

Backup and Restore FAQ

45070 | Backup and Restore | Web, Data, and Email Protection | 18-Apr-2016

Applies to:	TRITON AP-WEB and Web Filter & Security, v8.2.x TRITON AP-DATA, v8.2.x TRITON AP-EMAIL, v8.2.x
--------------------	--

Regularly back up configuration information for your Forcepoint™ TRITON® solution so that you can revert to a previous configuration when needed. Data saved by the backup process can also be used to transfer configuration settings to a different machine or V-Series appliance.

In most circumstances, when you use backup and restore to transfer configuration settings between servers, only same-platform transfers are supported. In other words, you can move from Windows to Windows or Linux to Linux, but not from Windows to Linux (or vice-versa).

When backing up a TRITON management server, note that there are separate backup processes for TRITON infrastructure and other components on the machine.

Synchronize the TRITON infrastructure backup with the backup procedures for other components.

- [*How do I back up and restore the TRITON infrastructure?*, page 2](#)
- [*How do I back up and restore V-Series appliances?*, page 6](#)
- [*How do I back up and restore web protection software?*, page 10](#)
- [*How do I back up and restore Content Gateway?*, page 17](#)
- [*How do I back up and restore TRITON AP-DATA?*, page 19](#)
- [*How do I back up and restore TRITON AP-EMAIL off-appliance components?*, page 22](#)
- [*How do I back up or restore web protection components and the TRITON Manager?*, page 24](#)
- [*How do I back up or restore multiple TRITON AP-WEB appliances?*, page 25](#)

How do I back up and restore the TRITON infrastructure?

45071 | Backup and Restore | Web, Data, and Email Protection | 18-Apr-2016

Applies to:	TRITON AP-WEB and Web Filter & Security, v8.2.x TRITON AP-DATA, v8.2.x TRITON AP-EMAIL, v8.2.x
--------------------	--

The TRITON infrastructure backup process saves:

- Global configuration and infrastructure information, including administrator and appliance data, stored in the TRITON Settings Database.
- Certificate files required for the TRITON browser components.

When you either initiate an immediate backup (see [Running immediate TRITON infrastructure backups](#)) or define a backup schedule (see [Scheduling TRITON infrastructure backups](#)), backup files are stored in the C:\EIPBackup directory by default. To change the backup location, see [Changing backup settings](#).

The backup process checks all TRITON infrastructure components on the machine, collects the data eligible for backup, and creates a new folder in the EIPBackup directory with the format:

mm-dd-yyyy-hh-mm-ss-PP

This format represents the date and time of the backup (05-10-2011-10-45-30-PM, for example).



Important

Make sure that all administrators log off from the TRITON Manager before you back up or restore your configuration.

Scheduling TRITON infrastructure backups

When you installed TRITON Manager, a scheduled task for backups was created. By default this task is disabled.

Notify TRITON administrators of the backup schedule, so that they can be sure to log off from TRITON Manager during the backup process.

Although backups do not interfere with system operation, as a best practice, schedule backups when the system isn't under significant load.

To schedule backups:

1. On the TRITON management server machine, open the Windows Task Scheduler:
 - Windows 2012: Open **Administrative Tools** and select **Task Scheduler**.
 - Windows 2008: Go to **Start > Administrative Tools > Task Scheduler**.
2. In the **Task Scheduler** window, select Task Scheduler Library.
3. Right-click the **Triton Backup** task and select **Enable**.
4. Right-click **Triton Backup** again and select **Properties**, then select the **Triggers** tab.
5. Click **Edit**, and edit the schedule as required. By default, the task is scheduled to run weekly on Saturdays at midnight.
6. Click **OK** twice.

If requested, enter the administrator password for the TRITON management server machine to confirm the changes to the task.

Running immediate TRITON infrastructure backups

Before running a manual backup, make sure that all administrators are logged off from TRITON Manager.

To launch an immediate backup:

1. On the TRITON management server, open the Windows Task Scheduler:
 - Windows 2012: Open **Administrative Tools** and select **Task Scheduler**.
 - Windows 2008: Go to **Start > Administrative Tools > Task Scheduler**.
2. In the **Task Scheduler** window, select Task Scheduler Library.
3. If the **Triton Backup** task is disabled, right-click the task and select **Enable**.
4. Right-click the **Triton Backup** task and select **Run**.

Restoring TRITON infrastructure backup data

You can activate the restore operation from the TRITON Infrastructure “Modify” wizard. Make sure that all administrators are logged off from TRITON Manager.

Before starting the restore process, it is recommended that you stop the TRITON Manager service. If you are running a web protection solution, see *How do I back up or restore web protection components and the TRITON Manager?*, page 24.

To restore TRITON infrastructure data:

1. On the TRITON management server, open the Windows Services tool:
 - Windows 2012: Go to **Server Manager > Tools > Services**.
 - Windows 2008: Go to **Start > Administrative Tools > Services**.

