Incremental Upgrade Guide

Incremental Upgrade Guide | Web Protecton Solutions | v8.5.x | 29-Apr-2022

The upgrade process for Forcepoint™ Web Security and Forcepoint™ URL Filtering allows you to upgrade your deployment incrementally, over a period of days or weeks, rather than requiring all machines and components to be upgraded simultaneously. Your deployment will continue to function normally as it is upgraded over a period of time. Policy enforcement, Internet activity logging, and reporting continues as the incremental upgrade progresses.

Note, however, that once the incremental upgrade process has started, there are specific limitations that affect the way your software functions, until all machines and components have been upgraded. These include:

- Once the upgrade process has been started, you are not allowed to add new components to your configuration until the full upgrade has been completed.
- After the primary Policy Broker is upgraded, no data synchronization occurs to any replica Policy Brokers that have not also been upgraded.
- When accessing the Forcepoint Security Manager, you can connect only to Policy Server instances whose version is supported by the Security Manager. In addition, the Control Service instance on the Policy Server machine must be running.
- If the database has been upgraded but investigative reports has not, you need to connect to an older database. Until that happens, investigative report scheduled jobs may fail.
- As the incremental upgrade proceeds, "not running" Health Alerts may appear on the System dashboard for services that are not yet upgraded, even though the service is actually running. The Alert is triggered by a version mismatch and clears as soon as that component is upgraded.

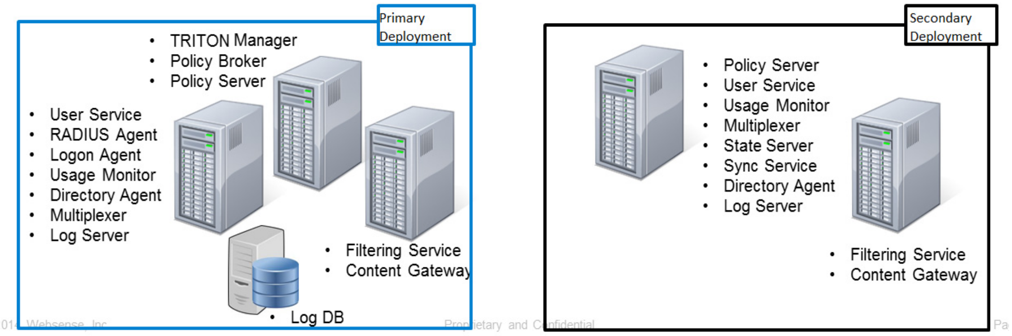
See *Limitations & restrictions* for a list of important details.

Important

A security update done for the v8.5.4 product release has resulted in a new requirement for a specific dynamic-link library (dll) when installing or upgrading to v8.5.4 or v8.5.5 on a Windows platform.

See the Install Guide for details.

The incremental upgrade process is based on the ability to upgrade one “logical deployment” at a time. Each logical deployment is made up of a Policy Server instance and all components that rely on it.



Potential SIEM data loss for upgrades to v8.5.4 or v8.5.5

SIEM Integration feature enhancements may result in the loss of SIEM data during an incremental upgrade to v8.5.4 or v8.5.5. Note that there is no loss of reporting log data during an incremental upgrade.

Follow these steps if you plan to upgrade incrementally and are concerned with SIEM data loss.

1. SIEM Integration must first be configured for all Policy Servers in your deployment. Use Forcepoint Security Manager to enable and configure SIEM Integration for any Policy Servers for which SIEM is not currently configured.

   The current SIEM feature was designed to send data for each Policy Servers assigned to the same Policy Broker to all SIEM solutions configured for those Policy Servers. This step is required to avoid losing data for a Policy Server not specifically configured for SIEM.

2. Download Forcepoint_Web_Security_854_Pre_Upgrade_Tool.zip from the v8.5.4 Downloads page, unzip it, and locate the package appropriate for the Forcepoint Web Security version you are upgrading from.

Note

When upgrading to v8.5.5:

- From 8.5.3, use the appropriate v8.5.4 package. For example, if the upgrade is on Windows, use Web_Security_854_Pre_Upgrade_from_853_Windows.zip.
- From 8.5.4, no additional steps are required. The same v8.5.4 functionality is included in v8.5.5.

