Managing Policy Broker Replication

Policy Broker Replication | Web Protection Solutions | v8.4, v8.5.x | 29-Apr-2022

Policy Broker is responsible for managing access to both policy data (including clients, filters, and exceptions) and global settings for web protection solutions.

You have the option to deploy Policy Broker in either a standalone or replicated configuration.

- In a **standalone** configuration, there is one Policy Broker for the entire deployment.
- In a **replicated** configuration, there is one **primary** Policy Broker, to which configuration and policy changes are saved, and one or more **replica** instances, each with their own read-only copy of the configuration and policy data.
  - The primary Policy Broker and all replica instances must reside on a Windows or Linux server. When you enable replication, Policy Broker cannot reside on an appliance.
  - If one Policy Broker instance becomes unavailable, components can connect to another instance, allowing database downloads, policy enforcement, and reporting to continue without interruption.
  - In geographically distributed deployments, having components retrieve information from a local Policy Broker may improve performance.

Important

A replicated environment requires bidirectional communication on port **6432** between the primary Policy Broker and each of its replicas. Make sure that your firewalls are configured to allow this communication.

You can configure how each Policy Server instance in your deployment connects to Policy Broker, including:

- Whether Policy Server attempts to connect to the primary Policy Broker or a replica Policy Broker at startup.
- How Policy Server attempts to connect to a new Policy Broker if it loses its connection to its default Policy Broker.

For each Policy Server, you can manage a Policy Broker connection list. If Policy Server cannot connect to the first Policy Broker in the list, it attempts to connect to the second, then the third, and so on, until it establishes a successful connection.

By default, Policy Server attempts to connect to the Policy Broker instance on the same machine (if one exists) first. This is true when Policy Server is installed:

- At the same time as Policy Broker
- On a machine that already hosts a Policy Broker

If Policy Broker is installed on a machine that already hosts a Policy Server instance, the Policy Server is not automatically updated to attempt to connect to the new Policy Broker first.

Manage Policy Broker connection lists on the **Web > Settings > General > Policy Brokers** page in the Forcepoint Security Manager.

Refer to the articles in this collection for information about how to:

- *Change the Policy Broker mode*, page 2
- *Update replica instances after the primary is restored from backup*, page 4
- *Configure Policy Server to connect to a new primary or standalone Policy Broker*, page 5
- *Reconfigure Policy Server after a standalone Policy Broker becomes a replica*, page 7

Also find tips about:

- *Backup and restore for the primary Policy Broker*, page 9
- *Backup and restore for replica instances*, page 9
- *Changing from replicated to standalone mode*, page 10
- *Remote Filtering Server and Policy Broker replication*, page 11

Change the Policy Broker mode

Policy Broker Replication | Web Protection Solutions | v8.4, v8.5.x | 29-Apr-2022

In some instances, it may become necessary to change the mode of a Policy Broker instance after installation. For example:

- A deployment uses a single Policy Broker in standalone mode, and the organization wants to switch to a replicated environment.

> **Note**
> Policy Broker must reside on Windows or Linux servers, and not on appliances, to enable replication.

- The machine hosting the primary Policy Broker has failed and is not immediately recoverable, so administrators want to transform a replica instance into the new primary.
- An organization decides that a replicated environment is no longer necessary, and wants to switch the primary Policy Broker to standalone mode and uninstall the replica instances.

To make the change, an administrator must use the **PgSetup** command from the command line on the Policy Broker machine as follows:

> **Note**
> Before changing the mode from replica to standalone or primary, make sure that no one is logged onto the Forcepoint Security Manager.

1. Stop all components connected to the Policy Broker instance whose mode you plan to change.
   - Windows: Open a command prompt and navigate to the **Web Security** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\), then enter the following command:

     ```
     WebsenseAdmin stop
     ```
   - Linux: Navigate to the **/opt/Websense/** directory and enter the following command:

     ```
     ./WebsenseAdmin stop
     ```
   - Appliance: Stop all web protection modules (for example, Network Agent and Content Gateway).
2. Navigate to the **bin** directory on the Policy Broker machine (/opt/Websense/bin/ or C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin).
3. If you are on a Linux server, enter the following command:

   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/Websense/bin
   ```
4. Enter one of the following commands:
   - To change a Policy Broker from primary or replica to standalone mode:

     ```
     PgSetup -m standalone
     ```

     Make a note of the **token** that is displayed when the mode switch is complete. You will need this to update your Policy Server configuration later.
   - To change a Policy Broker to primary mode:

     ```
     PgSetup -m primary -w <synchronization_password>
     ```

     All replicas must use this synchronization password to connect to the primary and receive updated policy and configuration data.

     Make a note of the **token** that is displayed when the mode switch is complete. You will need this to update your Policy Server configuration later.
   - To change a Policy Broker to replica mode:

```
PgSetup -m replica -l <replica_IP_address> -z
<primary_IP address> -w <synchronization_password>
```

The replica IP address is the IP address that the primary instance will use to communicate updated policy and configuration information to the replica. The synchronization password must match the one created when the primary Policy Broker was configured.

Note

If changing a Policy Broker from replica mode to primary mode fails, first change from replica to standalone mode and then from standalone to primary mode.

5. After making the change:
   - If you have promoted a replica Policy Broker to a primary instance, see *Configure Policy Server to connect to a new primary or standalone Policy Broker*, page 5.
   - If you have changed a standalone Policy Broker to a replica, see *Reconfigure Policy Server after a standalone Policy Broker becomes a replica*, page 7.
6. To complete the process, restart your web protection services (starting with the Policy Broker machines, then any additional Policy Server machines, then any additional machines with web protection components). Using the commands below ensures that components on each machine are restarted in the correct order.
   - Linux: Run the following command from the /opt/Websense/ directory:

     ```
     ./WebsenseAdmin restart
     ```
   - Windows: Run the following command from the C:\Program Files *or* Program Files (x86)\Websense\Web Security\ folder:

     ```
     WebsenseAdmin restart
     ```
   - Appliance: Start all web protection modules (for example, Network Agent and Content Gateway).

Update replica instances after the primary is restored from backup

Policy Broker Replication | Web Protection Solutions | v8.4, v8.5.x | 29-Apr-2022

Replica Policy Broker instances verify that they are synchronized to the latest version of the data from the primary Policy Broker by checking sequence numbers.

When you restore an older version of the Policy Database to the primary Policy Broker instance, replica instances do not recognize that they need to synchronize their data, because the sequence number is out of date. One symptom of the problem is that the **Web > Settings > General > Policy Brokers** page in the Forcepoint Security Manager will show a Last Policy Sync value of **Unknown**.

If you encounter this issue, perform the following steps for each replica Policy Broker:

1. On the replica Policy Broker machine, open a command shell and navigate to the **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/).
2. If you are on a Linux server, enter the following command:

   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/Websense/bin
   ```

3. Enter the following command:

   ```
   PgSetup -m standalone
   ```

   This temporarily disconnects the replica from the primary Policy Broker.

   You will see a prompt about manually updating config.xml files. You can ignore the prompt, because Policy Broker will become a replica again in the next step.

4. Enter the following command:

   ```
   PgSetup -m replica -l <replica_IP_address> -z <primary_IP
   address> -w <synchronization_password>
   ```

   This reconnects the replica to its primary Policy Broker.

5. After making the change, restart your web protection services (starting with the Policy Broker machines, then any additional Policy Server machines, then any additional machines with web protection components). Using the commands below ensures that components on each machine are restarted in the correct order.
   - Linux: Run the following command from the /opt/Websense/ directory:

     ```
     ./WebsenseAdmin restart
     ```

   - Windows: Run the following command from the C:\Program Files *or* Program Files (x86)Program Files *or* Program Files (x86)\Websense\Web Security\ folder:

     ```
     WebsenseAdmin restart
     ```

   - Appliance: Restart all web protection modules (for example, Network Agent and Content Gateway).

Configure Policy Server to connect to a new primary or standalone Policy Broker

Policy Broker Replication | Web Protection Solutions | v8.4, v8.5.x | 29-Apr-2022

When you configure a Policy Server instance to point to a new primary or standalone Policy Broker instance (for example, after a hardware failure or after changing the mode of an existing Policy Broker), you must edit the **config.xml** file for that Policy Server to reflect the new Policy Broker connection.

Note that if Policy Server resides on an appliance, Technical Support will need to assist with the process of updating the **config.xml** file.

To update the **config.xml** file for a Policy Server instance on a Windows or Linux server:

1. Stop the Policy Server instance.

- Linux: Use the /opt/Websense/WebsenseDaemonControl command to stop Policy Server.
- Windows: Use the Services tool to stop Policy Server.

2. Navigate to the **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/) and make a backup copy of **config.xml** in another location.
3. Open the original **config.xml** file in a text editor and navigate to the **BrokerService** container:

   ```
   <container name="BrokerService">
   ```

4. Delete the entire **Brokers** container within the **BrokerService** container. The Brokers container looks something like this:

   ```
   <container name="Brokers">
      <container name="0">
         <data name="Host">10.226.56.62</data>
         <data name="Port">55880</data>
         <data name="Priority">1</data>
      </container>
      <container name="1">
         <data name="Host">10.226.56.63</data>
         <data name="Port">55880</data>
         <data name="Priority">2</data>
      </container>
   </container>
   ```

5. If a primary Policy Broker has been changed to **standalone** mode, repeat steps 1 through 4 for each Policy Server that should no longer point to that Policy Broker.
6. Locate the **Config** container within the **BrokerService** container and update the **Host** container with the new Policy Broker IP address:

   ```
   <container name="Config">
      <data name="Country">US</data>
      <data name="Host">10.226.56.62</data>
   ```

7. Still in the **Config** container, update the **Token** field with the new Policy Broker token value that you recorded when you changed the Policy Broker mode.