2. Right-click the **Websense TRITON Unified Security Center** service and select **Stop**. (You may also need to stop web protection services. See the article linked above.)
3. Open the Windows Control Panel and select **Programs > Programs and Features**, then select **Websense TRITON Infrastructure**.
4. Click **Uninstall/Change**.
5. When asked if you want to modify, repair, or remove the TRITON Infrastructure, select **Modify**.
6. Click **Next** until you get to the **Restore Data from Backup** screen.
7. Mark the **Use backup data** box and click the **Browse** button to locate the backup folder.
8. Click **Next** until you begin the restore process.
9. Click **Finish** to complete the restore wizard.
10. Go back to the Services window and click **Refresh**. If any service that you stopped manually has not restarted, right-click it and select **Start**.

Once the restore process is complete, a file named **DataRestore.log** is created in the date-stamped backup folder that was used for the restore.

Changing backup settings

When you run your first backup, an **EIPBackup** directory is created to contain the date-stamped folders for each set of backup files. By default this directory is created in **C:**. You can change this location, and also define how many old backups are kept in the backup directory.

To change the settings for the backup files:

1. On the TRITON Management Server, go to the directory where you installed TRITON Unified Security Center (by default **C:\Program Files (x86)\Websense**), and access the **EIP Infra** directory.
2. Open **EIPBackup.xml** in a text editor such as Notepad.

This file contains the following parameters:

Parameter	Description
NUM_OF_COPIES	The number of old backups to store in the backup directory. Defaults to 5.
PATH	The location of the EIPBackup directory. Defaults to C:\ .
DOMAIN	Only required if the <PATH> parameter is set to access a remote machine and you need to supply credentials in the form domain\user to write to the location. Leave this field blank if you have defined a path on the local machine, or if you have entered credentials in <USER_NAME>.

Parameter	Description
USER_NAME	Only required if the <PATH> parameter is set to access a remote machine and you need to supply a user name to write to the location. Leave this field blank if you have defined a path on the local machine, or if you have entered credentials in <DOMAIN>.
PASSWORD	Only required if the <PATH> parameter is set to access a remote machine and you have entered credentials in either <DOMAIN> or <USER_NAME>. Passwords are stored as plain text.

3. Edit the <NUM_OF_COPIES> parameter to specify the number of old backups that should be kept. Once this number is reached, the oldest backup is deleted when the next backup is run.
4. Edit the <PATH> parameter to define the location of the backup files. The location must exist already as the backup process will not create it. For example, if you set the parameter to a location on the TRITON management server machine, such as:

<PATH>D:\TRITON\Backups</PATH>

the backup files will be stored in D:\TRITON\Backups\EIPBackup.

You can also set the location to be another machine on your network, for example:

<PATH>\\\hostname_or_IP_address\TRITON\backups</PATH>

If you do this, you may also need to enter credentials for access to the remote machine in the <USER_NAME> or <DOMAIN>, and <PASSWORD> parameters. This is not recommended as the password is stored as plain text and could therefore be accessed by other users. Instead, store the backups in a location to which you have write access without needing credentials.



Note

If you change the location of the backup files, outdated backup files will only be deleted in the new location. Old backups will not be deleted from any previous locations.

5. Save the file when done. Changes take effect when the next backup is run.

How do I back up and restore V-Series appliances?

45072 | Backup and Restore | Web and Email Protection Solutions | 18-Apr-2016

Applies to:	TRITON AP-WEB and Web Filter & Security, v8.2.x TRITON AP-EMAIL, v8.2.x
--------------------	--

Two types of backup are available on the V-Series appliance:

- A **full appliance configuration** backup saves:
 - All configuration settings for the appliance controller
 - Configuration and policy information for the Web module, if installed
 - Configuration and policy information for the Email module, if installedForcepoint LLC, recommends running a full backup on every appliance in your network on a regular basis. Note that the full backup file may be smaller than the module backup files, because of the compression used.
- A **module configuration** backup saves all configuration information for the selected module (Web or Email).
 - This includes any client and policy data stored on the selected appliance.
 - For TRITON AP-WEB appliances, the module backup includes Network Agent configuration, but not Content Gateway configuration.Content Gateway backups are performed in the Content Gateway manager. See [How do I back up and restore Content Gateway?, page 17](#).

Running the appliance backup utility

1. Log on to the Appliance manager and go to the **Administration > Backup Utility** page.
2. Do one of the following:
 - To run an immediate backup, click **Run Backup Now**.
 - To schedule the backup process to run at a regular interval, click **Configure Backup Schedule**.

If you are creating scheduled backups:

1. Select a **Backup frequency**: daily, weekly, or monthly.
 - For weekly backups, select which day of the week the backup is run.
 - For monthly backups, select which day of the month the backup is run. You cannot schedule backups to run on the 29th, 30th, or 31st day of the month, because not all months have those days.

