BigFix
WebUI Administrators Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page 85)*.

Edition notice

This edition applies to version 9.5 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

This guide is intended for BigFix Master Operators and those who administer an BigFix deployment. If you are looking for information about using the WebUI, see the BigFix WebUI User's Guide.

The WebUI harnesses the flexibility and power of BigFix. It augments the BigFix Console, but does not replace it. Many WebUI administration tasks are completed using the BigFix Console.

WebUI Audience

The WebUI might not be suitable for all BigFix deployments, and is not currently as scalable as a traditional BigFix deployment. Currently, the WebUI has the following upper use limits:

- Microsoft Windows
  - 250,000 managed endpoints.
  - 36 concurrent users.
- Red Hat Enterprise Linux
  - 250,000 managed endpoints.
  - 36 concurrent users.

While nothing prevents the use of the WebUI in larger deployments, there might be significant impact to performance. For more information, see Performance *(on page 60)*.

Chapter 2. Deployment Requirements

This guide contains information and procedures for installing the WebUI on BigFix Platform V9.5.5 or later. The WebUI is supported on BigFix Platform V9.5.5 and later versions.

Prepare your environment before you deploy the WebUI.

Before installing the WebUI service:

- Install BigFix Platform V9.5.5 or later. For instructions, see the BigFix Installation Guide.
- Install BigFix client on the same computer.
- BigFix Web Reports must be installed, running, and reachable via the REST API. If that prerequisite is not met, the WebUI will not be able to load some WebUI sites and applications such as Query and Profile, and Patch Policies or services like the Send Notification will not be available. Even when the BigFix Web Reports is installed on a remote server, and the datasource configured after the WebUI was started, these applications will not be available until the WebUI server is restarted.
- Make sure that your DBA grants the database user to be used for the WebUI installation:
    - Read access to all of the DBO tables in BFENT (DB2), BFEnterprise (MS SQL Server).
    - The ability to create stored procedures.
    - The ability to create new indexes in the WebUI namespace.
    - The ability to create new tables in the WebUI namespace.
- To use the Send Notification service:
    - BigFix Web Reports must be installed, running, and reachable via the REST API.
    - The notification service must be installed on the BigFix root server, not on a remote machine.
- If you are installing the WebUI service on a remote server:

    - The remote server must be running the BigFix Agent version 9.5.5 or later before you deploy the installation Fixlet.
    - The BigFix root server and the WebUI remote server must run on the same operating system family (either Windows or Red Hat); operating system versions can differ. The supported operating systems are:
        - Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019, or
        - Red Hat Linux 7 or 8 (64 bit).

    Note: Starting from the May 2021 WebUI update, WebUI no longer supports the Windows Server 2008 R2 and Red Hat Linux 6 operating systems.

- HTTP cookies must be enabled to use the WebUI. Users who have browser cookies disabled or blocked will not be able to log in. No warning or error message will appear.
- A network port must be open for WebUI communication; the default port is 80 and 443 for HTTP and HTTPS. For more information, see Network Port Conflicts *(on page 5)*.
- Certificate authority (CA) signed SSL certificates ensure secure communication with your WebUI deployment. For more information, see Configure SSL certificates *(on page 14)*.
- Access the WebUI with these supported internet browsers. You need a minimum screen resolution of 1024x768.
    - Microsoft Edge
    - Firefox, updated to the latest version.
    - Safari, updated to the latest version.
    - Chrome, updated to the latest version.

System requirements for using BigFix Query:

- BigFix version 9.5 Patch 2.
- Web Reports enabled in your environment.
- A license for BigFix Lifecycle, or BigFix Security and Compliance.

- To process BigFix Query requests, targeted clients must have:
  - The ability to receive UDP notifications.
  - BigFix V9.5 Patch 2 or later installed.
- BigFix V9.5 Patch 2 or later must be installed on all targeted clients and intermediate relays.

Hardware Requirements

Additional hardware resources are required to power the WebUI. Baseline hardware requirements for an BigFix deployment are described in the *BigFix Installation Guide*. Capacity planning for the WebUI depends on many factors, including number of endpoints, workload, time of day, server location, and the number of concurrent users. For best practices and recommendations to improve WebUI performance, see the *BigFix Capacity Planning Guide*, which provides configuration recommendations for the database server, operating system, and hypervisor.

