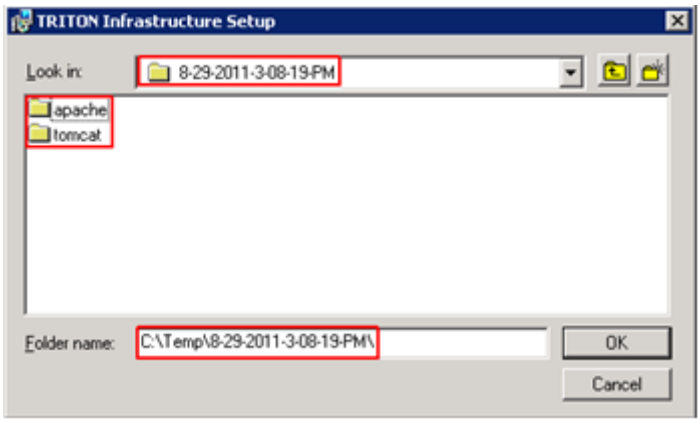
3. **Progress to the restore dialog.** Click Next through the dialog boxes until reaching the database restore dialog.



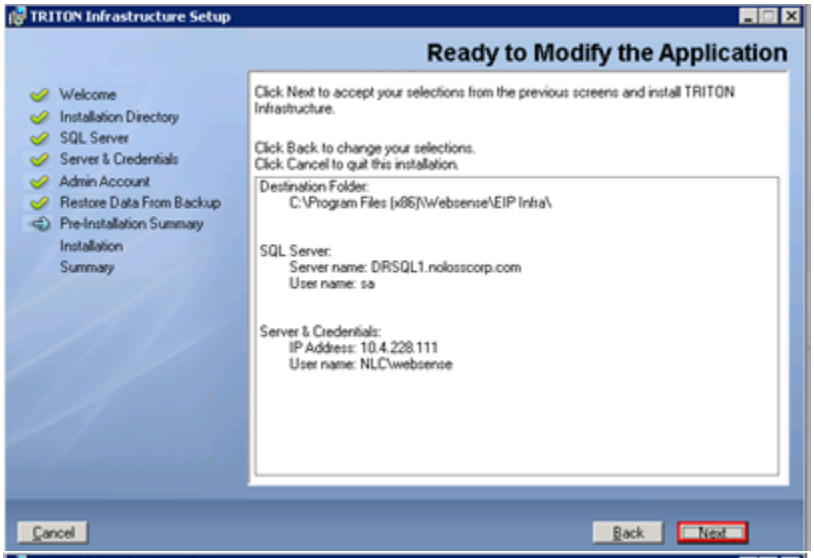


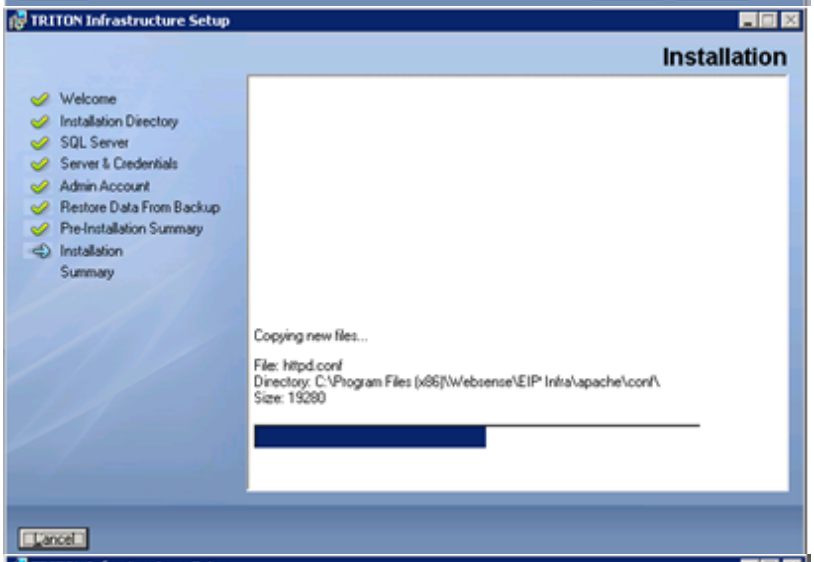
4. **Select the restore source.** Check **Use backup data** and select the dated folder containing the EIP restore. The name of the folder should be similar to the DS restore folder. You can identify the folder name by looking inside the folder; it should have only two subfolders (DS has four).

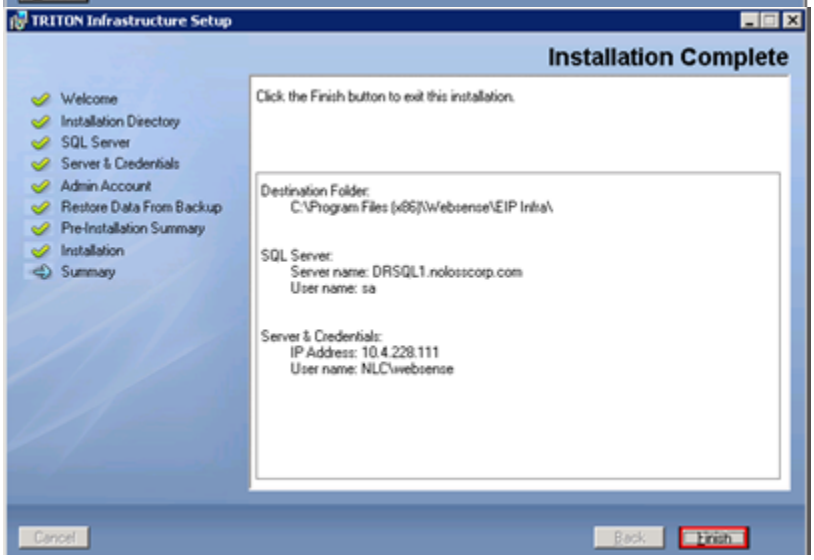




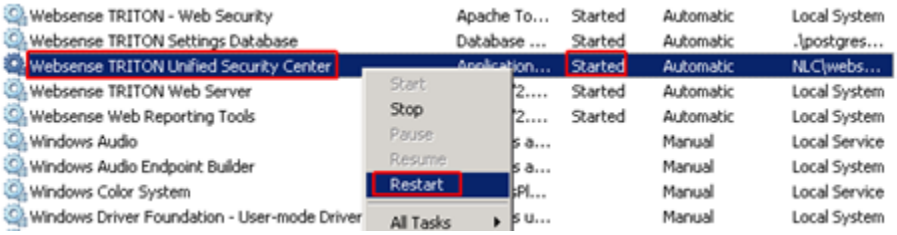
5. **Finish the installer wizard.** Progress through the installer wizard until it is complete.







6. **Restart the EIP service.** Locate the service named Websense TRITON Unified Security Center and click Restart.



7. **Results.** EIP information (such as login and directory integration, registered appliances) will be available in the EIP environment.

WSWPBRES – Restore WS Policy – Windows Policy Broker

Purpose: Restore the policy saved in WSWPBBU to a Windows Policy Broker and set up a token for the local Policy Server to connect to.

Perform on: Target Windows Policy Broker.

Perform when: In a DR Scenario.

Steps How:

1. **Stop Policy Broker and Policy Server.** Locate and stop the Websense Policy Broker. Then, locate and stop the Websense Policy Server in this order.

2. **Restore the Policy Database from the dump file.** Run the command (replacing the actual path for the dump file):

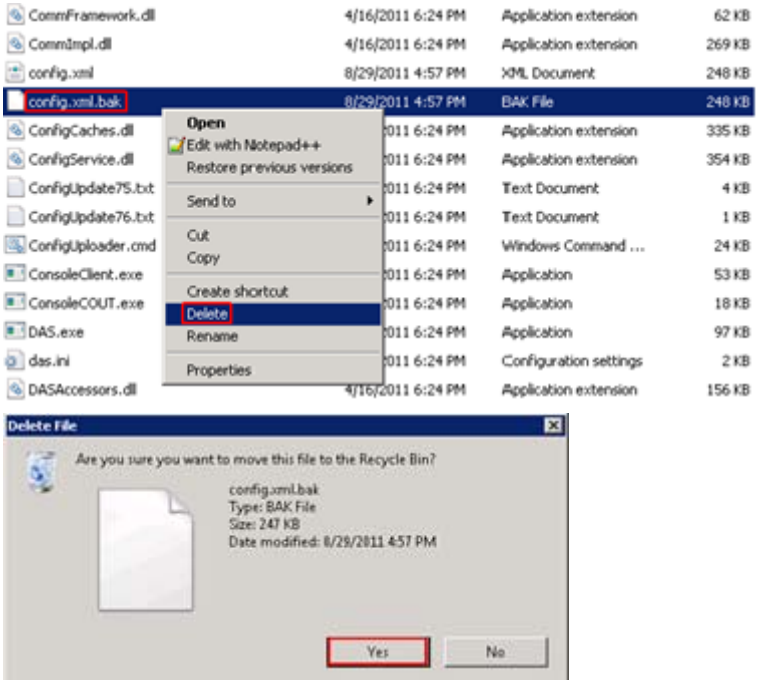
   C:\Program Files (x86)\Websense\Web Security\bin\PgSetup.exe

   Restore C:\Temp\policy.dmp.

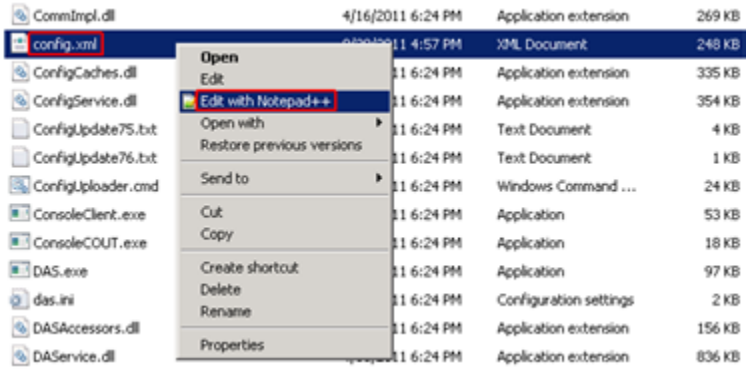
> **Note**
> The policy dump file cannot be read from a network share. PgSetup.exe does not produce any messages when it succeeds.

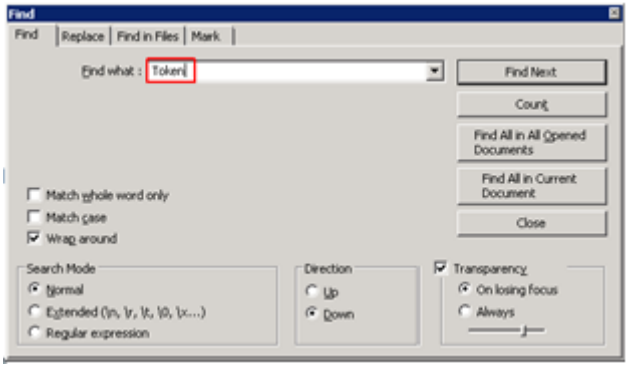
3. **Delete the backup config.xml file.** Browse to the Web Security bin folder: C:\Program Files (x86)\Websense\Web Security\bin

   Locate the file config.xml.bak and delete it.



4. Replace the token in the config.xml file and edit the config.xml file. Locate the token and replace it with the token from step 2 of procedure WSWPBBU. These screenshots use Notepad++ as an editor).





5. **Start the Policy Broker and Policy Server.** Locate and start the Websense Policy Broker and Websense Policy Server.

Verify that the services have been successfully started.

6. **Results.** Both services should start, restoring the policy from the environment affected by the disaster event.

WSVPOLSRC – Redirecting a V10K G2 to a different Policy source

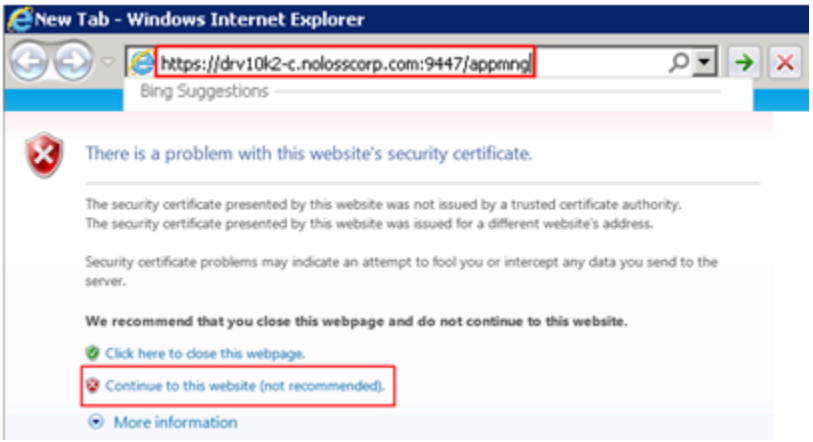
Purpose: Redirect an appliance with a non-active Policy source to ensure it continues operating.