2. Specify a **Start time** for the backup process. Enter the time in 24-hour format (where 00:00 indicates midnight, and 12:00 indicates noon).
 - Ideally, select a time when the appliance is unlikely to be under heavy load.
 - If you have multiple appliances, or a distributed environment, schedule backups for TRITON Manager and all machines that include web protection components to run within a 30 minute window. This simplifies the process of restoring a previous configuration, if required.
3. Provide a **Storage location** for the backup files. Only one remote backup location can be configured.
 - Select **Appliance** to have the file stored locally. A maximum of 20 backup files can be saved, and the backup file directory cannot be renamed, moved, or deleted.
 - Select **Remote machine** to store the backup file on another machine in the network, then indicate whether to use a **Samba file share** or **FTP server** and provide the following connection information:
 - a. The **IP address/hostname** of the remote machine, and the connection **Port** to use.
 - b. The **Default directory** in which backup files will be created. A different subdirectory will be created automatically for each backup file type.

Important

If you want to create backup files for multiple appliances on the same remote machine, be sure to use a separate directory for each appliance's backup files.

This avoids the possibility of conflicts that could lead to files being mistakenly overwritten or deleted.

- c. The **User name** and **Password** to use when connecting to the remote machine. If a network logon is used, also provide the **Domain** in which the account resides.

Make sure that the account entered has **read**, **write**, and, if necessary, **delete** permissions in the specified directory.
 - d. Click **Test Connection** to make sure the appliance can communicate with the remote machine and write to the specified location.

Note that the test process will verify that the specified account has **read** permissions, but may not completely verify **write** permissions. **Delete** permissions are not tested.
 - e. If you want remote backup files to be automatically deleted after a specified time period, mark the **Delete backup files that are older than** check box, and then select a time period from the list.
4. Click **Save** to save your changes and return to the Backup Utility page. The new backup schedule is displayed in the Perform Backup list.

Restoring your appliance configuration

When you initiate the restore process, all current settings for the appliance or module are erased. Backup files stored on the appliance are not affected. When restoring the full appliance configuration, at the end of the restore process, the appliance restarts. The appliance is not restarted after restoring a module.

To restore an appliance or module to a saved configuration:

1. Use the **WebsenseAdmin stop** command to stop all software components running off the appliance.

For example, stop Log Server, Sync Service, Linking Service, transparent identification agents, and components on the TRITON management server machine.

- Windows: Navigate to the C:\Program Files *or* Program Files (x86)\Websense\Web Security\ folder.
 - Linux: Navigate to the /opt/Websense/ directory.
2. Open the Appliance manager on the appliance whose configuration you want to restore and go to the **Administration > Backup Utility** page.
 3. Click the **Restore** tab, then select the configuration type that you want to restore from the **Select restore mode** list. Note that when you restore a full appliance configuration:
 - The current appliance version must match the version associated with the backup file. (The appliance version is displayed on the **Restore** tab.) Thus, a version 8.2 backup can be restored only to an appliance that is at version 8.2.
 - The current appliance policy source mode (full policy source, user directory and filtering, or filtering only) must match the policy source mode in effect when the backup file was created.
 - The current appliance mode (Email, Web, or Web and Email) must match that of the backup file. (For example, a backup from an Email-only appliance must be used to restore an Email-only appliance.)
 - The hardware model of the current appliance must be the same as the model that was backed up. (For example, a backup from model V10000 G4 must be used to restore a model V10000 G4 appliance.)
 - The original appliance that was backed up cannot also be running elsewhere in the network. Restoring a full configuration re-creates the original appliance and makes use of unique ID numbers from that appliance.
 4. Click **Run Restore Wizard**. The restore wizard opens.
 5. Select a radio button to indicate where the backup file is stored, and then click **Next**.
 - **This remote machine:** <*host name or IP address*>: Retrieve the file from the default location on the specified machine. The default location is the path specified in the backup schedule for the selected backup type.
 - **This appliance:** Use a backup file that was saved locally.

- **Another location (browse for file):** Use a file saved on any accessible machine in the network.
6. Select or specify the file to use.
 - If you selected the default local or remote backup file location, you are given a list of available backup files to use. Select an entry in the list, and then click **Next**.
 - If you selected another location, browse to the path on the remote machine where the backup file is located, and then click **Next**.
 7. Verify the details on the Confirm page, and then click **Restore Now**. The appliance is restored to the selected configuration.

If you have initiated a full appliance configuration restore, the appliance is restarted during the restore process.
 8. Use the **WebsenseAdmin start** command to start the components that are running off the appliance.
 - Windows: Navigate to the C:\Program Files *or* Program Files (x86)\Websense\Web Security\ folder.
 - Linux: Navigate to the /opt/Websense/ directory.

How do I back up and restore web protection software?

45073 | Backup and Restore | Web Protection Solutions | 18-Apr-2016

Applies to:	TRITON AP-WEB and Web Filter & Security, v8.2.x
--------------------	---

Use the Backup Utility to back up your web protection software settings and policy data, and to revert to a previous configuration.