Table 1. Hardware Recommendations for WebUI

Component	Additional CPU	Additional Memory (GB)	Additional Storage (GB)
BigFix WebUI	+2 per 10 concurrent users	+2 per 10 concurrent users	15% of BigFix database

Starting with BigFix Platform V9.5.5, a database cache is implemented for several counters to improve WebUI response times. The time-based cache has a default refresh interval of 10 minutes.

More about the WebUI Server from the *BigFix Capacity Planning Guide*:

The BigFix WebUI offers a scalable and highly responsive management interface. There have been a number of iterations of the WebUI server. If you are running an older version an upgrade to the most recent version is strongly recommended. Significant improvements have been delivered providing improved scale, function, and user experience.

- Hardware recommendations are in addition to BigFix root server requirements.
- If an anti-collocated instance is deployed (meaning an instance not deployed on the root server), the CPU requirements should be split across the database and WebUI servers, and the storage should be added to the database server.
- In terms of recommended scalability limits, both the Windows and Linux WebUI instances support 36 concurrent users on a 250k deployment base. Once again, these are highly active concurrent users per the previously provided capacity planning definitions.
- Concurrent users would typically be non-master operators, managing a subset of the estate.
- It is possible to manage at a larger scale based on user operations, infrastructure capability, etc. However, the stated bounds should be considered a good *"rule of thumb"* for the scale of the solution.

Network Port Conflicts

BigFix WebUI is set to communicate on network ports 80 (HTTP), and 443 (HTTPS), by default. These ports can be set to any value during WebUI enablement. It is critical that the chosen ports remain open and that no other applications use them. If you notice the WebUI failing to redirect from HTTP to HTTPS on WebUI login, or other odd WebUI behavior, check for port conflicts. Use the netstat command to check your running services.

- Linux: `netstat –l`
- Windows: `netstat -an`

If you find a conflict there are several ways to address the problem.

- Change where the WebUI is running. Adjust the network ports of essential WebUI services on the box. The client settings are:
  - _WebUI_HTTPS_Port (default: 443)
  - _WebUI_Redirect_Port (default: 80)
  - _WebUIAppEnv_APP_PORT (default 5000)
  - _WebUIAppEnv_APP_PORT_MIN (default 5001)
  - _WebUIAppEnv_APP_PORT_MAX (default 5999)
- Turn off the conflicting network services. Examples of competing services include:
  - SQL Server Reporting Services (ReportServer)
  - Web Deployment Agent Service (MsDepSvc)
  - BranchCache (PeerDistSvc)
  - Sync Share Service (SyncShareSvc)
  - World Wide Web Publishing Service (W3SVC)
  - Internet Information Server (WAS, IISADMIN)
  - SolarWinds Agent
  - Nutanix Guest

For more details on the WebUI Server settings, see Server Settings Definitions *(on page 66)*.

WebUI and Web Report Conflicts

A conflict can arise between the WebUI and BigFix Web Reports. In Platform version 9.2.4 and earlier, Web Reports defaults to port 80. As of Platform V9.2.5, Web Reports defaults to port 8080, to avoid conflict with WebUI. When upgrading an existing deployment to 9.2.5 or later, the port used for Web Reports is not changed, so it's possible to run a fully updated deployment and still encounter a port conflict.

During WebUI installation, any port conflict with Web Reports is detected and the option to change the Web Reports port is provided. For more information, see Change Communication Ports.

Chapter 3. WebUI Installation

Use these procedures to install or upgrade the WebUI on BigFix Platform versions 9.5.5, or later. Before you start the procedure:

- Review the WebUI deployment *(on page 2)* and hardware *(on page 4)* requirements, and verify that your environment is ready.
- Complete the BigFix Platform installation to V9.5.5 or later. For more information, see the BigFix Installation Guide.

Select the appropriate option for your environment.

- Use the WebUI Installation *(on page 8)* procedure to install the WebUI for the first time.
- Use the DB Schema Upgrade *(on page 13)* procedure to enable an existing WebUI installation to use Microsoft SQL Server (Windows systems), or IBM DB2 (Red Hat Enterprise Linux (RHEL) systems).