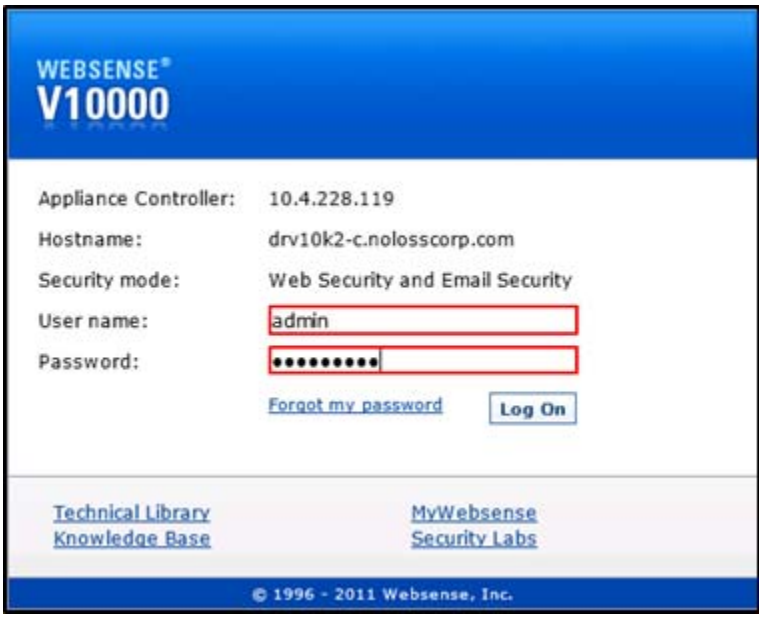
Perform on: V10K G2 appliance pointing to an inactive Policy source.

Perform when: In a DR Scenario

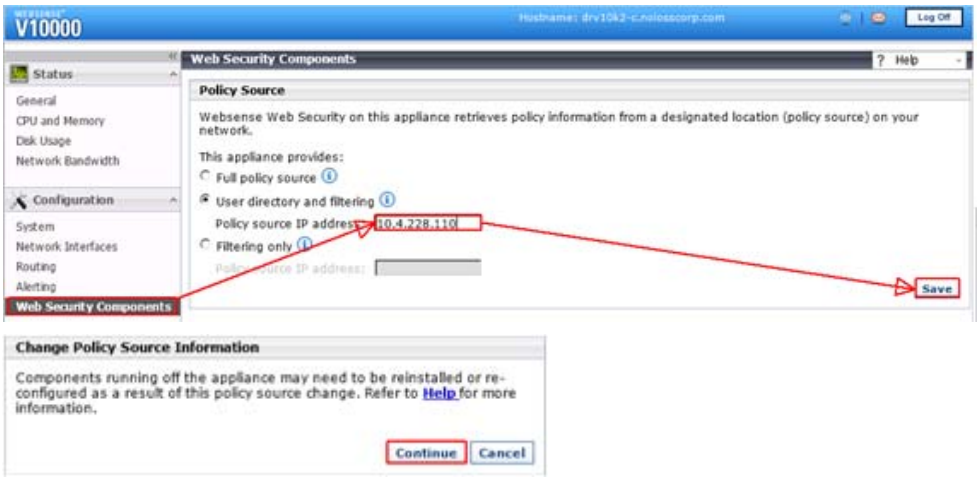
Steps How:

1. **Log on to the Appliance Management interface.** Browse to the address https://<IP address or name of the appliance>:9447/appmng and log on as the admin user.

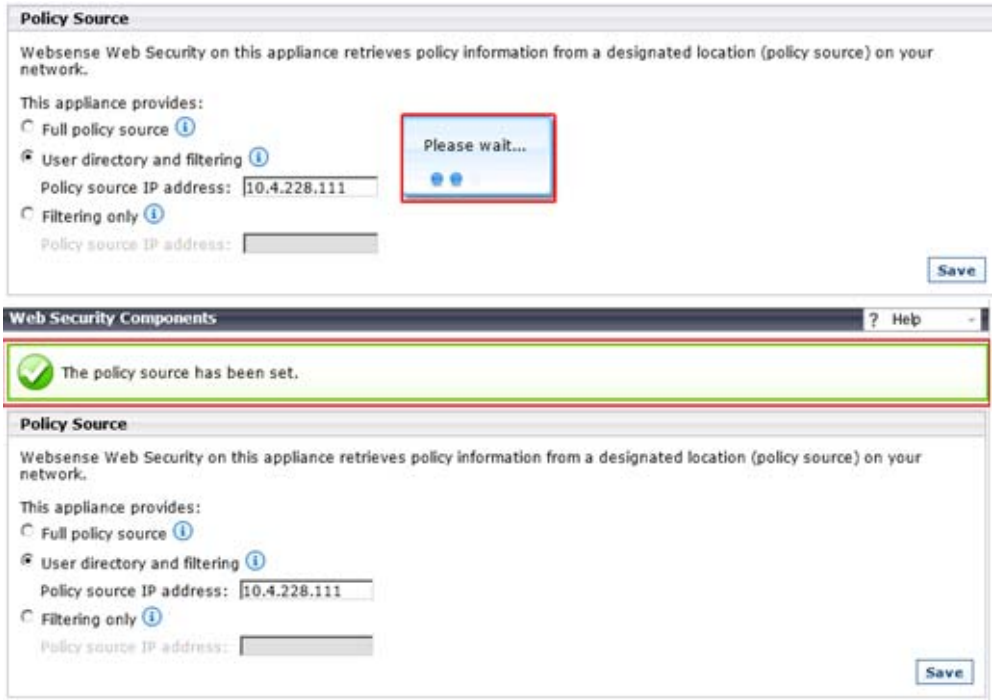




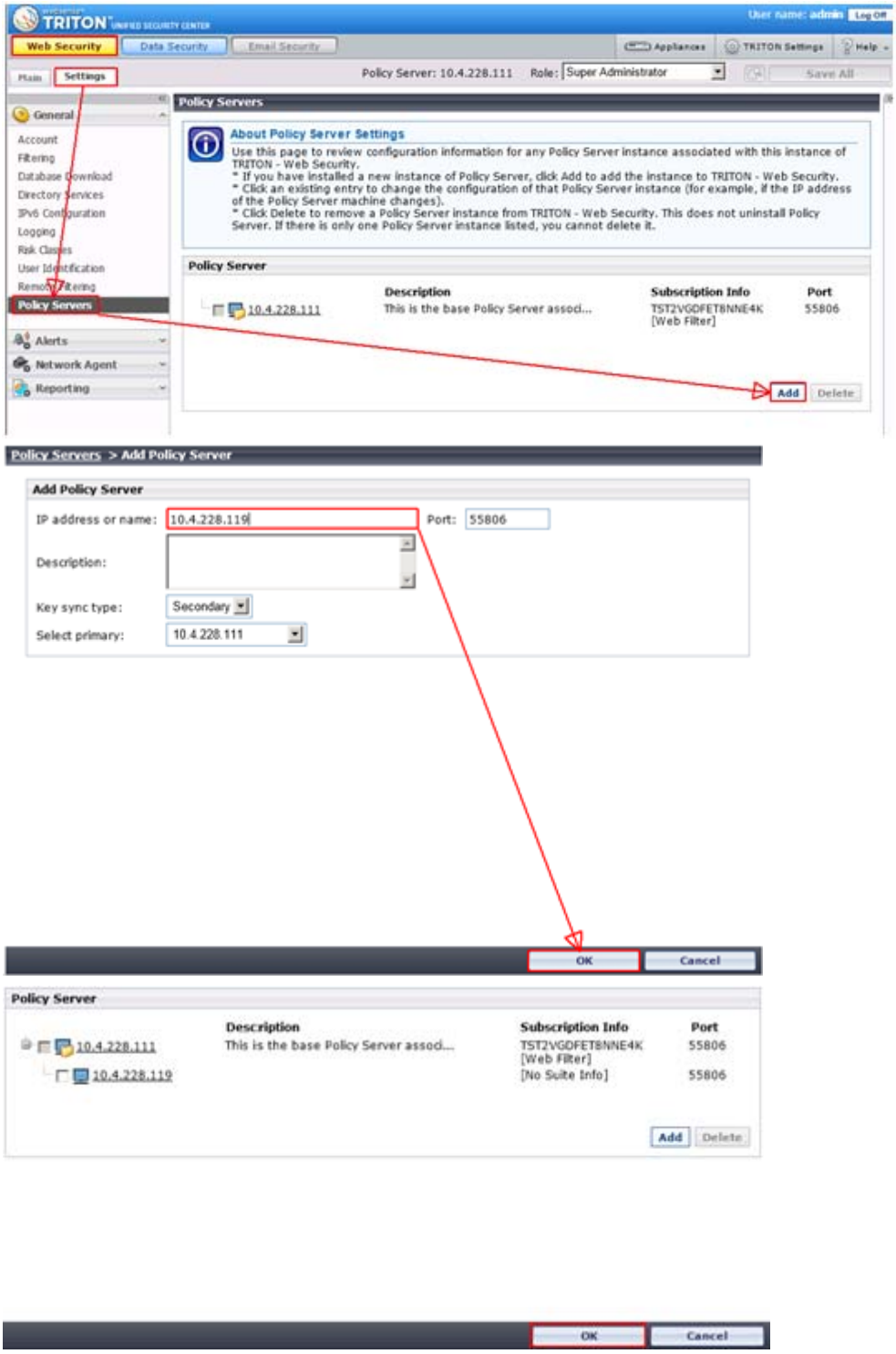
2. **Modify the Policy source IP address.** Select the Web Security Components page and modify the Policy source setting to reflect the new IP address of the Policy source. Leave the appliance in Policy Lite mode (this is the User directory and filtering option).



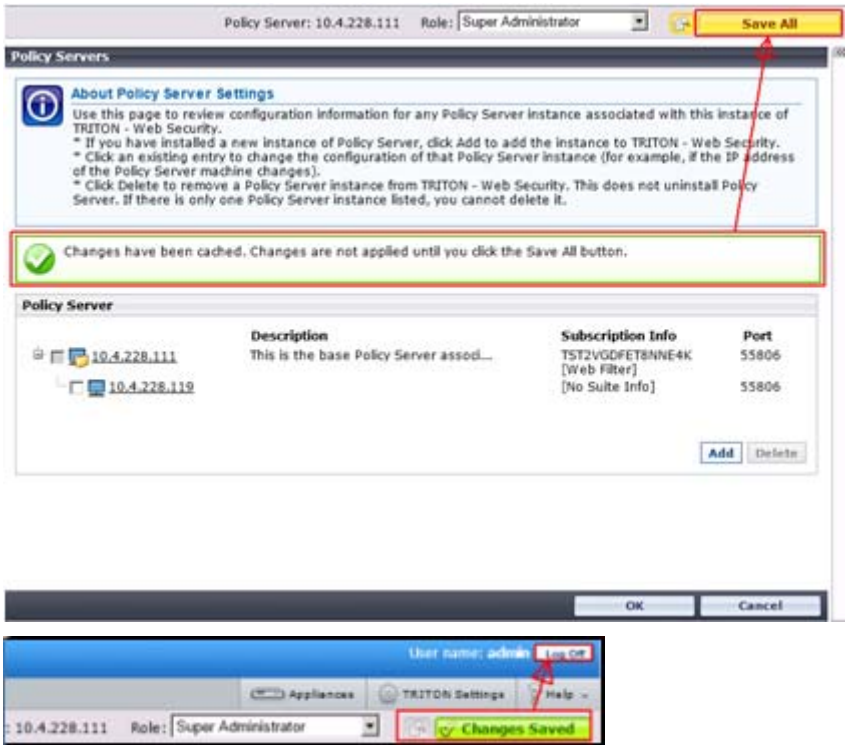
3. **Wait.** This process may take 5 minutes or more.



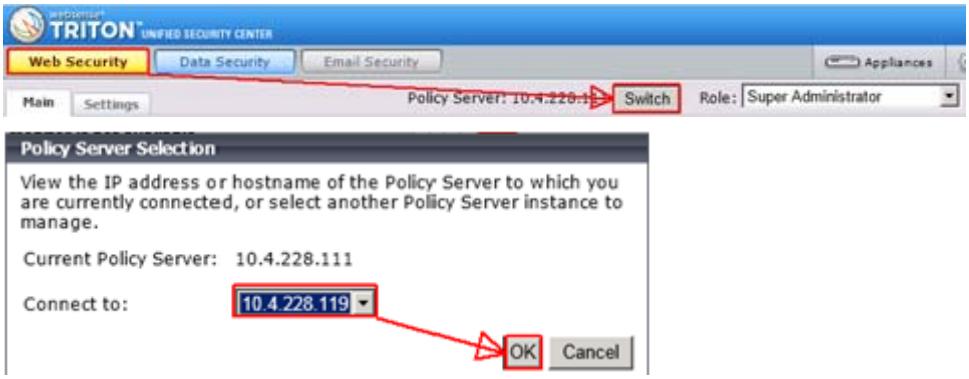
4. **Add the appliance as a Policy Server in TRITON settings.** Unless it is already configured, add the appliance's Policy Server to TRITON.



Press **Save All**. Wait until the green checkmark appears indicating that the changes have been saved. Then, log off from TRITON.



5. **Switch to the Policy Server on the V10K G2.** Under Web Security, click **Switch** to switch to the Policy Server on the V10K G2. In this example, 10.4.228.111 is the local TRITON machine and 10.4.228.119 is the V10K G2 C interface:



6. **Results.** The appliance will now work with the new TRITON server as a Policy sourcePolicy source. The TRITON manager machine is able to manage the new Policy Server.

WSWDBSET – Modify the ODBC data source on a Windows Log Server

Purpose: Point the TRITON server and Log Server on the DR machine at a clustered database that will survive the DR scenario.

Perform on: Target Windows Log Server / TRITON server.