- [*Running the Backup Utility on Windows or Linux*, page 10](#)
- [*Enabling scheduled backups on Windows servers*, page 12](#)
- [*Configuring how long backup files are stored*, page 13](#)
- [*Restoring your web protection configuration*, page 13](#)
- [*What files does the Backup Utility save?*, page 15](#)

Running the Backup Utility on Windows or Linux

As a best practice, run the backup process on all machines with web protection components within a 30 minute time window. This may include:

- V-Series appliances (see [*How do I back up and restore V-Series appliances?*, page 6](#))
- The TRITON management server

Note that on the management server, you need to run both the Backup Utility for your web protection product, as described in this section, and the backup procedure for the TRITON infrastructure components, as described in [*How do I back up and restore the TRITON infrastructure?*, page 2](#).

- Content Gateway (see [*How do I back up and restore Content Gateway?*, page 17](#))

When restoring a previous configuration, restore all machines using backup files created in the same 30 minute window.

To run the Backup Utility on your Windows or Linux servers (excluding machines that host Content Gateway):

1. Make sure that all administrators are logged off from TRITON Manager.
2. Do one of the following:
 - (Windows) Navigate to the **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin\).
 - (Linux) Navigate to the **bin** directory (/opt/Websense/bin/) and enter the following command:

```
export LD_LIBRARY_PATH=.
```

3. To run an immediate backup, enter the appropriate command for your operating system.

Windows:

```
wsbackup -b -d <directory>
```

Linux:

```
./wsbackup -b -d <directory>
```

Here, *<directory>* indicates a local or remote destination directory for the backup archive.



Warning

Do not store backup files in your product's \bin directory.
This directory is deleted if you uninstall your software.

4. To schedule the backup process to run on a regular basis, use the following command.

■ Windows:

```
wsbackup -s -t "<m> <h> <day_of_month> <month>  
<day_of_week>" -d <directory>
```



Important

There is an additional, important step that must be completed for scheduled backups to be created properly on Windows servers. After completing this procedure, continue with *Enabling scheduled backups on Windows servers*, page 12.

■ Linux:

```
./wsbackup -b -s -t "\<m> <h> <day_of_month> <month>  
<day_of_week>\\" -d <directory>
```

For example, to schedule a backup to run at 10:10 a.m. on Sundays:

```
./wsbackup -s -t "10 10 * * 0"
```

Here, the backup is scheduled to run at 10:10 a.m. on Sundays (regardless of the month or date).

Scheduled backup commands use **crontab** format, and the quotation marks and spaces are required.

In place of the variables shown in the example, provide the following information:

Variable	Information
<m>	0 - 59 Specify the precise minute to start the backup.
<h>	0 - 23 Specify the general hour of the day to start the backup.

Variable	Information
<day_of_month>	1 - 31 Specify the date to perform the backup. If you schedule a backup for days 29 - 31, the utility uses the standard substitution procedure for the operating system in months that do not include that date.
<month>	1 - 12 Specify the month to perform the backup.
<day_of_week>	0 - 6 Specify a day of the week. 0 represents Sunday.

Each field can take a number, an asterisk, or a list of parameters. Refer to any **crontab** reference for details.

After running an immediate backup, or after the scheduled backup process has completed successfully, the **WebsenseBackup.cfg** file is created in the backup directory. Use this file to configure how long backup files are retained. See [Configuring how long backup files are stored, page 13](#).

Enabling scheduled backups on Windows servers

On supported Windows servers, the scheduled task that the Backup Utility creates does not include user account information required by server security settings. This means that the backup file is not saved as expected.

To address this issue, manually update the scheduled task to add the required user account information as follows:

1. Open the Windows Task Scheduler (**Start > Administrative Tools > Task Scheduler** or **Server Manager > Tools > Task Scheduler**).
2. Select **Task Scheduler Library** in the left navigation pane.
3. Right-click the **Websense Backup** task and select **Export**.
4. Save the XML file in a temporary directory, then open the file in a text or XML editor.
5. Update the **<Author>** container with an account with local administrator permissions in the format DOMAIN\UserName. If the backup files will be saved to a remote drive, this must be a domain account, rather than a local account.
`<Author>WBSN-SVR\Administrator</Author>`
6. Update the **<UserId>** container with an account with local administrator permissions in the format DOMAIN\UserName. If the backup files will be saved to a remote drive, this must be a domain account, rather than a local account.
`<UserId>TEST-DOMAIN\NetworkUser</UserId>`
7. Verify that the correct path to the Backup Utility (wsbackup.exe) appears in the **<Command>** container.

8. Verify that the correct destination directory appears in the <Arguments> container. Note that the directory path should have the following format:
 - Local storage:
C:\folder\subfolder
 - Remote storage:
\\"10.102.55.4\BackupDirectory
- For example:
- ```
<Arguments>--backup --dir "C:\WbsnBackup"</Arguments>
```
- Note that there is no backslash at the end of the path.
9. Save and close the file.
  10. In the Task Scheduler, right-click the existing **Websense Backup** task and select **Delete**.
  11. In the right navigation pane, select **Import Task**.
  12. Navigate to the XML file that you edited in the previous steps, select it, and then click **Open**.
  13. To verify that the changes took effect correctly, right-click the new **Websense Backup** task and select **Run**, then make sure that a backup file was created in the expected location.

