Data, Email, and Web Security

v8.5.x

Backup and Restore FAQ

Revision A

Contents

Introduction

Regularly back up configuration information for Forcepoint web, data, and email security solutions. This provides protection in case of a serious system failure, and makes it possible to revert to a previous configuration when needed. Data saved by the backup process can also be used to transfer configuration settings to a different server or appliance.

In most circumstances, the backup and restore process can be used to transfer configuration settings only between servers with the same operating system. In other words, it is possible move from Windows to Windows or Linux to Linux, but not from Windows to Linux (or vice versa).

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

How do I back up and restore the Forcepoint management infrastructure?

The Forcepoint Infrastructure backup process saves:

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

When you either initiate an immediate backup (see *Running immediate infrastructure backups*) or define a backup schedule (see *Scheduling management 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 Forcepoint management 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 Forcepoint Security Manager before you back up or restore your configuration.

Related tasks

Running immediate infrastructure backups on page 4
Scheduling management infrastructure backups on page 3

Related reference

Changing backup settings on page 5

Scheduling management infrastructure backups

Before you begin

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

Notify Security Manager administrators of the backup schedule, so that they can be sure to log off of the Security 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:

Steps

1) On the Forcepoint management server machine, open the Windows 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 management server machine to confirm the changes to the task.

Running immediate infrastructure backups

Before running a manual backup, make sure that all administrators are logged off of the Forcepoint Security Manager.

To launch an immediate backup:

Steps

1) On the Forcepoint 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 infrastructure backup data

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

To restore management infrastructure data:

Steps

1) On the Forcepoint 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 *How do I back up or restore web protection components and the Forcepoint Security Manager?*.)
3) Open the Windows Control Panel and select **Programs** > **Programs and Features**, then select Forcepoint Management Infrastructure.
4) Click **Uninstall/Change**.
5) When asked if you want to modify, repair, or remove the Management 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**.

Next steps

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.

Related concepts

How do I back up or restore web protection components and the Forcepoint Security Manager? on page 23

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 Forcepoint management server, go to the directory where you installed the Forcepoint Security Manager (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>.
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>.

Parameter	Description
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. The path can either reside on the local machine or another machine in the network. For example:

```
<PATH>D:\mgmt\Backups</PATH>
```

```
<PATH>\\hostname_or_IP_address\mgmt\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 Forcepoint appliances?

Local backups are limited to 20. The oldest backup will be replaced with the newest when the limit of 20 is reached.

Two types of backup are available on Forcepoint appliances:

- A **full appliance configuration** backup saves the appliance controller and all installed modules. Forcepoint 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 configuration information for the selected module (Web or Email).
  - This includes any client and policy data stored on the selected appliance.
  - Web module backups include only data in the Web container. Neither the Network Agent or Content Gateway modules are included.
    Separate Content Gateway backups can be performed in the Content Gateway manager. See *How do I back up and restore Content Gateway?*.

    To include all modules, perform a full appliance backup.

Important

Backups can be restored *only* on Forcepoint appliances of the same type and version. Thus, a V10000 G4, version 8.4 backup can be restored only on a V10000 G4, version 8.4 appliance. For complete details, see *Restoring your appliance configuration*.

Note

- Backups can also be performed and restored via the Forcepoint Security Appliance Manager (FSAM).
- Refer to the latest Forcepoint Appliances CLI Guide for more information about the CLI and the most current updates to CLI commands.

Related concepts

How do I back up and restore Content Gateway? on page 17

Related tasks

Restoring your appliance configuration on page 8

Running the appliance backup utility

Steps

1) Log on to the appliance command-line interface (CLI) and elevate to **config** mode.

2) To perform an immediate backup, use:

```
create backup now
--location <local|filestore_alias>
[--desc <description>]
--type <full|email|web>
--save-path <filepath>
[--url <url>]
[--auth-required]
```

local places the backup file on the appliance.

filestore_alias places the backup in the remote storage location defined by filestore_alias. For information about defining a filestore_alias, see the *Forcepoint Appliances CLI Guide*.

3) To create scheduled backups use the following command:

```
create backup schedule
--type <full|web|email>
--location <local|filestore_alias>
--freq <daily|weekly|monthly>
--day <Mon|Tue|Wed|Thu|Fri|Sat|Sun>
--date <integer>
--time <hh:mm>
```

Important

To create backup files for multiple appliances on the same remote machine, use a separate directory for each appliance's backup files. This makes it easier to locate the backup file for a specific appliance and avoids the possibility of conflicts that could lead to files being mistakenly overwritten or deleted.

Restoring your appliance configuration

Before you begin

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 the restore completes, the appliance automatically restarts.

To restore an appliance or module to a saved configuration:

Steps

1) Stop all software components running off the appliance (including management components, Log Server, and transparent identification agents).
   - Windows: Navigate to the `C:\Program Files` *or* `Program Files (x86)\Websense\Web Security\folder` and enter the following command:
     `WebsenseAdmin stop`
   - Linux: Navigate to the `/opt/Websense/` directory and enter the following command:
     `./WebsenseAdmin stop`

2) In the appliance CLI, use the following command to restore a backup file:

```
restore backup
[--location <local|filestore_alias>]
[--file <file_name>]
[--url <backup_url>]
[--auth-required]
[--nocert-verification]
```

To see a list of available backup files, enter:

```
show backup list --location <local|filestore_alias>
```

When you restore a full appliance configuration:

- The current appliance version must match the version associated with the backup file. Thus, a version 8.5 backup can be restored only on an appliance that is at version 8.5.
- 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.
- The current appliance mode (Forcepoint Email Security, Forcepoint Web Security, or Forcepoint URL Filtering) must match that of the backup file. For example, a backup from an email appliance must be used to restore an email appliance.
- 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.
  User directory and filtering and **Filtering only** appliances must have retained the same policy-source IP address that was captured in the backup.
- 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.

3) Start the components that are running off the appliance.

- Windows: Navigate to the `C:\Program Files` *or* `Program Files (x86)\Websense\Web Security\ folder` and enter the following command:
  `WebsenseAdmin start`
- Linux: Navigate to the /opt/Websense/ directory and enter the following command:
  `./WebsenseAdmin start`

How do I back up and restore web protection software?

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

Related concepts

Running the Backup Utility on Windows or Linux on page 10
Configuring how long backup files are stored on page 14
Restoring your web protection configuration on page 14

Related tasks
Enabling scheduled backups on Windows servers on page 13

Related reference
What files does the Backup Utility save? on page 16

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:

- Forcepoint appliances (see *How do I back up and restore Forcepoint appliances?*)
- The Forcepoint 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 management infrastructure components, as described in *How do I back up and restore the Forcepoint management infrastructure?*.
- Content Gateway (see *How do I back up and restore Content Gateway?*)
  When restoring a previous configuration, restore all machines using backup files created in the same 30-minute window.

Related concepts
How do I back up and restore Forcepoint appliances? on page 6
How do I back up and restore the Forcepoint management infrastructure? on page 2
How do I back up and restore Content Gateway? on page 17

Procedure to run the Backup Utility on your Windows or Linux servers

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

Steps

1) Make sure that all administrators are logged off of the Forcepoint Security 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*.

- 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.
<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.

Next steps

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 retailed. See *Configuring how long backup files are stored*.

Related concepts

Configuring how long backup files are stored on page 14

Related tasks
Enabling scheduled backups on Windows servers on page 13

Enabling scheduled backups on Windows servers

Before you begin

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:

Steps

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>FP-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 Forcepoint Web Security or Forcepoint URL Filtering 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 Forcepoint Security Manager configuration from the same time period.
  - Review *How do I back up or restore web protection components and the Forcepoint Security Manager?*, before you begin.

- See *How do I back up and restore the Forcepoint management infrastructure?*.

- 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.

Related concepts

How do I back up or restore web protection components and the Forcepoint Security Manager? on page 23
How do I back up and restore the Forcepoint management infrastructure? on page 2

Procedure to restore a previous configuration

Steps

1) Make sure that all administrators are logged off of the Forcepoint Security 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_name>.tar.gz`

   Important

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

Next steps

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 names	

`\Program Files` or `Program Files (x86)\Websense\Web Security\ bin`
or
`/opt/Websense/bin`
	authserver.ini
	BrokerService.cfg
	config.xml
	das.ini
	diagnostics.cfg
	domains.txt
	eimserver.ini
	icap.conf
	ignore.txt
	linkingservice.ini
	LogServer.ini
	LSPProvider.cfg
	LSPConsumer.cfg
	mux.cfg
	muxplugins.cfg
	netcache.conf
	securewispproxy.ini
		SIEMConsumer.cfg
		StateServer.cfg
		syncservice.ini
		TestRestService.ini
		transid.ini
		ufp.conf
		ufp_sic.conf
		UsageMonitor.ini
		websense.ini
		WebUI.ini
		wsauthserver.ini
		wscitrix.ini
		WSE.ini
		wsedir.ini
		wsradius.ini
		WSSEK.DAT
		wsufpserver.ini

`bin/i18n`	i18n.ini	
`bin/postgres/data`	pg_hba.conf postgresql.conf	
`BlockPages/*/Custom`	All custom block page files	
`ssdata/pac`	websense.pac	
Windows only		
`rtm\db\bin\`	db.properties	
`rtm\conf\`	config.properties system.properties	
`rtm\tomcat\conf\`	catalina.properties	
`rtm\tomcat\conf\Catalina\localhost\`	rtm.xml	
`tomcat\bin\`	policyServers.ser	
`tomcat\conf\`	catalina.properties wbsn-pairing-map.txt	
`tomcat\conf\Catalina\Localhost`	mng.xml	
`webroot\`	websense.ini	
`webroot\Exlorer\`	favorites.xml websense.ini	

Path	File names
`Windows\system32\`	ignore.txt isa_ignore.txt wsMsp.ini
Linux only	
`conf/`	WebsenseDaemon
`conf/restore/`	local.policybroker.policies remote.policybroker.policies

How do I back up and restore Content Gateway?

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

Steps

1) In the Content Gateway manager, go to the **Configure** > **Snapshots** > **File System** tab.

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

Steps

1) Go to the **Configure** > **Snapshots** > **FTP Server** page.

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

Steps

1) Go 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...** box.

4) Click **Apply**.
   The Content Gateway system or cluster uses the restored configuration.

To restore a configuration snapshot from an FTP server

Steps

1) Navigate to the **Configure** > **Snapshots** > **FTP Server** tab.

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 Forcepoint DLP?

Back up your Forcepoint DLP system periodically to safeguard your policies, forensics, configuration data, fingerprints, encryption keys, and more.

Configuring and running the Forcepoint DLP backup task