- ReadMe.txt
- Web_Security_854_Pre_Upgrade_from_840_Windows.zip

- Web_Security_854_Pre_Upgrade_from_850_Windows.zip
- Web_Security_854_Pre_Upgrade_from_853_Windows.zip
- Web_Security_854_Pre_Upgrade_from_840_Linux.tar.gz
- Web_Security_854_Pre_Upgrade_from_850_Linux.tar.gz
- Web_Security_854_Pre_Upgrade_from_853_Linux.tar.gz
- Web_Security_854_Pre_Upgrade_from_840_Appliance.rpm
- Web_Security_854_Pre_Upgrade_from_850_Appliance.rpm
- Web_Security_854_Pre_Upgrade_from_853_Appliance.rpm

3. Copy the appropriate zip file to each machine on which a Policy Server is installed.
4. Follow the instructions in the ReadMe to run the script on each machine.

   This process will reset the SIEM Integration functionality back to the pre-v8.4 functionality, when the SIEM Integration process was initially enhanced.

   Note that pre-8.4 functionality did not support:

   - Forwarding hybrid log data to a SIEM Integration.
   - Cloud application log data for use in cloud app reports.
   - The following keys as part of a customized SIEM format string:
     - loginID
     - logRecordSource (added for Hybrid data).
     - cloudAppName (added for cloud app data).
     - cloudAppID (added for cloud app data).
     - cloudAppRiskLevel (added for cloud app data).
     - cloudAppType (added for cloud app data).
   - Forwarding data to multiple SIEM solutions.

   Once the flag is re-set, data will be forwarded only to the SIEM Integration configured for that Policy Server.
5. Start the incremental upgrade process, beginning with Policy Broker. Follow the instructions in *Steps for upgrading incrementally*.
6. When each Policy Server is upgraded, the reset will be reversed and the new v8.5.4 functionality will be enabled. See Forcepoint Security Information Event Management (SIEM) Solutions.

Requirements

The following requirements must be met for the incremental upgrade process to work correctly and not impact the functioning deployment.

1. To perform an incremental upgrade to v8.5, all components in your deployment must be at v8.1 or later.

   To perform an incremental upgrade to v8.5.3, all components in your deployment must be at v8.2 or later.

To perform an incremental upgrade to v8.5.4, all components in your deployment must be at v8.4 or later.

To perform an incremental upgrade to v8.5.5, all components in your deployment must be at v8.5.3 or later.

2. Back up your current deployment, including the Log Database, before you begin the upgrade process.
3. Stop all Log Servers and **stop all Log Database jobs**. This is to avoid any problems during the database upgrade.

   The Log Database upgrade occurs when the first Log Server instance is upgraded. During the upgrade process, the Log Database version is checked. If the database has not yet been updated, the upgrade will attempt to stop any jobs that are still running. Any jobs that cannot be stopped need to be stopped manually.

   When the database update is complete, the upgrade process attempts to re-start all Log Database jobs. Any Log Database jobs that were not automatically restarted and all Log Server instances can be restarted.
4. Upgrade the primary Policy Broker machine first.
5. In distributed Log Server deployments, upgrade the central Log Server first. This allows logging to continue uninterrupted. Log data sent from the remote Log Server instances continues to be processed.

   If your configuration is set up so that a remote Log Server is upgraded first, cache files sent to the central Log Server may not be in a recognized format and, therefore, not sent to the Log Database. To avoid interrupting the logging process, before upgrading the remote Log Server, do one of the following:

   a. If the central Log Server has not been upgraded, configure each remote Log Server to be a standalone Log Server (which sends log data directly to the Log Database).

      Set up the distributed environment after the central Log Server is upgraded.

   b. During the upgrade process, configure all Filtering Service instances to send log data to a Log Server with the same or newer version.

   Note

   A Log Server that has been upgraded can receive and log data from a Filtering Service that has NOT been upgraded. A Log Server that has not been upgraded, however, cannot receive log data from an upgraded Filtering Service. Be sure to upgrade Log Server if an associated Filtering Service is upgraded.

   Although distributed logging continues to be supported, note that, after all Log Servers have been upgraded, each can now be directly connected to the Log Database. Support of multiple Log Servers all connected to the same database is offered.
6. Once the upgrade of the primary logical deployment has started, the upgrade process for that logical deployment must be completed prior to making any changes that would impact the Policy Database.

> For example, after upgrading the primary Policy Broker and primary Policy Server, do not run the Management API to create new categories or make policy changes prior to upgrading the management server machine and Log Server.

All components on a machine are upgraded at the same time. You cannot select specific components for upgrade.

Steps for upgrading incrementally

Follow these steps to complete the upgrade.