## Configuring how long backup files are stored

---

After the first backup process has run, optionally use a text editor to edit the **WebsenseBackup.cfg** file, created with the backup archive, as follows:

- Specify a numeric value for the **KeepDays** parameter, which sets the number of days archive files remain in the backup directory (**365**, by default).  
When a file is older than the specified time period, it is deleted automatically.
- Specify a numeric value for the **KeepSize** parameter, which sets the maximum number of bytes allotted for backup files (**10857600**, by default).  
When the backup directory reaches the specified size limit, the oldest backup file is deleted automatically.

## Restoring your web protection configuration

---

When you restore your TRITON AP-WEB or Web Filter & Security configuration, make sure that you are restoring data for the components that exist on the current machine.

If the machine was rebuilt after, for example, a serious hardware failure, make sure that you have installed only the components that previously resided on the machine. The backup process can only restore configuration information for components that were present on the machine when the backup file was created.

Also, remember that cross-platform backup and restore (from Windows to Linux, for example) is not supported.

- When you restore your web protection configuration, also restore a TRITON console configuration from the same time period.
  - Review *Backing up or restoring both web protection components and the TRITON Manager*, page 22, before you begin.
  - See *How do I back up and restore the TRITON infrastructure?*, page 2.
- After restoring the configuration on the Policy Broker machine, restart all web protection services in your deployment.
- Make sure that all services are running after the restore process. Manually start any services that remain stopped.

To restore a previous configuration:

1. Make sure that all administrators are logged off from TRITON Manager.
2. Do one of the following:
  - (Windows) Navigate to the **bin** directory (C:\Program Files or Program Files (x86)\Websense\Web Security\bin\).
  - (Linux) Navigate to the **bin** directory (/opt/Websense/bin/) and enter the following command:

```
export LD_LIBRARY_PATH=.
```
3. Enter the following command to initiate the restore process:  
`wsbackup -r -f archive_file.tar.gz`

---

**Important**

The restore process may take several minutes. Do not stop the process while restoration is underway.

---

The Backup Utility saves some files used for communication with third-party integration products. Because these files reside outside the Forcepoint directory structure, you must restore them manually, by copying each file to the correct directory.

Files that must be restored manually include:

| File name      | Restore to           |
|----------------|----------------------|
| isa_ignore.txt | Windows\system32     |
| ignore.txt     | Windows\system32\bin |

## What files does the Backup Utility save?

---

The Backup Utility identifies and saves any of the following files that it finds on the machine on which it is run.

| Path                                                                                                | File name                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>\Program Files or Program Files (x86)\Websense\Web Security\bin<br/>or<br/>/opt/Websense/bin</b> | authserver.ini<br>BrokerService.cfg<br>config.xml<br>das.ini<br>diagnostics.cfg<br>domains.txt<br>eimserver.ini<br>icap.conf<br>ignore.txt<br>linkingservice.ini<br>LogServer.ini<br>LSPProvider.cfg<br>LSPConsumer.cfg<br>mux.cfg<br>muxplugins.cfg<br>netcache.conf<br>securewispproxy.ini<br>SIEMConsumer.cfg<br>StateServer.cfg<br>syncservice.ini<br>TestRestService.ini<br>transid.ini<br>ufp.conf<br>ufp_sic.conf<br>UsageMonitor.ini<br>websense.ini |
| <b>bin</b> directory (continued)                                                                    | WebUI.ini<br>wsauthserver.ini<br>wscitrix.ini<br>WSE.ini<br>wsendir.ini<br>wsradius.ini<br>WSSEK.DAT<br>wsufpserver.ini                                                                                                                                                                                                                                                                                                                                      |
| <b>bin/i18n</b>                                                                                     | i18n.ini                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>bin/postgres/data</b>                                                                            | pg_hba.conf<br>postgresql.conf                                                                                                                                                                                                                                                                                                                                                                                                                               |

| <b>Path</b>                                          | <b>File name</b>                                            |
|------------------------------------------------------|-------------------------------------------------------------|
| <b>BlockPages/*/Custom</b>                           | All custom block page settings                              |
| Windows: <b>rtm\db\bin\</b>                          | db.properties                                               |
| Windows: <b>rtm\conf\</b>                            | config.properties<br>system.properties                      |
| Windows: <b>rtm\tomcat\conf\</b>                     | catalina.properties                                         |
| Windows: <b>rtm\tomcat\conf\ Catalina\localhost\</b> | rtm.xml                                                     |
| <b>ssdata/pac</b>                                    | websense.pac                                                |
| Windows: <b>tomcat\bin\</b>                          | policyServers.ser                                           |
| Windows: <b>tomcat\conf\</b>                         | catalina.properties<br>wbsn-pairing-map.txt                 |
| Windows: <b>tomcat\conf\ Catalina\Localhost</b>      | mng.xml                                                     |
| Windows: <b>webroot\</b>                             | websense.ini                                                |
| Windows: <b>webroot\Exlorer\</b>                     | favorites.xml<br>websense.ini                               |
| <b>Windows\system32\</b>                             | ignore.txt<br>isa_ignore.txt<br>wsMsp.ini                   |
| Linux: <b>conf/</b>                                  | WebsenseDaemon                                              |
| Linux: <b>conf/restore/</b>                          | local.policybroker.policies<br>remote.policybroker.policies |