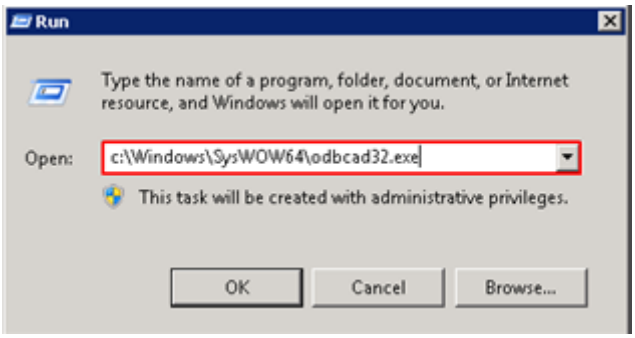
Perform when: In a DR Scenario (first time only or as a preparation for a DR scenario).

Steps How:

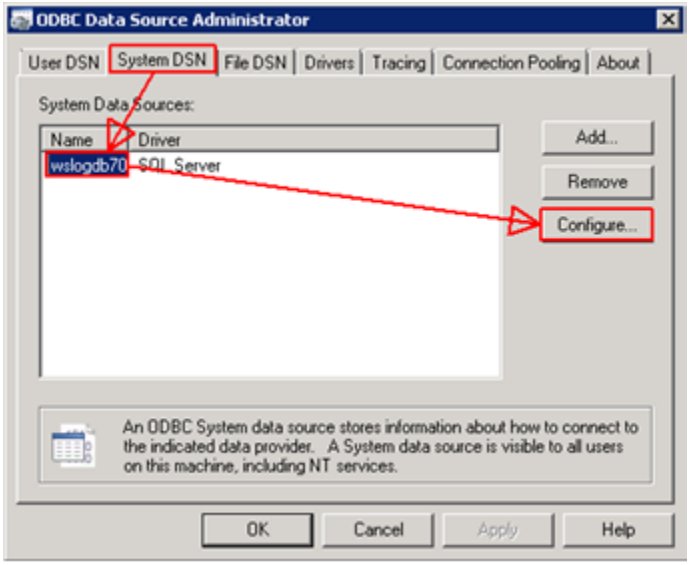
1. **Run WOW ODBC control applet.** Run the ODBC applet in the following location:

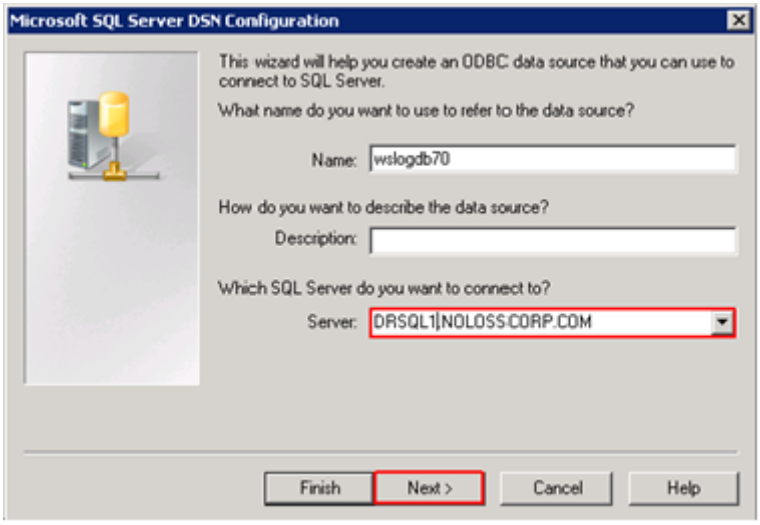
   C:\Windows\SysWOW64\odbcad32.exe

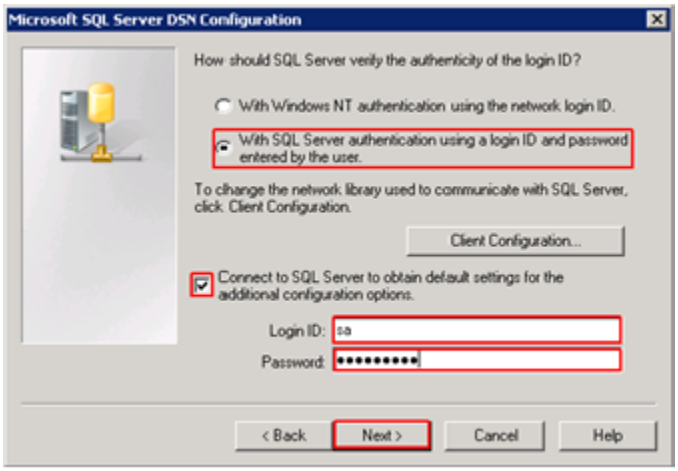
   DO NOT run it from the Administrative Tools menu because it is a different applet.

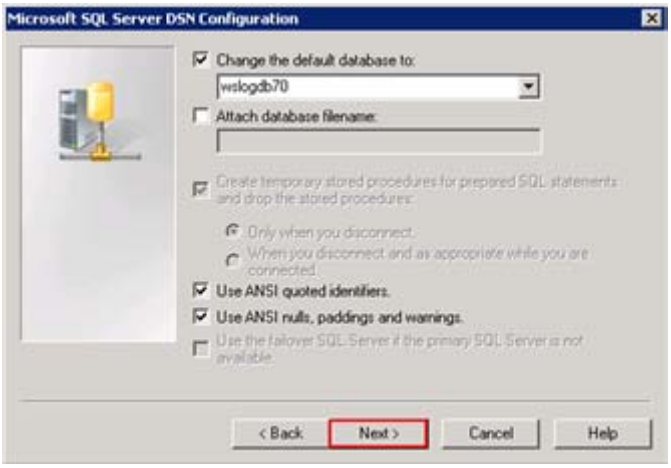


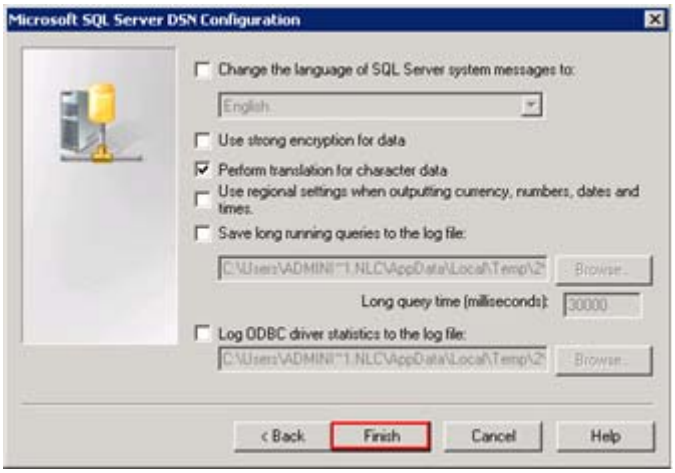
2. **Reconfigure the ODBC Data Source.** Configure the wslogdb70 Data Source. Modify the database, re-enter the credentials, and run the test at the end of the wizard.

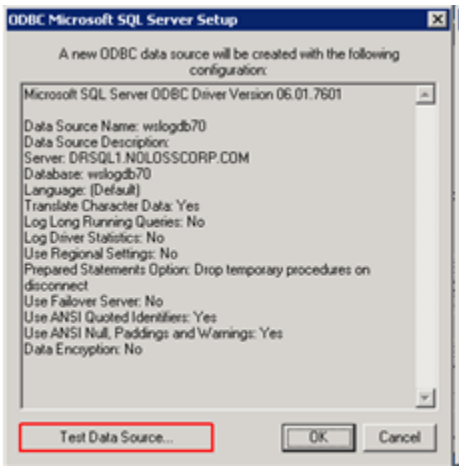


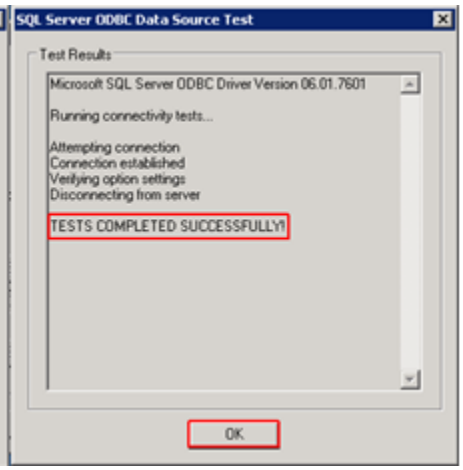




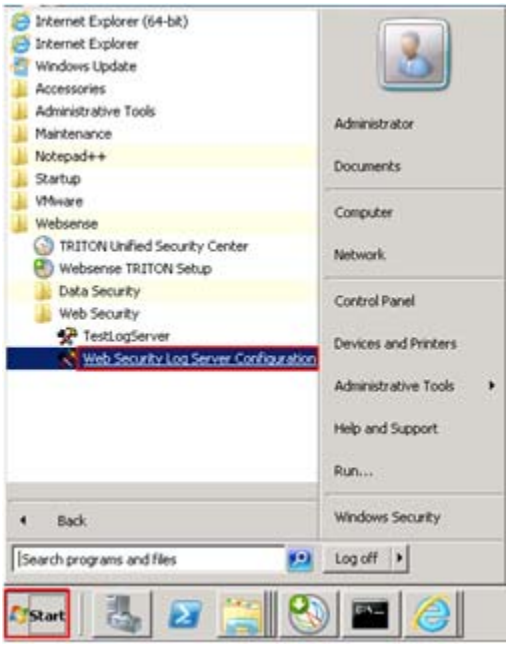

Microsoft SQL Server DSN Configuration
Change the default database to:
wslogdb70
Attach database filename:
Create temporary stored procedures for prepared SQL statements and drop the stored procedures:
Only when you disconnect.
When you disconnect and as appropriate while you are connected.
Use ANSI quoted identifiers.
Use ANSI nulls, paddings and warnings.
Use the failover SQL Server if the primary SQL Server is not available.
< Back
Next >
Cancel
Help

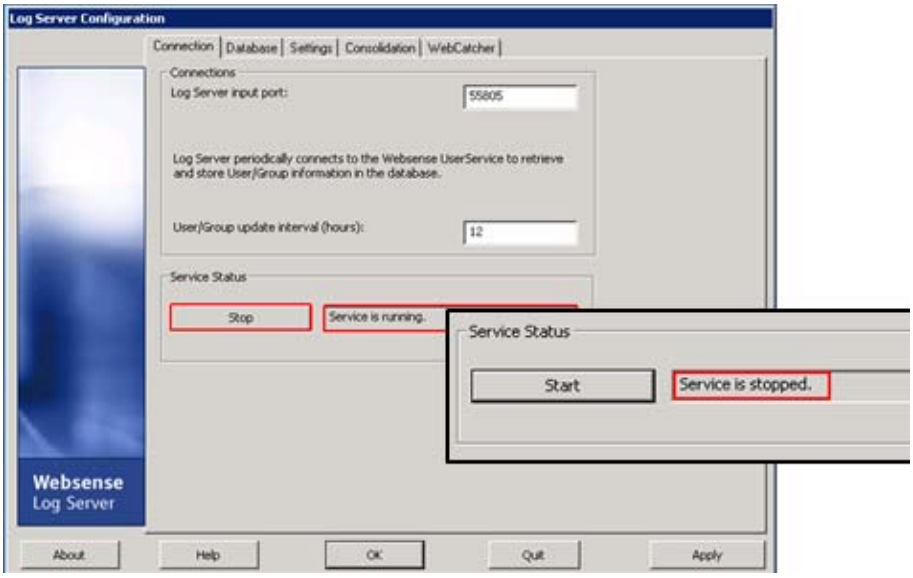

Microsoft SQL Server DSN Configuration
Change the language of SQL Server system messages to:
English
Use strong encryption for data
Perform translation for character data
Use regional settings when outputting currency, numbers, dates and times.
Save long running queries to the log file:
Browse...
Long query time (milliseconds):
30000
Log ODBC driver statistics to the log file:
Browse...
< Back
Finish
Cancel
Help


ODBC Microsoft SQL Server Setup
A new ODBC data source will be created with the following configuration:
Microsoft SQL Server ODBC Driver Version 06.01.7601
Data Source Name: wslogdb70
Data Source Description:
Server: DRSQL1.NOLOSSCORP.COM
Database: wslogdb70
Language: (Default)
Translate Character Data: Yes
Log Long Running Queries: No
Log Driver Statistics: No
Use Regional Settings: No
Prepared Statements Option: Drop temporary procedures on disconnect
Use Failover Server: No
Use ANSI Quoted Identifiers: Yes
Use ANSI Null, Paddings and Warnings: Yes
Data Encryption: No
Test Data Source...
OK
Cancel