For information on using the WebUI in SAML-Only mode, see SAML 2.0 *(on page 72)*.

Installation Procedure

Use this procedure to install the WebUI on BigFix Platform versions 9.5.5, or later.

The WebUI Installation Fixlets default to SQL Server on Windows systems and DB2 on Red Hat Enterprise Linux systems.

Note: This task only installs the WebUI service, which will then automatically install and configure the rest of the WebUI. After this task is completed, you need to wait for the WebUI service to complete several post-installation operations before you can actually use the WebUI.

Before you start:

- Review the WebUI deployment *(on page 2)* and hardware *(on page 4)* requirements, and verify that your environment is ready. For example, if the database account permissions are not correct, the WebUI will not start correctly.
- Complete the BigFix Platform installation to V9.5.5 or later. For more information, see the BigFix Installation Guide.

1. On the BES Support site, locate the Install BigFix WebUI Service Fixlet that is relevant for your root server version. For example, if you are running Platform V9.5.5, use the Fixlet **Install BigFix WebUI Service (Version 9.5.5)**.
2. Have the host name or IP address of server where the WebUI will be installed ready.
    - The default installation directories for the WebUI are:
        - On Windows systems:

          ```
          C:\Program Files (x86)\BigFix Enterprise\BES WebUI
          ```

        - On RHEL systems:

          ```
          /var/opt/BESWebUI and /opt/BESWebUI
          ```

3. If you are not using the defaults, have the WebUI target drive and directory ready.
    - On Windows systems, the specified targets are created automatically.
    - On Red Hat Linux systems:
        a. Create the target directory.
        b. Symlink the default directory to the target directory.
4. The WebUI needs to connect directly to the BigFix Server database. If your BigFix Server uses a remote database, the WebUI will connect to that database as well. Routine database credential changes can cause the WebUI initialization to fail, so the account used to access the WebUI database should be used exclusively for that purpose.

    Note: If you change the account password after installing the WebUI, run the Deploy/Update WebUI Database Configuration Fixlet. The same Fixlet can also be used to repair a credential-based initialization failure.