# How do I back up and restore Content Gateway?

45074 | Backup and Restore | TRITON AP-WEB | v8.2.x | 18-Apr-2016

The Content Gateway configuration snapshot feature lets you save all current configuration settings and restore them if needed. Content Gateway can store configuration snapshots on the node where they are taken, on an FTP server, and on portable media. Content Gateway restores a configuration snapshot on all the nodes in the cluster.

## Taking Content Gateway configuration snapshots

---

You can save all the current configuration settings on your Content Gateway system through the Content Gateway manager.

### To take a configuration snapshot and save it on the local system

1. Navigate to **Configure > Snapshots > File System**.
2. The **Change Snapshot Directory** field displays the name of the directory where Content Gateway saves configuration snapshots.
  - The default location is the Content Gateway **config/snapshots/** directory.
  - To change the directory, enter the full path in the **Change Snapshot Directory** field.  
If you enter a relative path, Content Gateway assumes that the directory is relative to the **/opt/WCG/config/** directory.
3. In the **Save Snapshot** field, type the name you want to use for the current configuration.
4. Click **Apply**.

### To take a configuration snapshot and save it on an FTP server

1. Navigate to **Configure > Snapshots > FTP Server**.
2. In the fields provided, enter the FTP server name, the login and password, and the remote directory where the FTP server stores configuration snapshots.
3. Click **Apply**.  
After you have successfully logged on to the FTP server, the **FTP Server** page displays additional fields.
4. In the **Save Snapshot to FTP Server** field, enter the name of the configuration snapshot you want to take.
5. Click **Apply**.

# Restoring Content Gateway configuration snapshots

---

If you are running a cluster of Content Gateway servers, the configuration is restored to all the nodes in the cluster.

## To restore a configuration snapshot stored on the local node

1. Navigate to the **Configure > Snapshots > File System** tab.
2. From the **Restore > Delete Snapshot** drop-down list, select the configuration snapshot that you want to restore.
3. Click the **Restore Snapshot from “<directory\_name>” Directory** box.
4. Click **Apply**.

The Content Gateway system or cluster uses the restored configuration.

## To restore a configuration snapshot from an FTP server

1. Navigate to **Configure > Snapshots > FTP Server**.
2. In the fields provided, enter the FTP server name, the login and password, and the remote directory in which the FTP server stores configuration snapshots.
3. Click **Apply**.  
After you have successfully logged on to the FTP server, the **FTP Server** tab displays additional fields.
4. In the **Restore Snapshot** drop-down list, select the configuration snapshot that you want to restore.
5. Click **Apply**.

The Content Gateway system or cluster uses the restored configuration.

# How do I back up and restore TRITON AP-DATA?

45075 | Backup and Restore | TRITON AP-DATA | v8.2.x | 18-Apr-2016

Back up your TRITON AP-DATA system periodically to safeguard your policies, forensics, configuration data, fingerprints, encryption keys, and more.

## Configuring and running the TRITON AP-DATA backup task

---

To configure the TRITON AP-DATA backup process:

1. Log on to TRITON Manager, select the Data module, and go to the **Settings > General > Backup** page.
2. Enter a **Path** for storing backup files and, if necessary, **Credentials** for an account with read, write, and delete privileges to the path. The path must be in UNC format. C: is the default location for storing backups.
3. Enter a value between 1 and 60 in the **How many backup copies do you want to keep?** field to specify how many separate backups to maintain (5, by default).  
Each backup is stored in a separate folder. When the maximum number of copies is reached, TRITON AP-DATA reuses the oldest folder, overwriting the previous information.
4. Indicate whether or not to **include forensics** in the backup.
5. Click **OK** to save the settings.

Schedule backups when the system isn't under significant load. Each backup contains a complete snapshot of the system. The process collects needed information from other TRITON AP-DATA machines.

To schedule the backup task:

1. On the TRITON Management Server, go to **Start > Administrative Tools > Task Scheduler**.
2. In the Task Scheduler window, select **Task Scheduler Library**.
3. Right-click the **Websense TRITON AP-DATA Backup** task and select **Enable**.
4. Right-click **Websense TRITON AP-DATA Backup** again and select **Properties**, then select the **Triggers** tab.
5. Click **Edit**, and edit the schedule as required.
6. Click **OK** twice.

If requested, enter your administrator password for the TRITON Management Server machine to confirm the changes to the task.