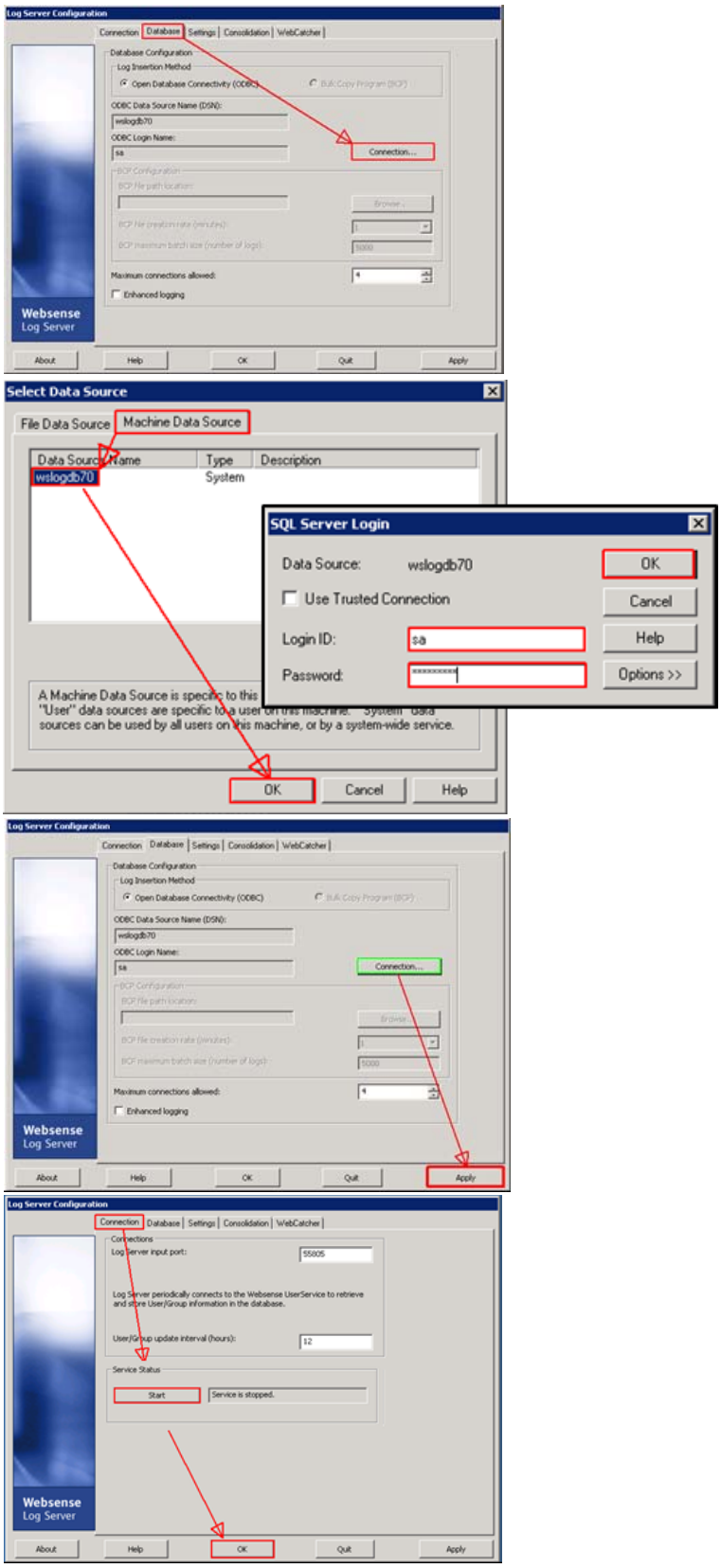

SQL Server ODBC Data Source Test
Test Results
Microsoft SQL Server ODBC Driver Version 06.01.7601
Running connectivity tests...
Attempting connection
Connection established
Verifying option settings
Disconnecting from server
TESTS COMPLETED SUCCESSFULLY!
OK

3. **Reconfigure the Log Server.** Start the Web Security Log Server Configuration applet and stop the service.





Then, re-select the ODBC Data Source. Then, click Apply.



4. **Restart the Websense TRITON Service.** Locate the service called Websense TRITON – Web Security and click Restart.

5. **Results.** The Log Server will use the active database. TRITON data will now come from the active database.

WSVPOLBU – Back up the policy from a Policy source on V10K G2

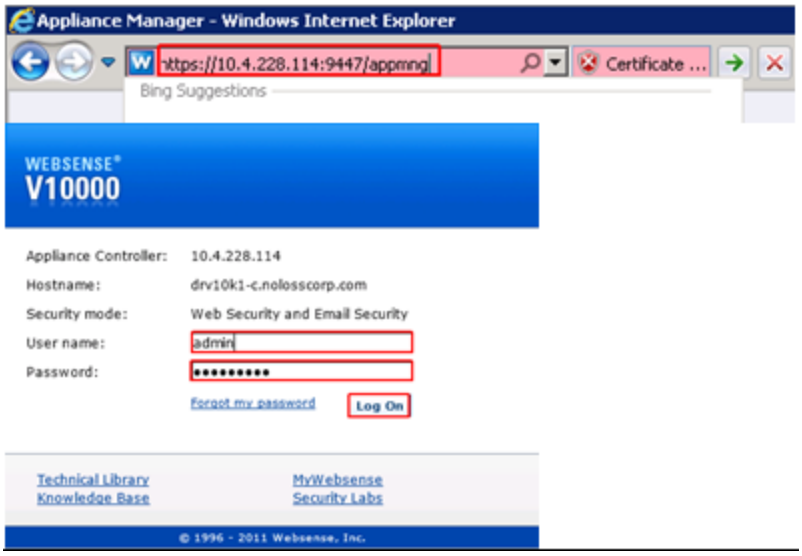
Purpose: Back up the policy from the Policy source to a remote medium that will survive a Disaster Scenario.

Perform on: V10K G2 designated as the Policy source.

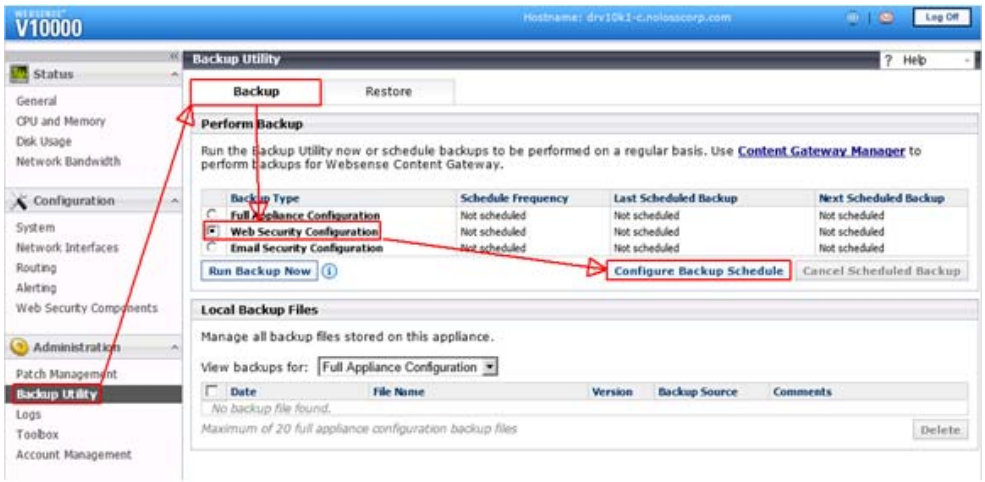
Perform when: Periodically (back up).

Steps How:

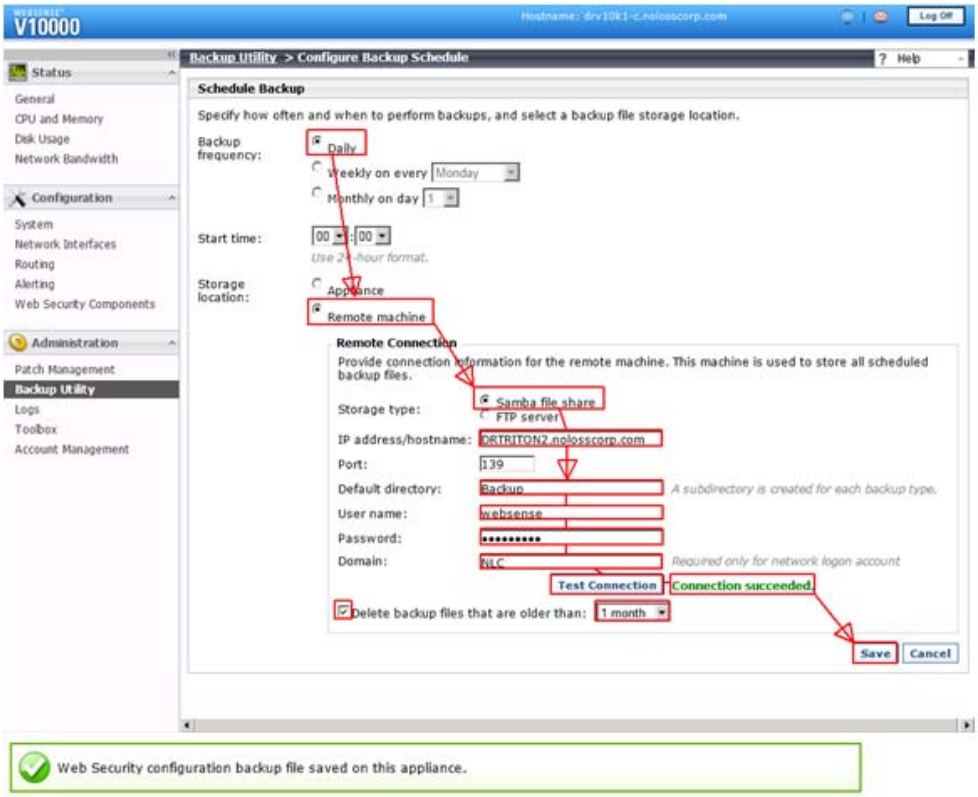
1. **Log on to the Appliance Manager.** Log on to the V10K G2 appliance management console.



2. **Configure Backup Schedule.** Go to the backup schedule configuration screen and select Web Security Configuration only.



Then, set up the schedule and the location with access credentials.



3. **Result.** The appliance will back up the WWS Policy daily to the configured destination.

WSPSLSCFG – Configure a Policy Server to use an active Log Server

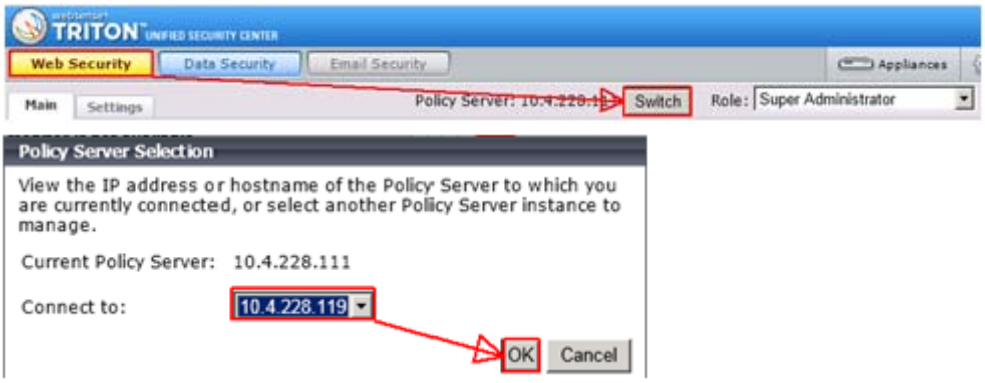
Purpose: Configure a Policy Server to use an active Log Server. In a DR scenario, the Log Server configured on a Policy Server may not be available and may need to be modified to active.

Perform on: TRITON server connected to the Policy Server.

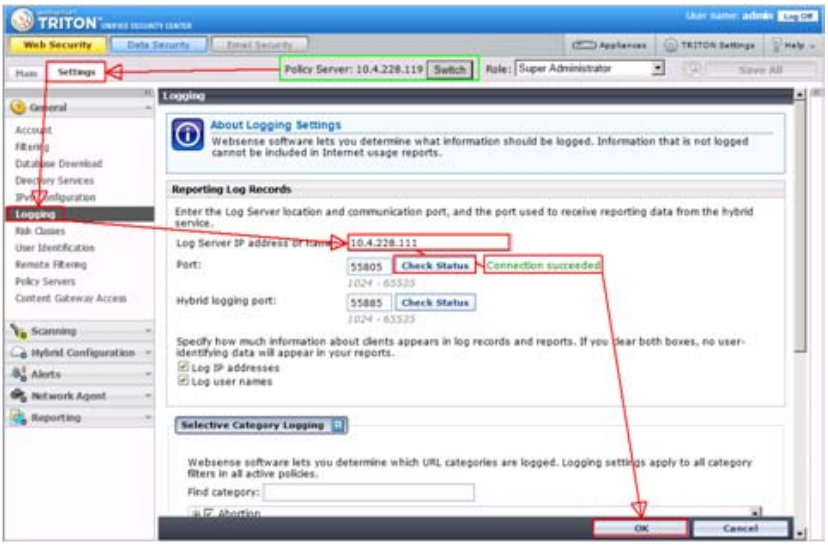
Perform when: In a DR Scenario.

Steps How:

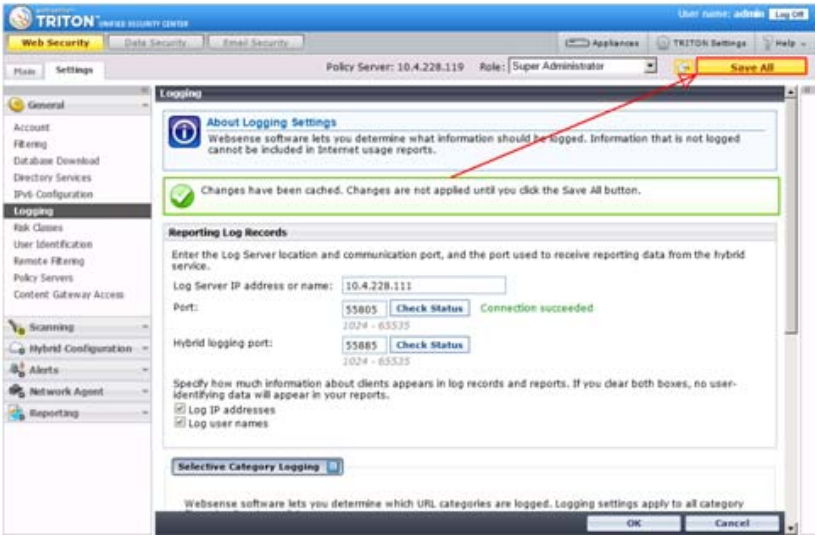
1. **Log on to TRITON console and Switch to the Policy Server on the V10K G2.** Log on to TRITON. If you have more than one Policy Server configured, there will be a Switch button. Click **Switch** to switch to the Policy Server on the V10K G2. In this example, 10.4.228.111 is the local TRITON machine and 10.4.228.119 is the V10K G2 C interface.