1. To prepare for upgrade:
   a. Back up your existing deployment, especially the Policy Broker machine and the Log Database.
   b. To upgrade to v8.5, first upgrade to v8.1.x, v8.2.x, v8.3.x, or v8.4.x. (if necessary)

      To upgrade to v8.5.3, first upgrade to v8.2.x, v8.3.x, v8.4.x, or v8.5. (if necessary)

      To upgrade to v8.5.4, first upgrade to v8.4.x, or 8.5.x. (if necessary0);

      To upgrade to v8.5.5, first upgrade to v8.5.3 or 8.5.4 (if necessary).
   c. Stop all Log Server instances and Log Database jobs.
   d. Identify the primary logical deployment.
2. Upgrade the primary Policy Broker

   All other web protection components on the primary Policy Broker machine are upgraded automatically.
3. After the primary Policy Broker has been upgraded, continue by upgrading the logical deployment that uses the primary Policy Broker. Follow these steps to complete the upgrade of the primary logical deployment.
   a. Restart services on each machine before starting the upgrade.

      Before upgrading any Policy Server, reboot the machine. If you are using a Forcepoint Appliance, do a full restart of the appliance.
   b. Upgrade the Policy Server machine first.
   c. Upgrade machines with Filtering Service, Network Agent, and User Service components associated with this Policy Server.
   d. Upgrade Log Server. You can then restart any other Log Servers that were previously stopped. (If using a distributed Log Server environment, please see the Requirement #5 above.)
   e. Restart Log Database jobs.
   f. Upgrade the management server machine.
   g. Upgrade other machines where any additional components are installed.
4. As time permits, continue by upgrading each logical deployment. All components in a logical deployment should be upgraded at the same time.

   Follow these steps as needed to upgrade each logical deployment. Note that a replica Policy Broker must be upgraded before all Policy Server instances connected to it.
   a. Restart services on each machine before starting the upgrade
   b. Upgrade the Policy Broker machine first.
   c. Upgrade Policy Server (if it resides on a different machine than Policy Broker).

d. Upgrade machines with Filtering Service, Network Agent, and User Service components associated with this Policy Server.

e. Upgrade Log Server.

f. Upgrade other machines where any additional components are installed.

Optionally, replica Policy Brokers running on a dedicated machine (with no other web protection components installed) can be upgraded prior to the remaining logical deployments. This allows data synchronization between the primary and replica instances.

Note that this deployment model is not typical, because a Policy Server instance is typically installed with each Policy Broker instance. (See *Limitations & restrictions* below.)

Limitations & restrictions

Once the incremental upgrade process has started, there are specific limitations that impact the way your software functions until all upgrades have been completed.

- Once the upgrade process has been started, you will not be allowed to add new components to your configuration until the full upgrade has been completed.
- After the primary Policy Broker is upgraded:
  - No data synchronization occurs to any replica Policy Brokers that have not also been upgraded. Replica Policy Brokers whose version does not match are not allowed to synchronize policy and configuration data. When viewed on the **Installed Policy Broker Instances** table, the **Last Policy Sync** column will display an “out of sync” message for any replica Policy Broker that has not been upgraded.
  - If the mode of a replica Policy Broker that has not been upgraded is changed to either standalone or primary mode, any attempt to change the mode back to replica will fail.
  - If the primary Policy Broker is on a machine by itself, any web protection components connected to it may have switched to a secondary Policy Broker when the primary was being upgraded. You must restart those components to re-connect to the upgraded primary Policy Broker.

    To restart components on Windows or Linux servers, run the following command from the C:\Program Files\Websense\Web Security\ or /opt/Websense/ directory:

    ```
    WebsenseAdmin restart
    ```

    On appliances, restart the Forcepoint Web Security or Forcepoint URL Filtering, Content Gateway (if applicable), and Network Agent modules. See the Forcepoint Appliances CLI Guide.
- When accessing the Forcepoint Security Manager, you can only connect to Policy Server instances whose version is supported by the Security Manager.

  The supported versions are:

- 8.1 (upgrades to v8.5 only)
- 8.2 (not supported for upgrades to v8.5.4 or v8.5.5)
- 8.3 (not supported for upgrades to v8.5.4 or v8.5.5)
- 8.4 (not supported for upgrades to v8.5.5)
- 8.5 (upgrades to v8.5.3 or v8.5.4 only)
- 8.5.3 (upgrades to v8.5.4 or v8.5.5)
- 8.5.4 (upgrades to v8.5.5)

In addition, the Control Service instance on the Policy Server machine must be running.

Important

Forcepoint Security Manager must have been upgraded to v8.5.x to support the connection to Policy Servers with earlier versions.