To run the task immediately, right-click **Websense TRITON AP-DATA Backup** and select **Run**. Running this task creates a DSSBackup folder and a time stamp folder in

the destination folder you specified. For example: \DSSBackup\2-6-2016-2-10-35-AM, where the numbers stand for the month, day, year, hour, minutes, and seconds.

The DSSBackup folder includes these items:

- \certs: Certificate
- \crawlers: Crawler jobs information
- \forensics\_repository: Forensics
- \MngDB: DSS SQL DB (wbsn-data-security)
- \PreciseID\_DB: Fingerprinting repository + FPNEs
- Backup.text: DSS version
- DataBackup.log: Backup log
- Ep-profile-keys.zip: Endpoint encryption keys (configured in the profile)
- Subscription.xml: License file
- \ResourceRepositoryCache + \ResourceRepositoryCachedXmIs: Cached resources

## Restoring your TRITON AP-DATA configuration

---

1. Make sure all TRITON AP-DATA modules—servers, agents, protectors—are registered with the TRITON management server and the system is operating normally.
2. On the TRITON management server, open the Windows Control Panel and select **Programs > Uninstall a program**.
3. Select TRITON AP-DATA, then click **Uninstall/Change**.
4. When asked if you want to add, remove, or modify TRITON AP-DATA, select **Modify**.
5. Click **Next** until you get to the **Restore Data from Backup** screen.
6. Select the **Load Data From Backup** check box and click the **Browse** button to locate the backup file.
7. Select the **Clear Forensics since last backup** check box if you want to use only the stored forensics from your backup file; this will remove all forensics gained since the last backup. (Leaving it unchecked means that your forensics data after the restore will include the backed-up forensics and the forensics added since that backup.)
8. Click **Next** until you begin the restore procedure.
  - During the restore process, a command-line window appears; it may remain for some time, but it disappears when the recovery is complete.
  - The restore operation completely erases all policies and data (and, if checked, forensics) of the current system, and replaces them with the backed-up data.
9. Complete the restore wizard.

10. To review the restore activity, read the **DataRestore.log** file located in the backup folder (for example, MM-DD-YYYY-HH-MM-SS).
11. Log onto the Data module of TRITON Manager.
12. To enable your crawlers to work with the newest encryption keys, open each discovery, fingerprint, and machine learning task in your system and edit it in some way, even just the description.
  - If you have Box discovery tasks, edit them and enter your Box credentials again.
  - If your fingerprint tasks were configured to be exported to a machine with credentials, edit them and reenter the machine credentials.
13. Select **Deploy**.



**Note**

If the backup system contains many policies, it may take a while to load the policies and deploy them.

---

# How do I back up and restore TRITON AP-EMAIL off-appliance components?

45076 | Backup and Restore | TRITON AP-EMAIL | v8.2.x | 18-Apr-2016

Use the TRITON AP-EMAIL backup and restore feature to safeguard the following configuration settings stored in the Email module of TRITON Manager:

- Database configuration
- The TRITON AP-EMAIL appliances list
- TRITON AP-EMAIL administrator settings
- Presentation report templates and data

The backup and restore function includes a Backup and Restore Log, which displays time-stamped backup and restore activities for the Email module of TRITON Manager. Because the Backup/Restore utility stops the Email manager service, backup and restore activities are recorded only in the Backup and Restore log.

Backup and restore functions for an appliance cluster work properly only when cluster settings have not changed between the backup and restore operations. You may have unexpected results if any of the following settings have been changed between the backup and restore.

- Appliance mode (cluster or standalone)
- IP address or hostname

You may need to rebuild a cluster if a restore operation encounters problems. The backup settings file size may not exceed 10 MB.



## Note

If you specify your backup file location for a remote server, ensure that your restore operation is configured to restore configuration files from that remote server location.

## Running the TRITON AP-EMAIL backup or restore process

To backup the current configuration:

1. Log on to the Email module of TRITON Manager and go to the **Settings > General > Backup/Restore** page.
2. Click **Backup** to activate the utility, then specify a local folder for the backup file. That folder location appears in the File Location field in the Restore Settings section of the page.
3. If you want to save your backup settings on the Log Database server, mark the corresponding check box.

When you make this selection, the Remote Log Database Server Access box is enabled for you to enter the following server information:

- **Domain/Host name.** Enter the domain if a domain account is used; otherwise, enter the hostname of the SQL Server machine.
- **User name.** Enter a user with SQL Server log-in permission.
- **Password.** The password may not contain more than 1 double quotation mark.
- **Backup/Restore file path.** Enter the shared folder path on the remote SQL Server machine (for example, \\10.1.1.2\shared\).

The version of the backed up settings must match the version of the currently installed product.

Click **Check Status** to ensure that the remote log database server is accessible.

To restore an existing configuration:

1. Go to the **Settings > General > Backup/Restore** page.
2. Click **Restore**.
3. Specify the backup file to use.

After the restore process is complete, TRITON AP-EMAIL restarts automatically.