To configure the Forcepoint DLP backup process:

Steps

1) Log on to the Forcepoint Security Manager and go to the **Data** > **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, Forcepoint DLP 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.

Next steps

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 Forcepoint DLP machines.

To schedule the backup task

Steps

1) On the Forcepoint management server, open the Windows 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 a management server administrator password to confirm the changes to the task.

Next steps

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 + \ResourceRepositoryCachedXmls: Cached resources

Restoring your Forcepoint DLP configuration

Steps

1) Make sure all Forcepoint DLP modules—servers, agents, protectors—are registered with the Forcepoint management server and the system is operating normally.

2) On the management server, open the Windows Control Panel and select **Programs** > **Uninstall a program**.

3) Select Forcepoint DLP, then click **Uninstall/Change**.

4) When asked if you want to add, remove, or modify Forcepoint DLP, select **Modify**.

5) Click **Next** until you get to the **Restore Data from Backup** screen.

Note

Backups must be enabled in order to restore a backup from another DLP management server. See the DLP installation guide for instructions.

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 Security module of the Forcepoint Security 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 Forcepoint Email Security off-appliance components?

Use the Forcepoint Email Security backup and restore feature to safeguard the following configuration settings stored in the Email Security module of the Forcepoint Security Manager:

- Database configuration
- The Forcepoint Email Security appliances list
- Forcepoint Email Security 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 Security module of the Security Manager. Because the Backup/Restore utility stops the Email Security management services, 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 Forcepoint Email Security backup or restore process

To backup the current configuration:

Steps

1) Log on to the Email Security module of the Forcepoint Security 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.

   Backup and restore settings must both use either local or remote file storage. You cannot restore a local file using remote settings.

   The following special characters are not supported in backup server entries: |, <, >, and &. Click **Check Status** to ensure that the remote log database server is accessible.

To restore an existing configuration

Steps

1) Go to the **Settings** > **General** > **Backup/Restore** page.

2) Click **Restore**.

3) Specify the backup file to use.

Next steps

After the restore process is complete, Forcepoint Email Security restarts automatically.

How do I back up or restore web protection components and the Forcepoint Security Manager?

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

- When you restore a previous management 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 Forcepoint Security 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 management 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 Security 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 Forcepoint Web Security appliances?

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 Forcepoint appliance

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

Steps

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 Forcepoint appliance in the following order:
   a) Full policy source
   b) User directory and filtering
   c) Filtering only

   Use the appliance CLI to run an immediate backup or schedule backups at regular intervals. See *Running the appliance backup utility*.

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*.

Next steps

After completing this process, you have a time-compatible set of backups on all machines hosting Forcepoint Web, Data, and Email protection components in the network.

Related concepts
Running the Backup Utility on Windows or Linux on page 10

Related tasks
Running the appliance backup utility on page 7

To restore a previous configuration

Steps

1) Stop all off-appliance (software only) components.

2) Restore the appliances the following order:
   a) Full policy source
   b) User directory and filtering
   c) Filtering only

   See *Restoring your appliance configuration*.

   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*.

   The off-box web protection services or daemons may need to be restarted manually.

4) Log on to the CLI for each appliance to verify that all services are running correctly.

5) Log on to the Web Security module of the Forcepoint Security Manager and confirm that there are no alert messages indicating stopped services.

Related concepts
Restoring your web protection configuration on page 14

Related tasks
Restoring your appliance configuration on page 8

Performing backup and restore procedures when the policy source is not a Forcepoint 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:

Steps

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*.

   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 Forcepoint appliance in the following order:

   a) Full policy source

   b) User directory and filtering

   c) Filtering only

   Use the appliance CLI to initiate the backup process. See *Running the appliance backup utility*.

4) Use the Backup Utility to back up any other off-appliance components (not running on the policy source machine).

Next steps

After completing this process, you have a time-compatible set of backups on all machines hosting Forcepoint Web, Data, and Email protection components in the network.

Related concepts
Running the Backup Utility on Windows or Linux on page 10

Related tasks
Running the appliance backup utility on page 7

To restore a previous configuration

Steps

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*.

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

3) Restore the appliances the following order:

   a) Full policy source

   b) User directory and filtering

   c) Filtering only

   See *Restoring your appliance configuration*.

   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 CLI for each appliance to verify that all services are running correctly.

6) Log on to the Web Security module of Forcepoint Security Manager and confirm that there are no alert messages indicating stopped services.

Related concepts
Restoring your web protection configuration on page 14

Related tasks
Restoring your appliance configuration on page 8

Published 03 November 2023