- Automatic logon to a secondary Policy Server occurs if any of the following is true:
  - The primary Policy Server version is not supported.
  - The primary Policy Server is unreachable.
  - The Control Service on the primary Policy Server machine is not running.

  Logon will fail if any of the following is true:
  - Control Service on the management server is not running.
  - Policy Server is a supported version but unreachable and there is no reachable secondary Policy Server with a supported version.
  - The Policy Server version is not supported and there is no reachable secondary Policy Server with a supported version.
  - Control Service is not running on the Policy Server machine box and there is no reachable secondary Policy Server with a supported version.
  - The Control Service on the secondary Policy Server machine is not running.
- When logged on to the Forcepoint Web Security module of the Forcepoint Security Manager,
  - Help, Find Answers information, field labels, and error messages are based on the version of the Forcepoint Security Manager, even when the connection is to a Policy Server with a different version.
  - Some of the pages of the Security Manager may not be accessible if the Policy Server and Security Manager versions do not match.
  - In multiple Policy Server environments, use the information on the Policy Server Map on the **Status** > **Deployment** page to view the version of the primary Policy Server and associated secondary Policy Servers.
  - Health Alerts may appear indicating that services that have not been upgraded are not running. The service is running; the alert is triggered by the version mismatch.

- The **Status** > **Dashboard** page, presentation reports, and application reports will display a notification message if the Forcepoint Security Manager version does not match the Log Database version. The Log Database is upgraded when Log Server is upgraded.
- If a Policy Server version is not supported by the Security Manager or, if the Policy Server or the Control Service on the Policy Server machine is not running:
  - Switching to that Policy Server is not allowed.
  - Adding or editing that Policy Server is not allowed.
- If a secondary Policy Server with a supported version is added or edited but the version does not match the primary Policy Server, Directory Services settings cannot be inherited.

  If the **Inherit from the primary Policy Server** option has been checked but the versions don’t match, the Directory Services settings for the secondary Policy Server are left available for entry. When it can be determined that the Policy Server versions match, the Directory settings are copied from the primary Policy Server to the secondary, and the settings for the secondary Policy Server are disabled.

  In the Forcepoint Security Manager, use the Policy Server Map on the **Status** > **Deployment** page to view the version of each Policy Server
- If the version of the Log Database (upgraded when Log Server is upgraded) does not match the version of the various reporting tools:
  - Emails sent by presentation reports scheduled jobs will include specific text indicating that the versions are different.
  - Access to investigative reports is allowed, but may require entering a new Log Database connection in the **Investigative Reports** > **Options** page.

    If the database has been upgraded but investigative reports has not, you will need to connect to an older database. Until that happens, investigative report scheduled jobs may fail.

    Note that if the investigative reports tool has been upgraded, but the Log Database has not, the connection to the database will not require a change and scheduled jobs should run as expected.
  - WebCatcher will not run and an appropriate message is added to the webcatcher.log file.
  - Use of the **Import Sample Data** option for Threats dashboard data on the **Settings** > **Reporting** > **Dashboard** page is not supported.
  - You can set up connections to a Log Database with the same version or a more recent version than the Log Server version on the **Settings** > **Reporting** > **Log Server** page. This can be used in distributed Log Server environments for Log Servers that have not yet been upgraded.
- As a best practice, for upgrades from v8.1, if a Policy Server has been upgraded, avoid adding a policy exception that includes Referer sites. Policy Servers and Filtering Services that have not been upgraded will permit general access to the sites in the URL list.

- Beginning with v8.4, data for each Policy Server (including those without a SIEM solution) is sent to all SIEM solutions configured for other Policy Servers assigned to the same Policy Broker.

  For upgrades from v8.3 (or earlier) to v8.4, v8.5, or v8.5.3:

  - If, in the earlier deployment, SIEM solutions have been configured for different Policy Servers under the same Policy Broker, an upgraded Policy Server will receive SIEM data from all Policy Servers under that Policy Broker.
  - To allow this feature to work correctly after upgrade in multiple Policy Server environments, stop all Event Message Brokers (located with each Policy Server) after the primary Policy Broker has been upgraded. As each Policy Server is then upgraded, Event Message Broker will be upgraded and restarted. During this process, some SIEM data will not be sent until the upgrade is complete.

  Upgrades to v8.5.4 or v8.5.5 will continue to use the SIEM solution configurations from the earlier version. SIEM enhancements in v8.5.4 removed the sharing of SIEM data between Policy Servers.