# How do I back up or restore web protection components and the TRITON Manager?

45077 | Backup and Restore | Web Protection Solutions | 18-Apr-2016

|                    |                                                 |
|--------------------|-------------------------------------------------|
| <b>Applies to:</b> | TRITON AP-WEB and Web Filter & Security, v8.2.x |
|--------------------|-------------------------------------------------|

When you are getting ready to restore an existing TRITON infrastructure or web protection configuration from backup, keep the following points in mind:

- When you restore a previous TRITON infrastructure configuration, use a web protection backup file created in the same time period to restore configuration information for your web protection components.
- If you are restoring both management and web protection components, do not restart the management components (listed below) until after the web protection component restore process is complete.
- Before restoring a previous web protection configuration (for example, on the Policy Broker machine or full policy source appliance), stop the following TRITON Manager and reporting services:
  - Websense TRITON Unified Security Center
  - Websense TRITON Web Server
  - Websense TRITON - Web Security
  - Websense Web Reporting Tools
  - Websense RTM Server
  - Websense RTM Database
  - Websense RTM Client
- Before restoring a TRITON infrastructure configuration, stop the following services:
  - Websense TRITON Unified Security Center
  - Websense TRITON Web Server
  - Websense TRITON - Web Security
- If administrators receive a browser 404 error when they attempt to log on to the TRITON Manager after a restore process is complete, use the Windows Services tool to restart the **Websense TRITON Unified Security Center** service.

# How do I back up or restore multiple TRITON AP-WEB appliances?

45078 | Backup and Restore | TRITON AP-WEB | v8.2.x | 18-Apr-2016

As a best practice, synchronize the backup process to back up all components (on and off-appliance) at approximately the same time (within a 30-minute window).

During the restore process, use backup files from the same time period to revert all components on all machines (on and off-appliance) to an earlier configuration.

## Performing backup and restore procedures when the policy source is a V-Series appliance

---

If the deployment includes an appliance configured as a **Full policy source**, complete the following steps to do a full system backup:

1. Before you begin, make sure that all components on and off the policy source appliance are working as expected. Restart services, if needed.
2. Back up each V-Series appliance in the following order:
  - a. Full policy source
  - b. Filtering and user identification
  - c. Filtering onlyUse the Appliance manager to run an immediate backup or schedule backups at regular intervals. See [Running the appliance backup utility, page 6](#).
3. Use the Backup Utility to back up all off-appliance (software only) components. You can either run an immediate backup, or schedule backups to coincide with appliance scheduled backups. See [Running the Backup Utility on Windows or Linux, page 10](#).

After completing this process, you have a time-compatible set of backups on all machines hosting TRITON/web/data/email protection components in the network.

To restore a previous configuration:

1. Stop all off-appliance (software only) components.
2. Restore the appliances the following order:
  - a. Full policy source
  - b. Filtering and user identification
  - c. Filtering only

See [Restoring your appliance configuration, page 8](#).



### Important

Make sure you select time-compatible backup files for the restore process.

3. Use the Backup Utility to restore your web protection configuration on each non-appliance machine. See [Restoring your web protection configuration, page 13](#).  
The off-box web protection services or daemons may need to be restarted manually.
4. Log on to the Appliance manager for each appliance to verify that all services are running correctly.
5. Log on to the Web module of TRITON Manager and confirm that there are no alert messages indicating stopped services.

## Performing backup and restore procedures when the policy source is not a V-Series appliance

If the deployment uses a non-appliance policy source (a software installation of Policy Broker and Policy Server), complete the following steps to do a full system backup:

1. Before you begin, make sure that all appliance and off-box components are running normally. Restart services, if needed.
2. Use the Backup Utility to back up the policy source (Policy Broker) machine. See [Running the Backup Utility on Windows or Linux, page 10](#).  
The utility can be used to schedule regular backups to coincide with appliance backups, or to initiate the backup process manually.
3. Back up each V-Series appliance in the following order:
  - a. Full policy source
  - b. Filtering and user identification
  - c. Filtering onlyUse the Appliance manager to initiate the backup process. See [Running the appliance backup utility, page 6](#).
4. Use the Backup Utility to back up any other off-appliance components (not running on the policy source machine).

After completing this process, you have a time-compatible set of backups on all machines hosting TRITON/web/data/email protection components in the network.

To restore a previous configuration:

1. Stop all off-appliance (software-only) components, including those on the policy source (Policy Broker) machine.

2. Use the Backup Utility to restore the configuration on the policy source (Policy Broker) machine. See [Restoring your web protection configuration, page 13](#).

If necessary, restart the Websense services or daemons on the machine.

3. Restore the appliances the following order:

- a. Full policy source
- b. Filtering and user identification
- c. Filtering only

See [Restoring your appliance configuration, page 8](#).



#### Important

Make sure you select time-compatible backup files for the restore process.

4. Use the Backup Utility to restore the configuration of all other off-appliance components. If necessary, restart the web protection services or daemons manually.
5. Log on to the Appliance manager for each appliance to verify that all services are running correctly.
6. Log on to the Web module of TRITON Manager and confirm that there are no alert messages indicating stopped services.