2. **Configure the destination Log Server.** Configure the Policy Server's Log Server configuration to send log records to the active Log Server (running on the TRITON box):



3. **Save the settings.** Click **Save All** to save the settings.



4. **Results.** The Policy Server will now send log events to the specified Log Server.

WSVPOLRES – Restore the backed up policy to an alternate V10K G2

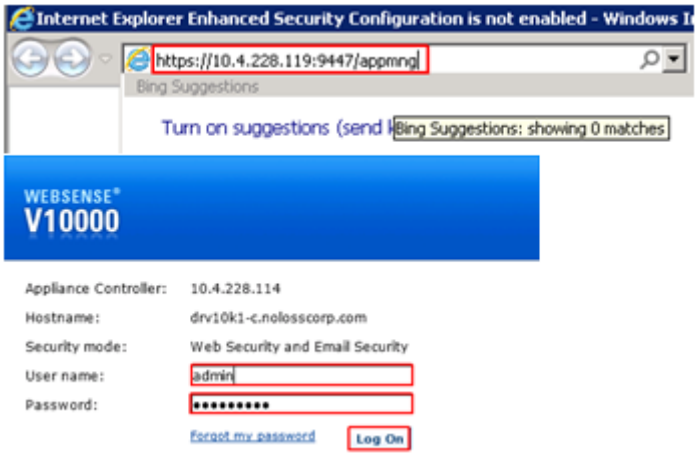
Purpose: Restore the backup to the V10K G2 appliance that was previously configured as Policy Lite to become the new Policy source.

Perform on: V10K G2 that is designated to become the new Policy source.

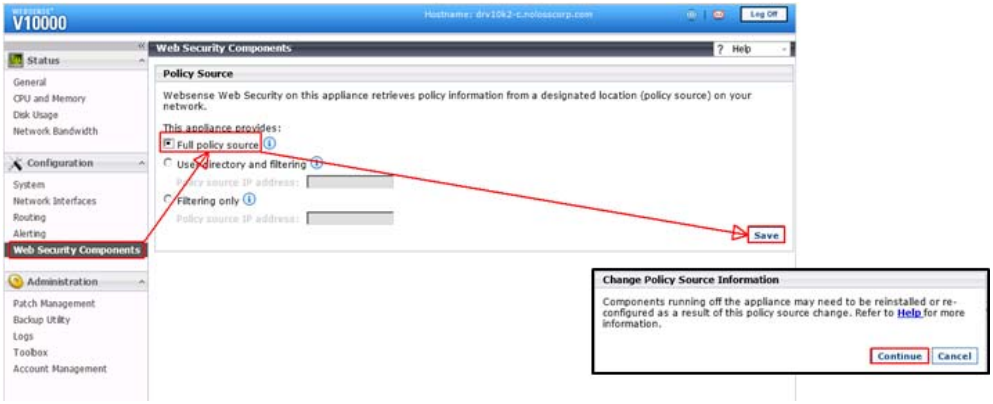
Perform when: In a DR Scenario.

Steps How:

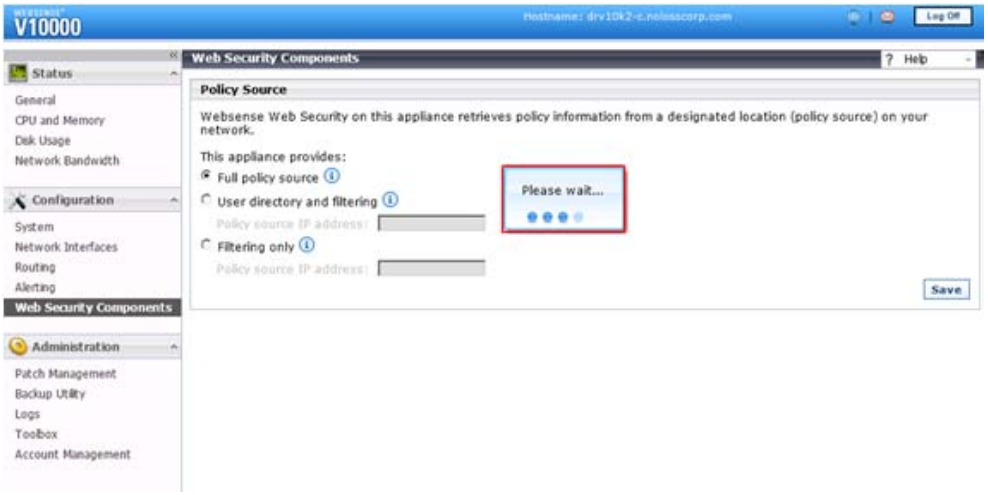
1. **Log on to the Appliance Manager.** Log on to the V10K G2 appliance management console.



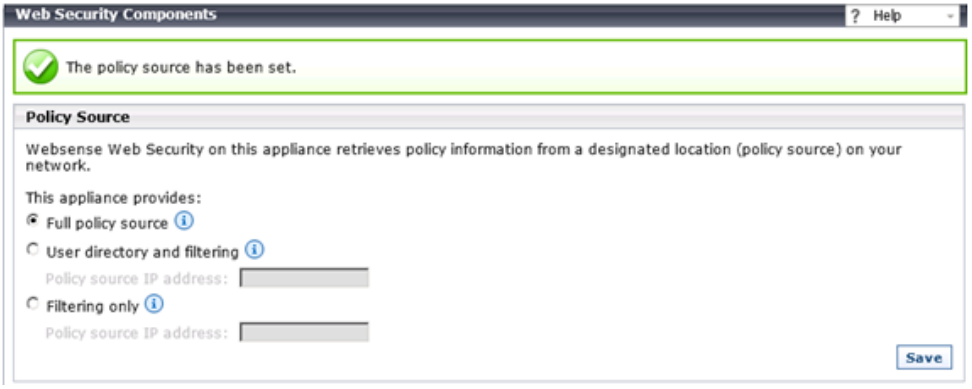
2. **Configure the appliance as a Policy source.** Through the Web Security Components screen, select Full Policy source mode.



3. **Wait.** This process may take up to 5 minutes or more.

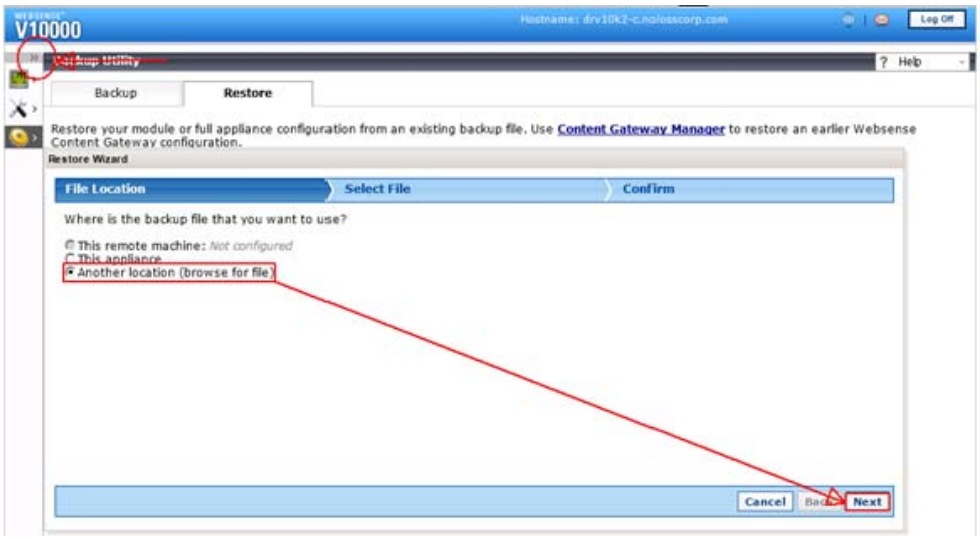


A green check mark indicates that the Policy source has been set up.



4. **Start the Restore Wizard.** Under the Backup Utility Restore tab, select Web Security Configuration. Then, click Run Restore Wizard.

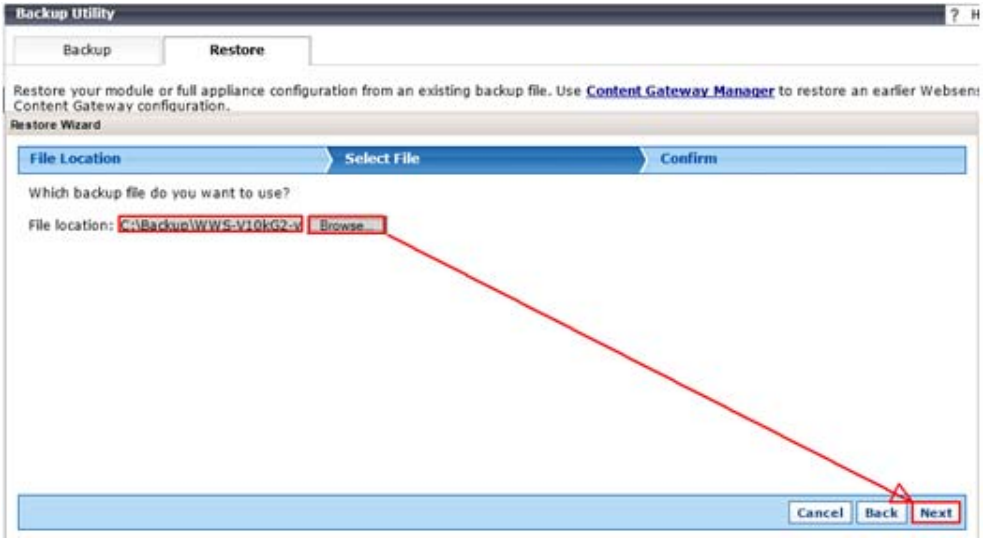
5. **Select the restore source.** Select the **Another location (browse for file)** option and click Next.



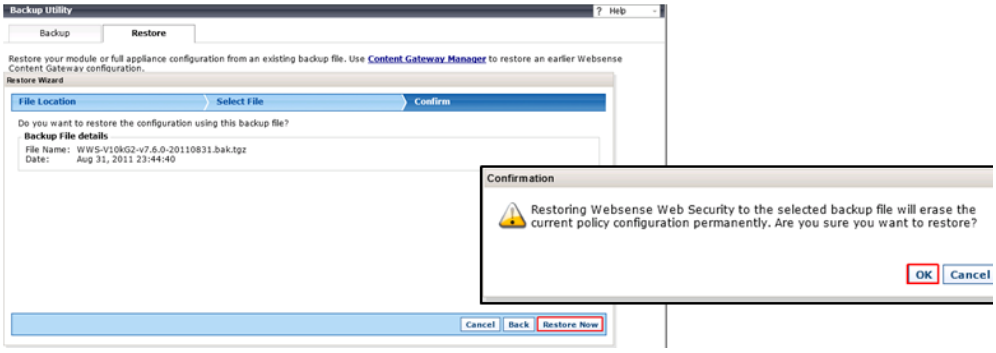
Note

If the “Next” button does not appear, minimize the left side pane to make it visible.

Then, click Browse and select the backup file.

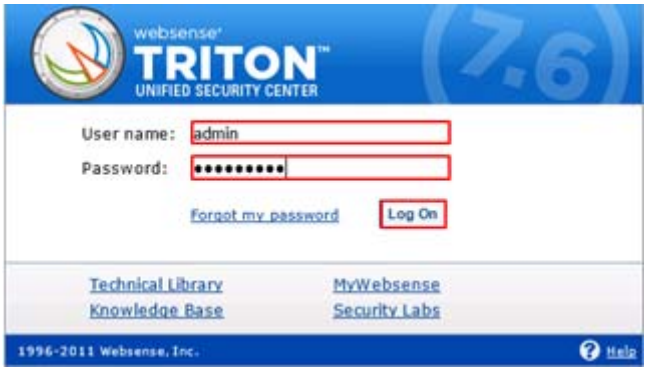


6. **Complete the restore process.** Confirm the details and click Restore Now. Confirm the restore.

