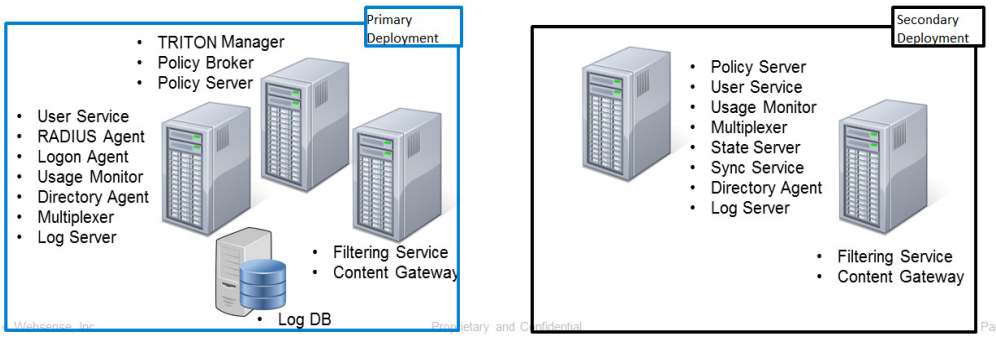
Incremental Upgrade

The upgrade process for TRITON AP-WEB and Web Filter & Security allows you to upgrade your deployment incrementally, over a period of days or weeks. Your deployment will continue to function while it is upgraded over a period of time. Policy enforcement, logging, and reporting will continue as the upgrade progresses.

Note, however, that once the incremental upgrade process has started, there are specific limitations that affect the way your software will function, 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 will occur to any replica Policy Brokers that have not also been upgraded.
- When accessing the management console, you can connect only to Policy Server instances that have the same version as the management console. 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 will need to connect to an older database. Until that happens, investigative report scheduled jobs may fail. See *Limitations & restrictions* for a list of important 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.



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 v8.0.0, all components in your deployment must be at v7.8.3 or v7.8.4.
2. If upgrading from v7.8.3, install **Hotfix 90 (Incremental Upgrade Support)** on:
   a. All Log Server machines
   b. The TRITON management server
3. Back up your current deployment, including the Log Database, before you begin the upgrade process.
4. 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. After that, all Log Server instances and Log Database jobs can be restarted.

   When you are upgrading from 7.8.3 or earlier, a new logging partition is added to your Log Database. Please make sure you do not have 70 active partitions (the limit) prior to upgrading. If you have more 70 active partitions, you will be prompted to select one or more partitions to be disabled.
5. Upgrade the primary Policy Broker machine first.
6. In distributed Log Server deployments, upgrade the central Log Server first. This will allow logging to continue uninterrupted. Log data sent from the remote Log Server instances will continue 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 (sends data directly to 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.

   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. Upgrade to v7.8.3 or v7.8.4 (if necessary)
   c. If upgrading from v7.8.3, install **Hotfix 90 (Incremental Upgrade Support)** on the TRITON management server and all Log Server machines.
   d. Stop all Log Server instances and Log Database jobs.
   e. Identify the primary logical deployment.
2. Upgrade the primary Policy Broker

   All other TRITON 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.
   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 #6 above.)
   e. Restart Log Database jobs.
   f. Upgrade the TRITON 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 Websense 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 will function until all components and machines have been upgraded.

- 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 will occur to any replica Policy Brokers that have not also been upgraded. Replica Policy Brokers whose version does not match will not be 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 Websense 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 Websense appliances, restart the TRITON AP-WEB or Web Filter & Security, Content Gateway (if applicable), and Network Agent modules from the Appliance manager.
- When accessing the management console, you can only connect to Policy Server instances that have the same version as the management console. In addition, the Control Service instance on the Policy Server machine must be running.

  Automatic logon to a secondary Policy Server occurs if any of the following is true:
  - The primary Policy Server is the wrong version.
  - 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 the correct version but unreachable and there is no reachable secondary Policy Server with the correct version.
- Policy Server is the wrong version and there is no reachable secondary Policy Server with the correct version.
- Control Service is not running on the Policy Server machine box and there is no reachable secondary Policy Server with the correct version.
- The Control Service on the secondary Policy Server machine is not running.

- The Status > Dashboard page, presentation reports, and application reports will display a notification message if the management console version does not match the Log Database version. The Log Database is upgraded when Log Server is upgraded.
- If a Policy Server version does not match the management console version 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 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 will be 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.