   The token looks something like this, and must be entered as a single line (no line breaks):

   ```
   <data name="Token">0542A478BC2AB7773AE226F8471E4DD12E7AB7
   8DEFF21A3A151621EFBF5A98559211A5746D4263F00797190AFD30A5F
   D507DD5560362F6C5538C780F350C5467E106DC6A1D46FF2670FC1348
   331640AA95D0ADDAD8999D491137C8C9ED831846599BF6C99242D512B
   FABA28938E3CA975197AFED65CD335BC738E1BE933B48F7816C8F51D4
   0AEE8B9C4F401815FAD21BD427175DBD1B06B28465CC20C41AD452DE2
   B7798A71CF17E</data>
   ```

8. Save and close the **config.xml** file.
9. After making the change, restart the web module services on the Policy Server machine.
   - Linux: Run the following command from the /opt/Websense/ directory:

     ```
     ./WebsenseAdmin restart
     ```

- Windows: Run the following command from the C:\Program Files *or* Program Files (x86)\Websense\Web Security\ folder:

  ```
  WebsenseAdmin restart
  ```

Reconfigure Policy Server after a standalone Policy Broker becomes a replica

Policy Broker Replication | Web Protection Solutions | v8.4, v8.5.x | 29-Apr-2022

When a standalone Policy Broker is converted to a replica, you must update the **config.xml** file for each Policy Server instance that connected to the standalone Policy Broker. The update adds information about the primary Policy Broker for the deployment.

Note that if Policy Server resides on an appliance, Technical Support will need to assist with the process of updating the **config.xml** file.

Step 1: Collect required information

First, identify a Policy Server that is already configured to connect to the primary Policy Broker (for example, the Policy Server instance on the Policy Broker machine).

On the machine that hosts the Policy Server you identified:

1. Navigate to the **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/) and make a backup copy of the **config.xml** file in another location.
2. Open the original **config.xml** file in a text editor and navigate to the **BrokerService** container:

   ```
   <container name="BrokerService">
   ```

3. Locate the **Config** container and **Token** container within the **BrokerService** container.

   The Config container looks something like this:

   ```
   <container name="Config">
      <data name="Country">US</data>
      <data name="Host">10.226.56.62</data>
   ```

   The Token container looks something like this:

   ```
   <data name="Token">0542A478BC2AB7773AE226F8471E4DD12E7AB7
   8DEFF21A3A151621EFBF5A98559211A5746D4263F00797190AFD30A5F
   D507DD5560362F6C5538C780F350C5467E106DC6A1D46FF2670FC1348
   331640AA95D0ADDAD8999D491137C8C9ED831846599BF6C99242D512B
   FABA28938E3CA975197AFED65CD335BC738E1BE933B48F7816C8F51D4
   0AEE8B9C4F401815FAD21BD427175DBD1B06B28465CC20C41AD452DE2
   B7798A71CF17E</data>
   ```

4. Make a copy of the contents of the each of these containers in a new text file.

This information will need to be added or copied to the **config.xml** file for each Policy Server that is being reconfigured.

5. Close the **config.xml** file.

Step 2: Update Policy Server configuration

Reconfigure each Policy Server instance that was originally set up to connect to the former standalone Policy Broker (now a replica).

1. Stop the Policy Server instance.
   - Linux: Use the opt/Websense/**WebsenseDaemonControl** command to stop **Policy Server**.
   - Windows: Use the Services tool to stop **Websense Policy Server**.
2. Navigate to the **bin** directory (C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/) and make a backup copy of **config.xml** in another location.
3. Open the original **config.xml** file in a text editor and navigate to the **BrokerService** container:

   ```
   <container name="BrokerService">
   ```

4. If a **Brokers** container exists, delete it. A Brokers container looks something like this:

   ```
   <container name="Brokers">
      <container name="0">
         <data name="Host">10.226.56.62</data>
         <data name="Port">55880</data>
         <data name="Priority">1</data>
      </container>
      <container name="1">
         <data name="Host">10.226.56.63</data>
         <data name="Port">55880</data>
         <data name="Priority">2</data>
      </container>
   </container>
   ```

5. Locate the **Config** container within the **BrokerService** container and update the **Host** container with the Policy Broker IP address copied in the previous procedure. For example:

   ```
   <container name="Config">
      <data name="Country">US</data>
      <data name="Host">10.226.56.62</data>
   ```

   Still in the **Config** container, update the **Token** field with the Policy Broker token value copied in the previous procedure. The token looks something like this, and must be entered as a single line (no line breaks):

   ```
   <data name="Token">0542A478BC2AB7773AE226F8471E4DD12E7AB7
   8DEFF21A3A151621EFBF5A98559211A5746D4263F00797190AFD30A5F
   D507DD5560362F6C5538C780F350C5467E106DC6A1D46FF2670FC1348
   ```

```
331640AA95D0ADDAD8999D491137C8C9ED831846599BF6C99242D512B
FABA28938E3CA975197AFED65CD335BC738E1BE933B48F7816C8F51D4
0AEE8B9C4F401815FAD21BD427175DBD1B06B28465CC20C41AD452DE2
B7798A71CF17E</data>
```

6. Save and close the **config.xml** file.
7. Delete the **config.xml.bak** file from the **bin** directory.
8. After making the change, restart the web module services on the Policy Server machine.
   - Linux: Run the following command from the /opt/Websense/ directory:
     ```
     ./WebsenseAdmin restart
     ```
   - Windows: Run the following command from the C:\Program Files *or* Program Files (x86)\Websense\Web Security\ folder:
     ```
     WebsenseAdmin restart
     ```

Replication tips

Policy Broker Replication | Web Protection Solutions | v8.4, v8.5.x | 29-Apr-2022

Backup and restore for the primary Policy Broker

As a best practice, perform regular backups of the primary Policy Broker so that you can revert to a previous configuration if needed.

In order to ensure that the restore process goes as smoothly as possible, perform a backup:

- Any time you change the password for **admin**, the default administrator.
- Any time you add or remove a replica Policy Broker from your deployment.

This helps to minimize errors and lessen the need for post-restore reconfiguration, should you have to restore configuration for your primary Policy Broker.

Backup and restore for replica instances

Because replica Policy Broker instances host a read-only copy of the data stored in the primary Policy Database, you do not need to back up your replica Policy Broker instances.

Should the replica Policy Database become corrupted, the simplest way to get back to a working database is to uninstall and reinstall the replica.

If the installer returns an “unable to uninstall” error for the replica, try changing the replica to standalone mode (see *Change the Policy Broker mode*, page 2), then change back to replica mode.

When the reinstalled or reconfigured replica connects to the primary Policy Broker instance, it will receive the latest policy and configuration data in its synchronized copy of the Policy Database.

Changing from replicated to standalone mode

If you reconfigure your primary Policy Broker to become a standalone Policy Broker, be sure to remove all replica Policy Broker instances from your network.

If there are still replica instances running in your network after you change to standalone mode:

- The replica Policy Database instances are not updated.
- Policy Server instances configured to connect to a replica Policy Broker continue to connect to the replica, meaning that Policy Server and its associated components receive outdated information.

If you are unable to immediately remove the replica Policy Broker instances after changing to standalone mode, on each affected Policy Server machine:

1. Stop the Policy Server instance.
   - Linux: Use the opt/Websense/**WebsenseDaemonControl** command to stop **Policy Server**.
   - Windows: Use the Services tool to stop **Websense Policy Server**.
2. Navigate to the **bin** directory (/opt/Websense/bin or C:\Program Files *or* Program Files (x86)\Websense\Web Security\bin) and make a backup copy of **config.xml** in another location.
3. Open the original **config.xml** file in a text editor and navigate to the **Brokers** container. For example:

```
<container name="Brokers">
   <container name="0">
      <data name="Host">10.226.56.62</data>
      <data name="Port">55880</data>
      <data name="Priority">1</data>
   </container>
   <container name="1">
      <data name="Host">10.226.56.63</data>
      <data name="Port">55880</data>
      <data name="Priority">2</data>
   </container>
</container>
```

4. Delete the entire **Brokers** container.
5. Save and close the file.
6. Delete the **config.xml.bak** file from the **bin** directory.
7. Restart the web protection services on the Policy Server machine.

Remote Filtering Server and Policy Broker replication

Unlike other components, Remote Filtering Server (available to Forcepoint URL Filtering customers who purchase the Remote Filter Module) does not use the Policy Server connection list to determine its Policy Broker connection order. Instead, Remote Filtering Server always connects to the primary Policy Broker.

If the primary Policy Broker becomes unavailable, however, Remote Filtering Server continues to function normally:

- There is only one setting that Remote Filtering Server retrieves from Policy Broker: whether to fail open or fail closed if Remote Filtering Client cannot connect to Remote Filtering Server.
- If Remote Filtering Server cannot retrieve the setting from Policy Broker, it uses the default option (fail open).