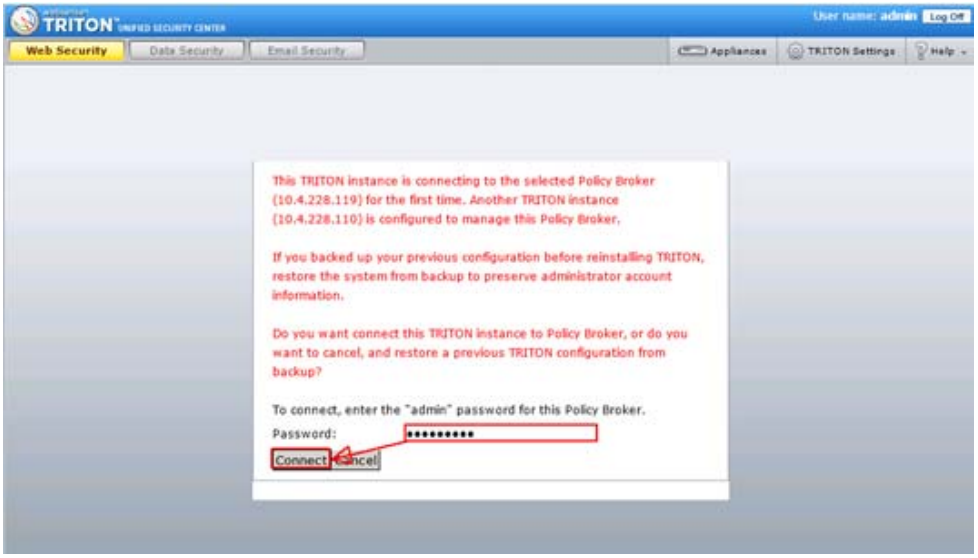


Then, wait until it completes.

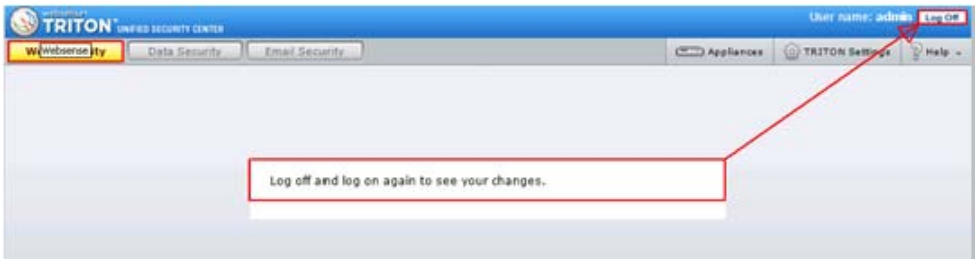
7. Log on to the target TRITON.



8. **Confirm the TRITON instance change.** The backup TRITON should be already set up to use the Policy Server on the designated appliance. Confirm that the changes to the TRITON instance that manages the particular Policy Server have been made:



Then, log off and log on again.



9. **Results.** The appliance is now configured as a Policy source and is restored. The TRITON server is now set up to manage the Policy Server on the appliance.

DSMGRRES – Restore Data Security policies and forensics

Purpose: Restore Data Security forensics and policies so that they are available to view from the DR TRITON. Point the DR TRITON to the correct database.

> **Note**
>
> This procedure requires a few external utilities that are referenced below.

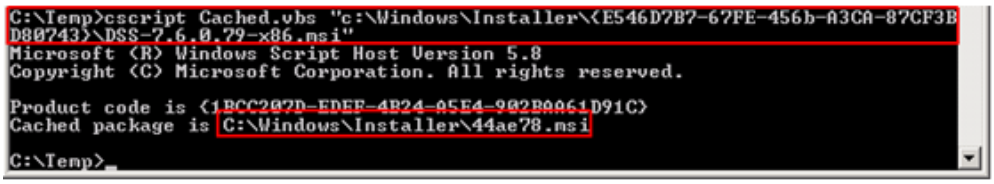
Perform on: TRITON server.

Perform when: In a DR Scenario.

Steps How:

1. **Augment the installer.** The DSS installer has a restore script that is incompatible with this scenario. To modify it and introduce the proper script, locate the cached copy of the of the DSS installer using the scriptCached.vbs:

   cscript Cached.vbs "c:\Windows\Installer\{E546D7B7-67FE-456b-A3CA-87CF3BD80743}\DSS-7.6.0.79-x86.msi"

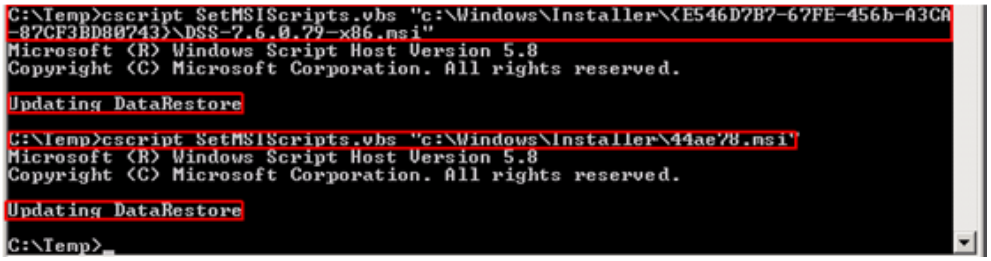


   Then, use the SetMSIScript.vbs to modify both the original and the cached copies:

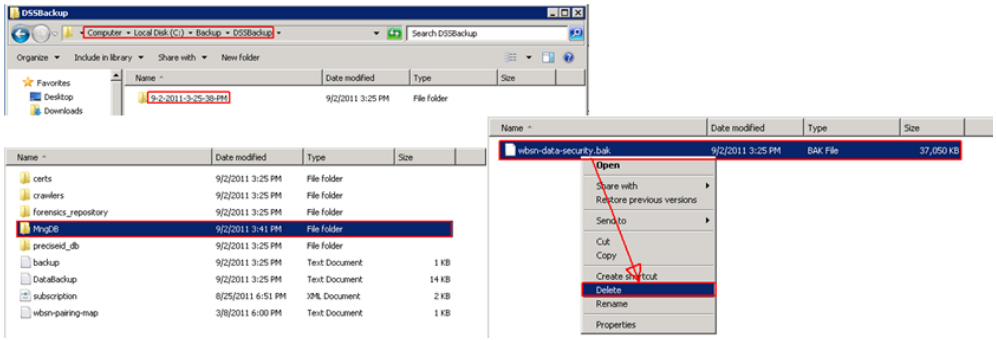
   cscript SetMSIScripts.vbs "c:\Windows\Installer\{E546D7B7-67FE-456b-A3CA-87CF3BD80743}\DSS-7.6.0.79-x86.msi"

   cscript SetMSIScripts.vbs "c:\Windows\Installer\44ae78.msi"

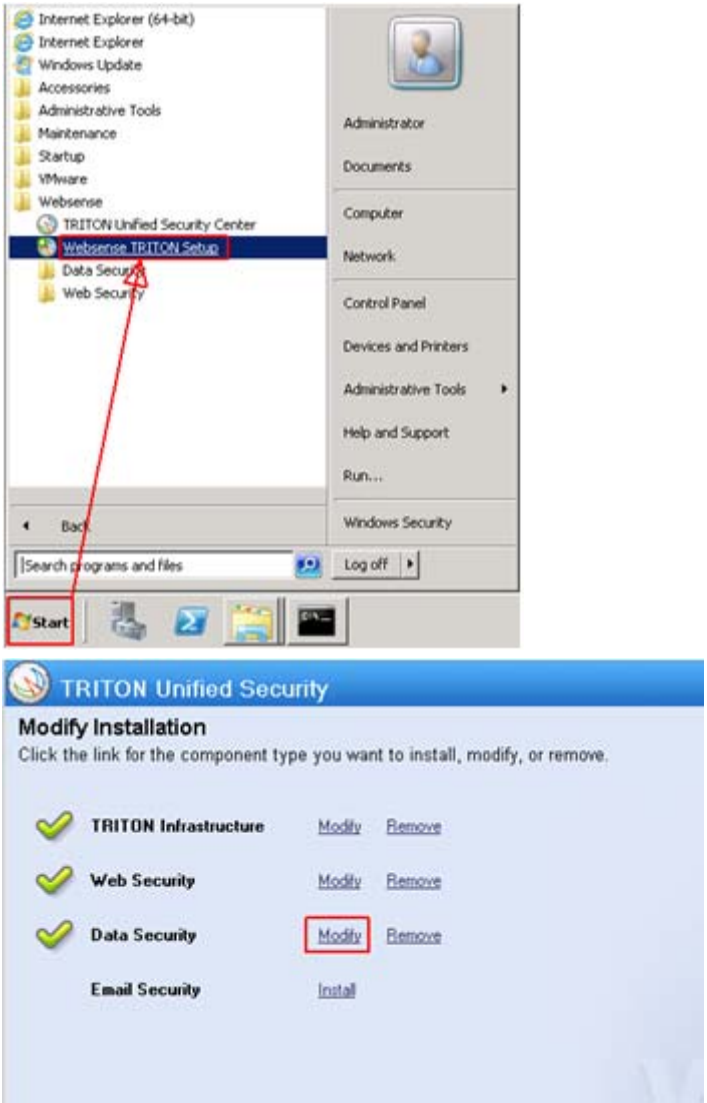
> **Note**
>
> Please note that this script must be run from the same folder as the file DataRestore.txt



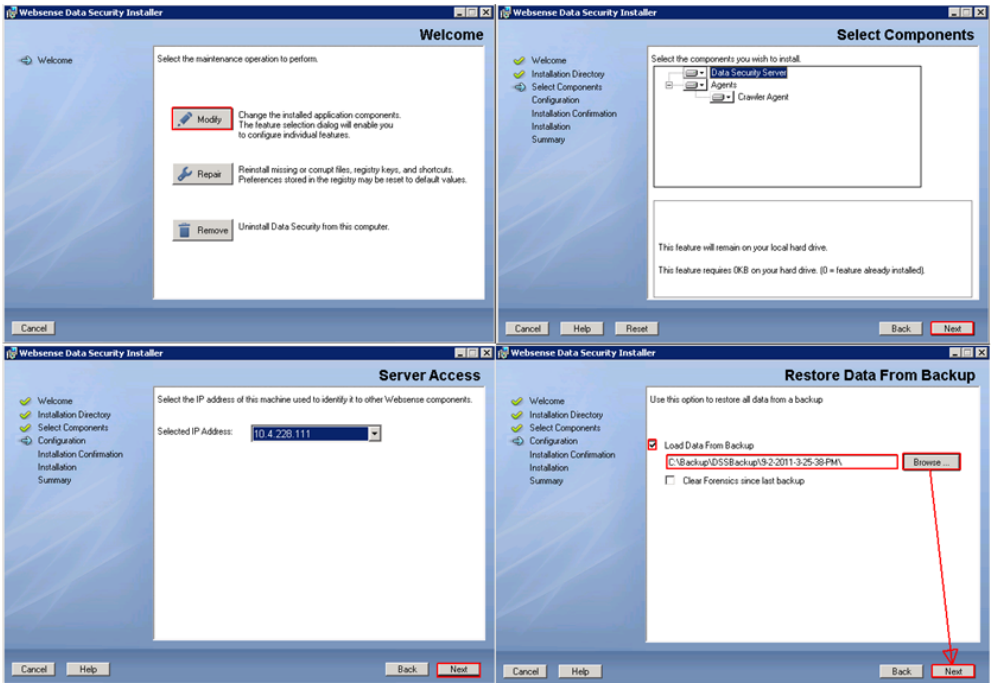
2. **Delete the backup.** Locate the dated folder name for the DSS backup:



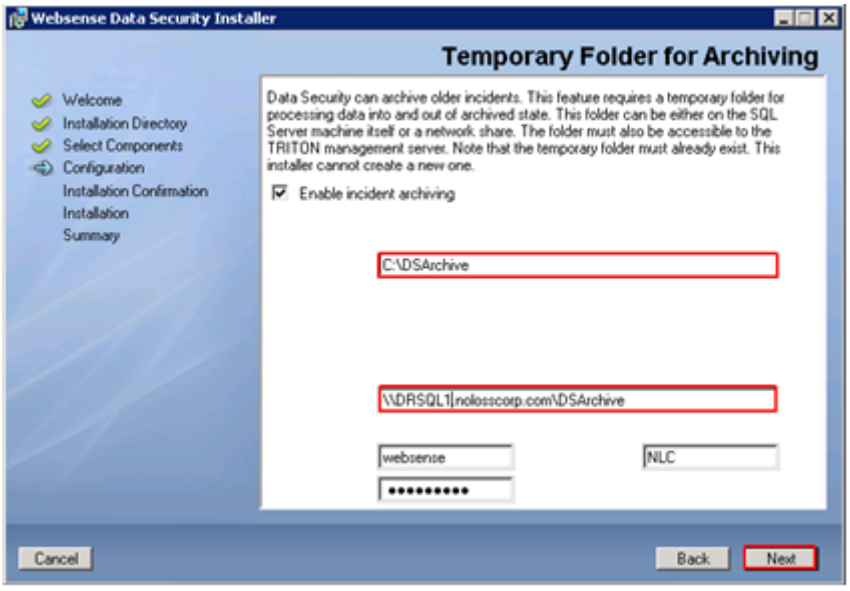
3. **Run the Data Security installer in Modify mode.** Run the Websense TRITON Setup. Then, select the Data Security Modify link.



