This document provides information on how to deploy the BigFix custom connector.

With the BigFix custom connector, you can use CA Privileged Access Manager to view and update passwords for BigFix Console operator accounts.

# Prerequisites

The following conditions must be satisfied in order to use the BigFix custom connector:

* Privileged Access Manager must be running version 3.3 or later.
* Install the Custom Connector Server. For installation instructions, see the CA Privileged Access Manager documentation.
* The target account must be defined as a BigFix Console operator with the **Can use REST API** and the **Custom Content** permissions set to **YES** in its definition or in one of the assigned roles.



* Obtain the SSL certificate from BigFix Server.

# Deploy the BigFix Target Connector

Follow these steps:

1. On the Tomcat Custom Connector Server, copy the **bigfix.war** file to the **webapps\_targetconnectors** directory.

# Specify a Remote Target Server

Follow these steps:

1. Log in the CA Privileged Access Manager UI.
2. In the UI, select **Devices**, **Manage Devices**.
3. From the Devices page, select **ADD**.
4. In the Add Device dialog, complete the required fields in the Basic Info tab.
5. For the **Device Type**, select the **Password Management** checkbox. Keep the Access checkbox selected.
6. Go to the **Access Methods** tab and specify an access protocol, such as SSH. The appliance uses the access method to contact the remote target server.
7. Select **SAVE AND ADD TARGET APPLICATIONS** to complete the configuration.

# Add the BigFix Target Connector Application

Follow these steps:

1. Select or enter values for the **Application Name** field.
2. In the **Application Type** field, select **BigFix**.



1. A new tab labelled **BigFix** is displayed.
2. On the **BigFix** tab, specify values for the following fields:
* **Server Port**: Specify the port that the BigFix Server listens on. Default: 52311.
* **Base 64 encoded x.509 Certificate**: Specify the SSL certificate for the BigFix Server.
* **Hostname Verification**: Select this box to enable hostname verification when connecting to BigFix Server.



1. Select **OK**.

# Add the Target Account

Follow these steps:

1. Select **Credentials**, **Manage Targets**, **Accounts**.
2. Select **ADD**.
3. Complete the required fields:
* **Host Name**: Enter or specify the remote target server you defined.
* **Device Name**: Enter the name for the target server you added.
* **Application Name**: Select the BigFix application name that you configured in the previous procedure.
* **Password**: The password of the user account at the remote target server.



1. On the **Password** tab, select **Update both the Password Authority Server and the target system**.



1. On the **BigFix** tab, specify values for the following fields:
* **Master Account**: Specify whether to use the existing target account or an alternative account to change the password.



1. Select **OK** to save the account.