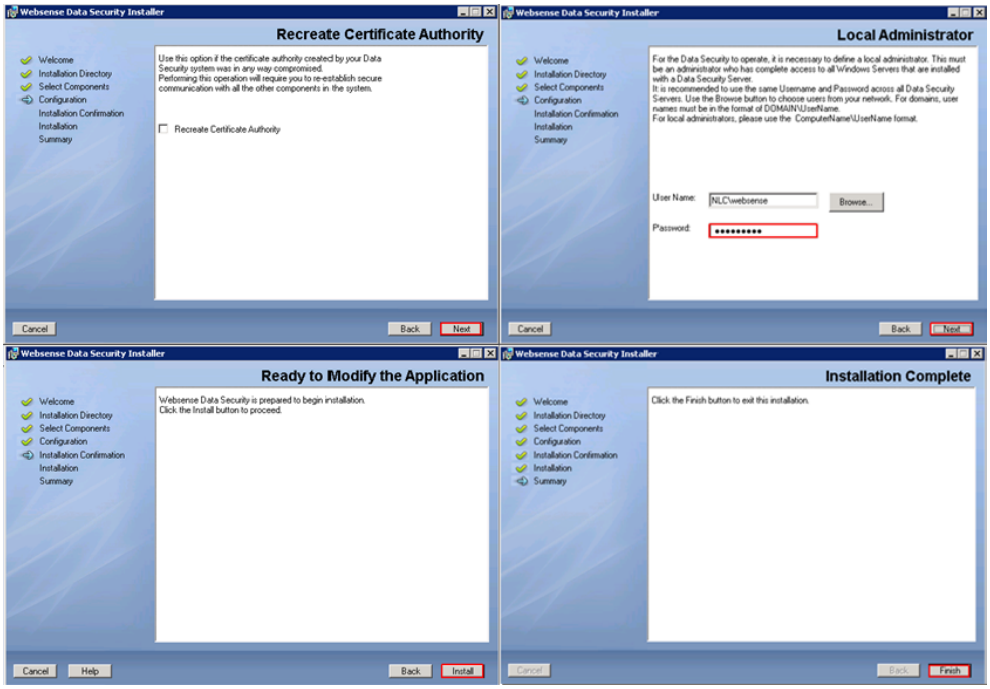
4. **Point the installer at the DSS Backup folder.** Click Modify. Then progress through the wizard to the backup folder selection. Click Browse to select the dated backup folder using and click Next.



5. **Modify the archive location.** Modification of the location of the archive folder to reflect the change in SQL Server may be required. If clicking Next produces an error accessing the SQL Server, this indicates that the EIP restore was not performed properly.



6. **Complete the wizard.** Progress through the wizard until it is completed. Enter the password for the admin user if prompted.



7. **Results.** The DSS Manager has been restored. The forensic data has been linked to the database.

DSSVRREG – Re-register a DSS server with a new TRITON server

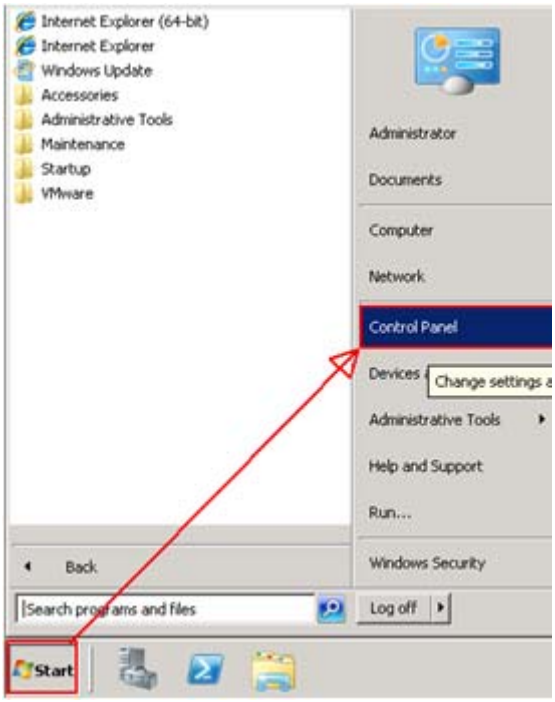
Purpose: Re-establish the communication between a DSS server and the DR TRITON server to enable correct policy deployment and continued service.

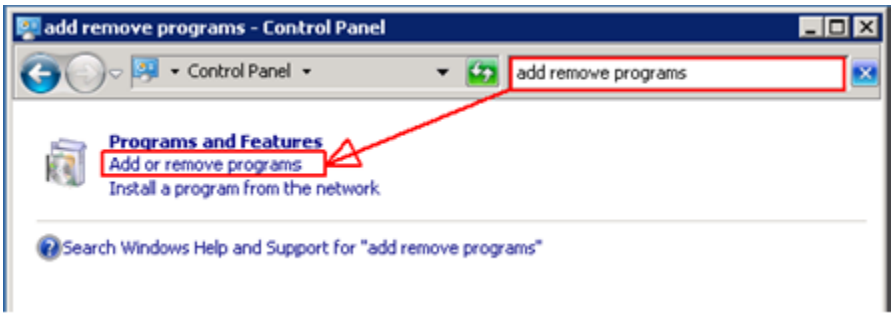
Perform on: Data Security Server.

Perform when: In a DR Scenario.

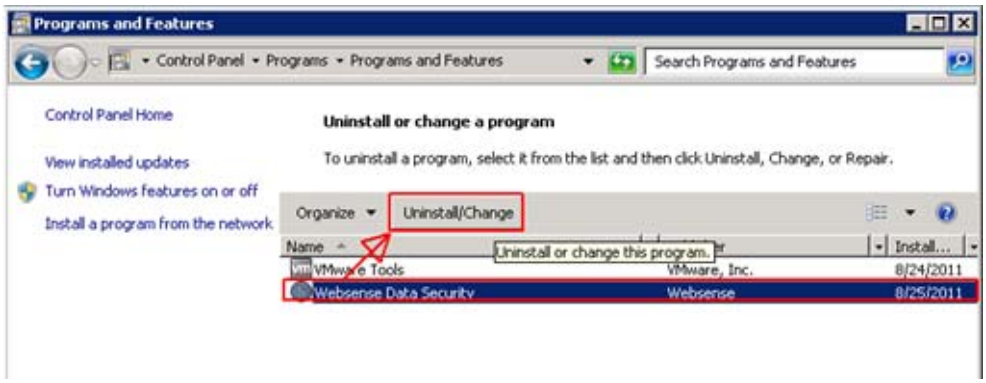
Steps How:

1. **Run the Data Security Server installer in Modify mode.** Run the Data Security Server installer in Modify mode. To re-establish the communication with the TRITON server, open the control panel and run the **Add or remove programs** applet.

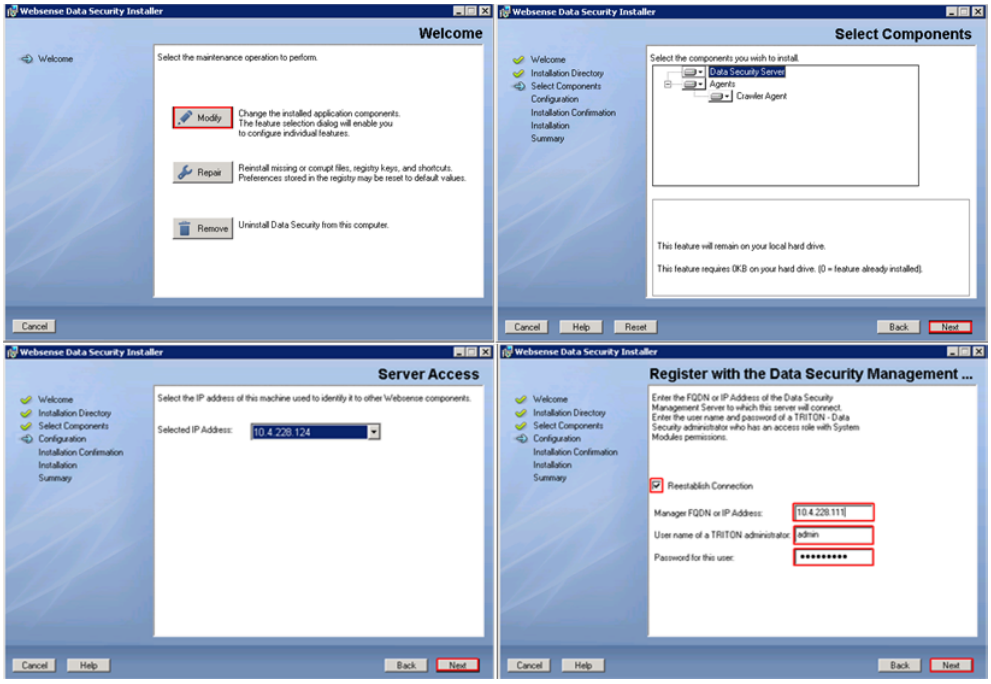




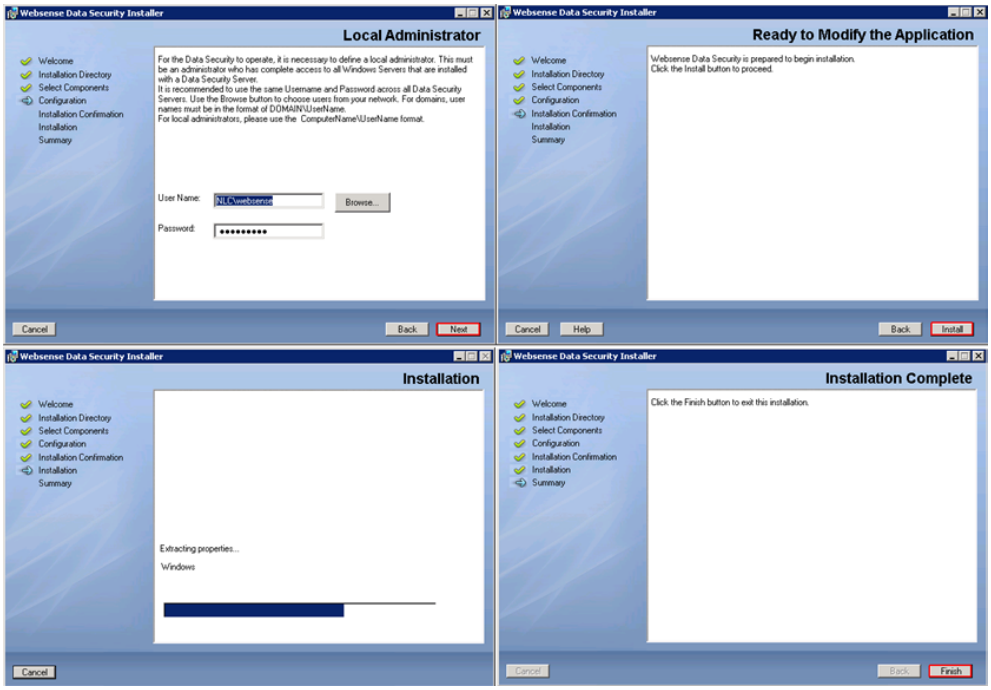
Then, select the Websense Data Security program.



2. **Re-register the DSS server.** Click Modify and progress through the wizard to the Register with the Data Security Management screen. Check **Reestablish Connection**, and fill in the new IP address.



3. **Complete the installer.** Progress through the wizard screens until it completes.



4. **Results.** DSS Server is now configured to accept policy and report incidents to the TRITON manager.

DSWCGREG – Re-register a WCG server with a new TRITON server

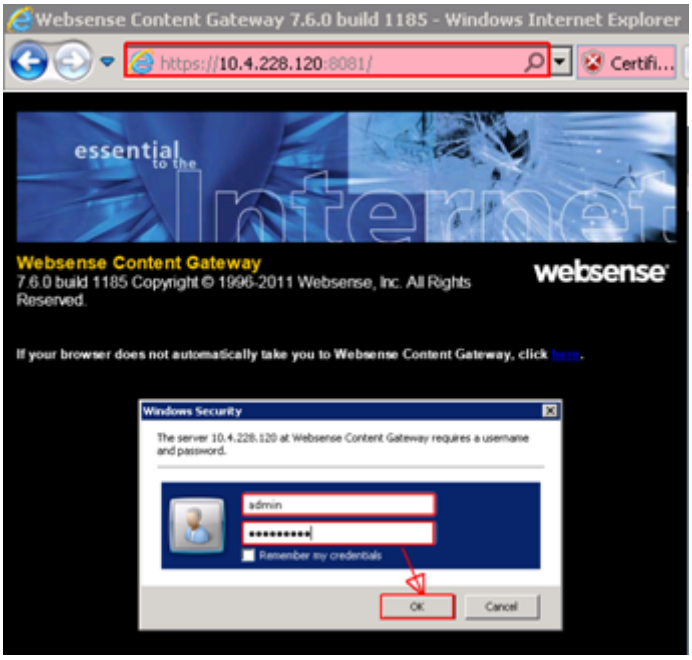
Purpose: Re-establish the communication between a WCG server and the DR TRITON server to enable correct policy deployment and continued service

Perform on: WCG Server

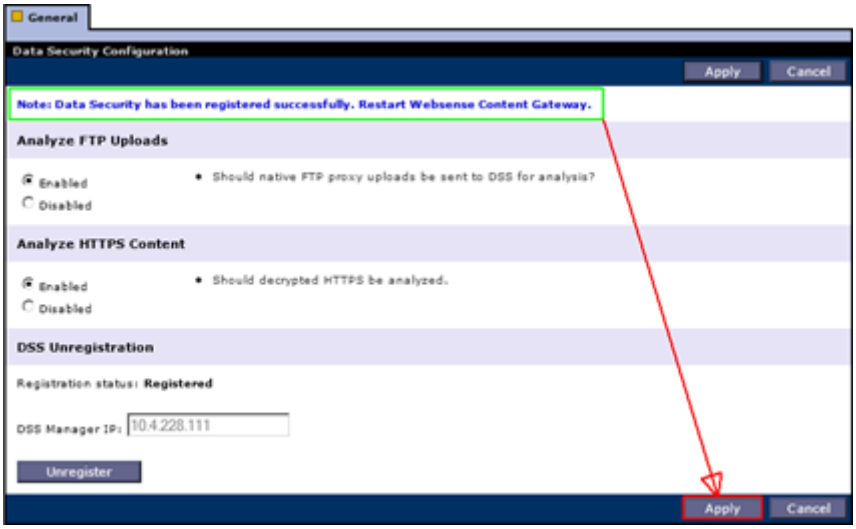
Perform when: A DR Scenario

Steps How:

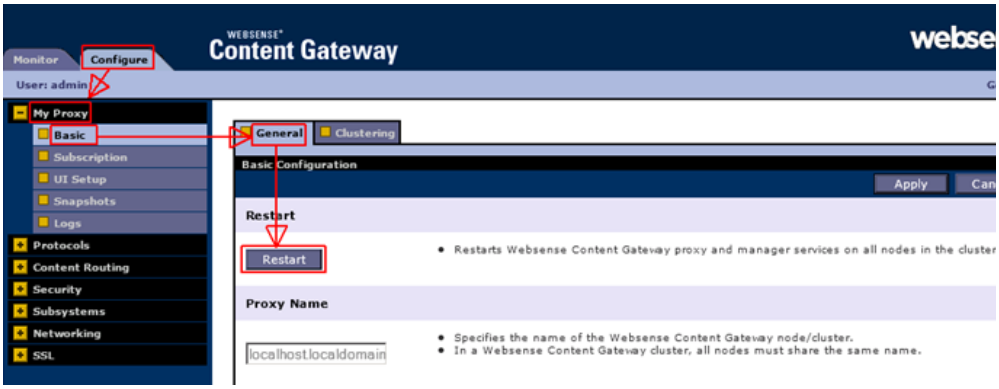
1. **Unregister WCG.** Log on to WCG (V10K G2 “P1” port). Go to Data Security Configuration and click Unregister.



2. **Re-register WCG.** Enter the TRITON IP address, username and password. Then click Register.



3. **Restart the WCG.** Select **Basic** from the **My Proxy** submenu in the configuration tab, then click Restart.



4. **Result.** WCG is now configured to accept policy and report incidents to the TRITON manager.

DSMGRDEP – Deploy settings for all re-registered components

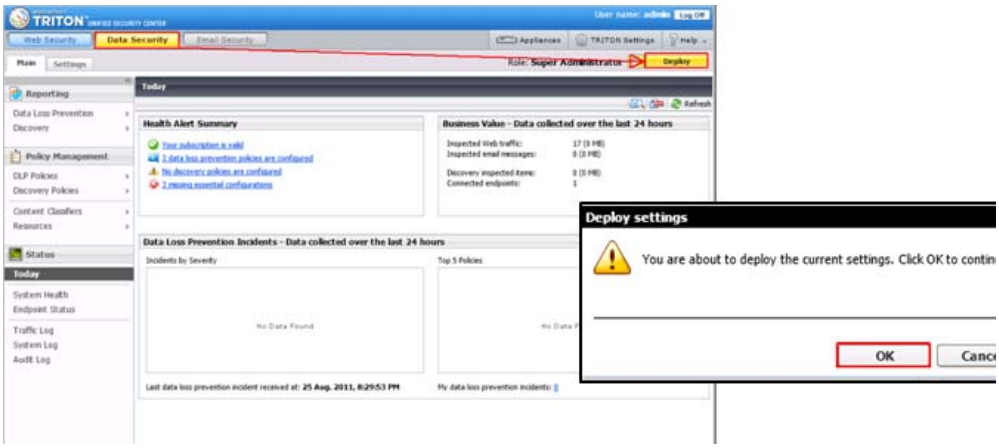
Purpose: Deploy current settings to all re-registered DSS components.

Perform on: TRITON server.

Perform when: In a DR Scenario.

Steps How:

1. **Log on to the DSS TRITON console and Deploy.** Log on to the DR TRITON console. Then, click the yellow Deploy button.



2. **Wait for a successful deployment of all components.** Enter the TRITON IP address, username and password. Then, click Register.

Deployment Process

Name	Status	Deployment Results	Last Configuration	Deployed by
DSS Server on DRTRITON1....	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Endpoint Server DRTRITON...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Policy Engine DRTRITON1...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Forensics Repository DR...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Primary Fingerprint Repo...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Crawler DRTRITON1.noloss...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
DSS Server on DRSERVER2....	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Endpoint Server DRSERVER...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Policy Engine DRSERVER2...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Secondary Fingerprint Re...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Crawler DRSERVER2.noloss...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Content Gateway on drv1...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Policy Engine drv10k2-c...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin
Secondary Fingerprint Re...	Processing	Not Deployed	02 Sep. 2011, 11:42:32 PM	admin

Deployment Process

Name	Status	Deployment Results	Last Deployment	Deployed by
DSS Server on DRTRITON1....	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:45 PM	admin
Endpoint Server DRTRITON...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:43 PM	admin
Policy Engine DRTRITON1...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:43 PM	admin
Forensics Repository DR...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:35 PM	admin
Primary Fingerprint Repo...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:44 PM	admin
Crawler DRTRITON1.noloss...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:45 PM	admin
DSS Server on DRSERVER2....	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:45 PM	admin
Endpoint Server DRSERVER...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:44 PM	admin
Policy Engine DRSERVER2...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:43 PM	admin
Secondary Fingerprint Re...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:44 PM	admin
Crawler DRSERVER2.noloss...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:45 PM	admin
Content Gateway on drv1...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:53 PM	admin
Policy Engine drv10k2-c...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:53 PM	admin
Secondary Fingerprint Re...	Success	All configuration settings were committed successfully	02 Sep. 2011, 11:42:53 PM	admin

3. **Result.** Policy and settings are deployed to all of the DSS components. Components that did not survive the DSS scenario will fail the deployment and can safely be ignored.

WSRFSCFG – Reconfigure Remote Filtering Servers to point to active server

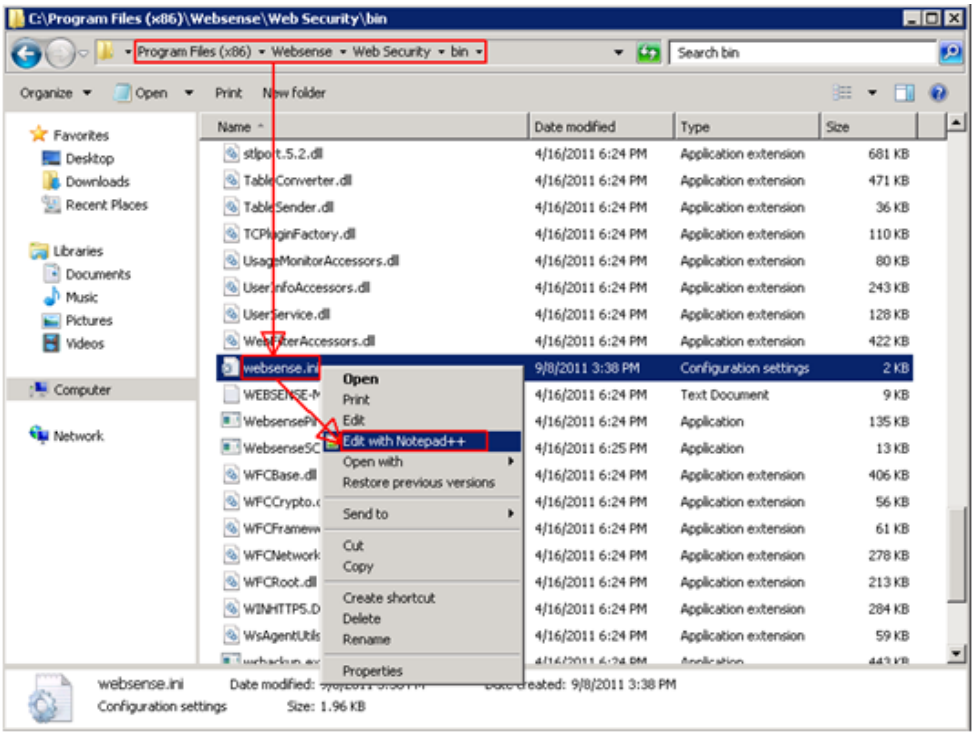
Purpose: A Remote Filtering Server should be redirected in the event it survives the DR scenario, but the Policy Server/ Filtering Service it is using does not.

Perform on: Remote Filtering Service machine

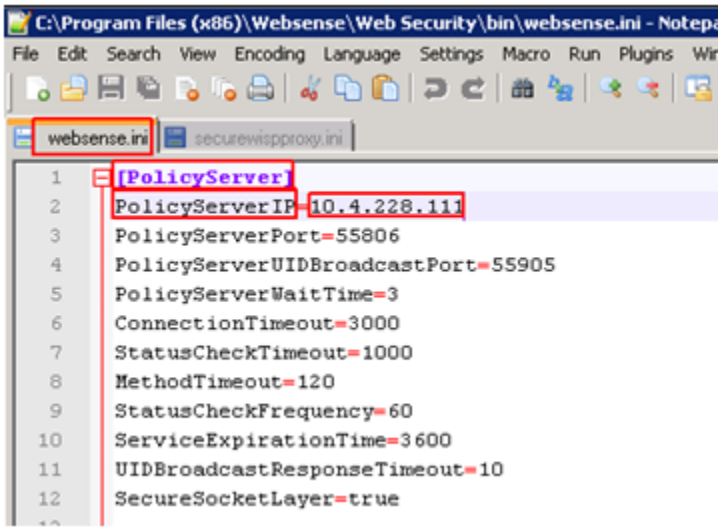
Perform when: In a DR Scenario.

Steps How:

1. **Modify websense.ini to change the Policy Server.** Log on to the RFS and open the websense.ini file.

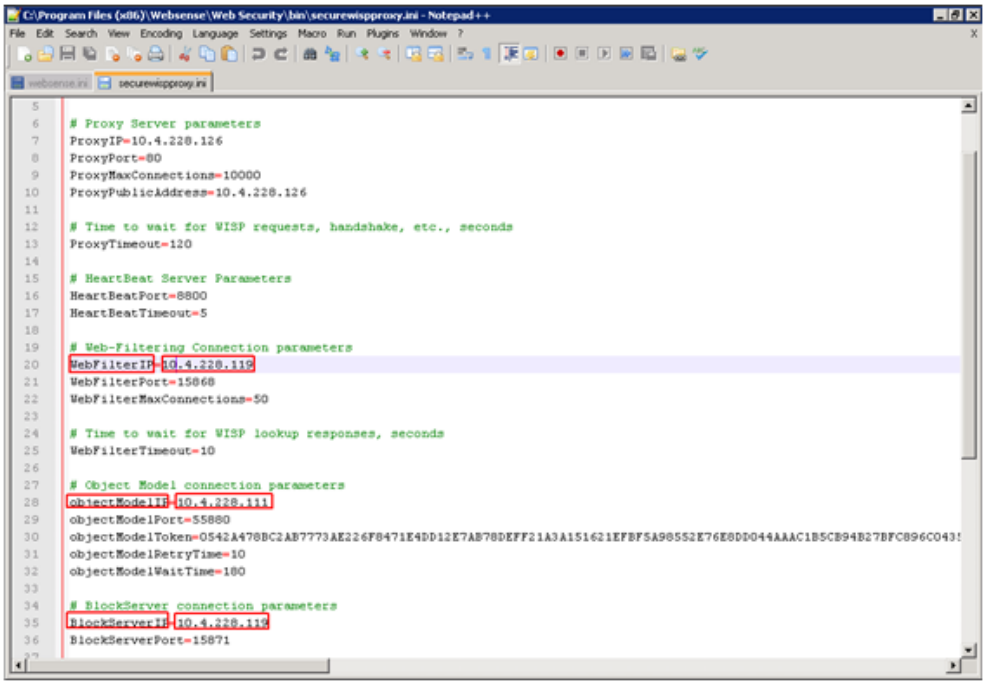


Then, edit the PolicyServerIP value in the PolicyServer section (should be toward the beginning of the document) to the IP address of a Policy Server on a surviving V10K G2 appliance. If the Policy Server pointed to by the value survived the disaster, there is no need to modify it.

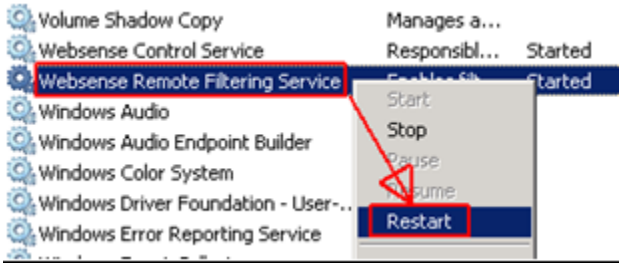


2. **Modify the securewispproxy.ini file to change the Policy Server and Filtering Service.** Edit the securewispproxy.ini file.

Then, edit the values WebFilterIP, objectModelIP, and BlockServerIP to point to the Policy Server / Filtering Service. The WebFilterIP and BlockServerIP point to the Filtering Service, and the objectModelIP points to the Policy Server. The same IP address may be used in cases where the V10K G2 appliance contains both.



3. **Restart the Remote Filter Service.** Run the services applet and restart the Websense Remote Filtering Service.



4. **Result.** The Remote Filtering Service will use the new Policy Server / Remote Filtering Service.