5. If you are using SQL Server:

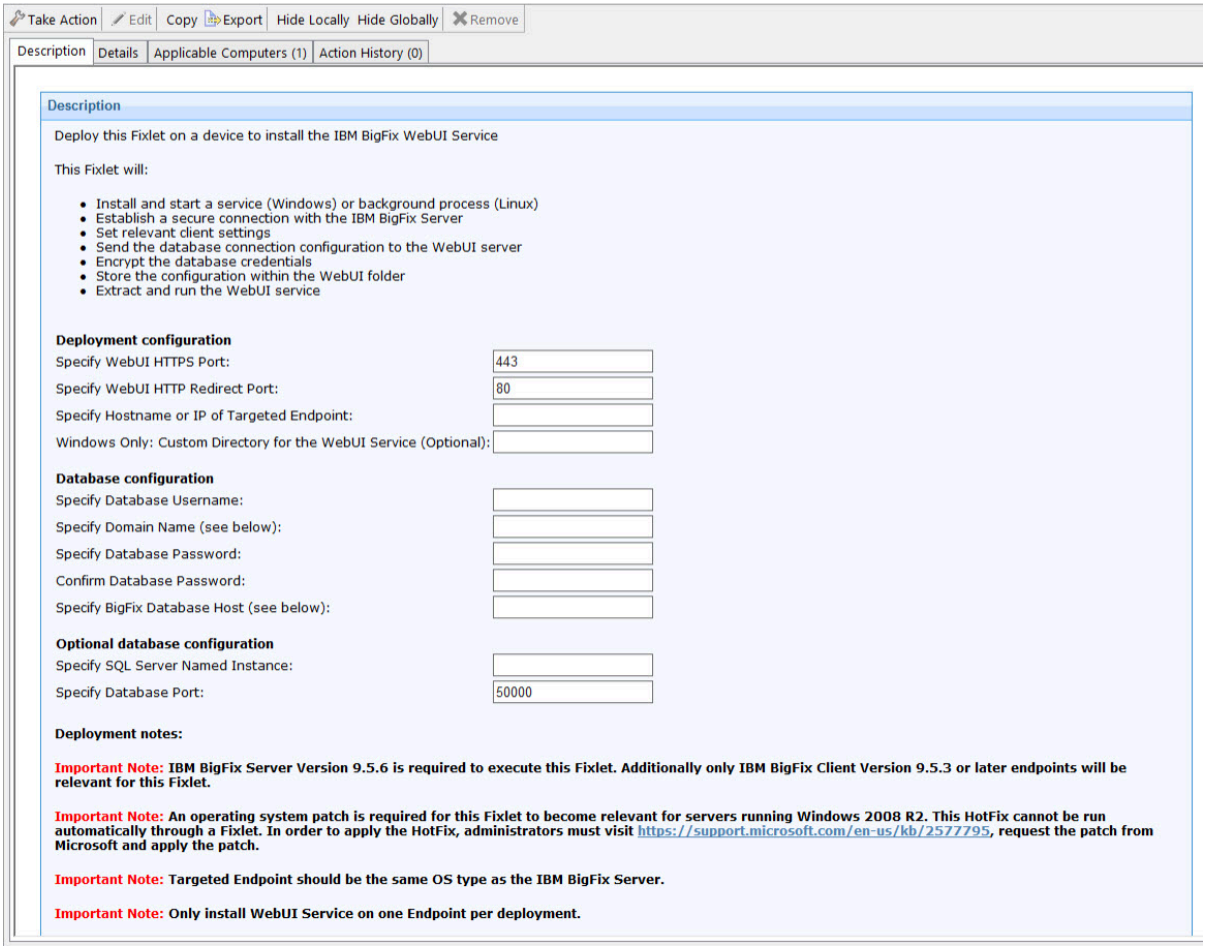
- Select the appropriate value in the Specify Database Authentication Type field.
- If you selected Windows authentication, in the Specify Database Username field, enter your username in the format DOMAIN\username, where DOMAIN must be a NetBIOS domain name.
- If you selected SQL Server authentication, with an SQL credential, in the Specify Database Username field, enter your plain SQL Server username, the default is sa.
- In the Specify BigFix Server Database Host, enter the host name or the IP of the computer that hosts the database of your BigFix Server. The host name must be DNS-resolvable.
- You can use either the Specify SQL Server Named Instance field or the Specify Database Port field. Select one to edit it. To use the default database instance, enter its port, which by default is 1433. To use a named database instance, enter its name (e.g. SQLEXPRESS).
- If you selected to connect to a named database instance, enter the instance name in the Specify SQL Server Named Instance field.

6. If you are using IBM DB2:
   - In the target database computer, ensure that the DB2 configuration parameter extended_row_sz is set to ENABLED. Starting from DB2 10.5, this parameter is ENABLED by default. However, it could be set to DISABLED if DB2 has been upgraded from version 10.1 or earlier. This parameter can be manually changed. Ensure it is set to ENABLED for all Linux Server installations, otherwise the WebUI cannot start successfully.
   - In the Fixlet, specify the DB2 database username and password.
   - In the Specify BigFix Server Database Host, enter the host name or the IP of the computer that hosts the database of your BigFix Server. The host name must be DNS-resolvable.
   - Enter the DB2 database port in the Specify Database Port field.
7. Ensure that the following ports will be available and allowed:
   - The default HTTP redirect port is 80.
   - The default HTTPS port is 443.

- If you use SAML 2.0, the port 5000 of the WebUI server must be reachable by the Web Reports server and the BigFix main server. For more details, see How to configure BigFix to integrate with SAML 2.0.
- For its internal scope, WebUI uses also the port 5001. Ensure that it is available on the WebUI server.

Note: If the WebUI is installed on another machine, ensure that the *WebUI port* on the BigFix main server is allowed as well. The *WebUI port* value is calculated as follows: *Server port number* increased by 4. The *Server port number* can be configured by the BigFix Administrator during the installation and, as default, its value is 52311: the default value for the *WebUI port* is equal to 52315. For more information about the *Server port number*, see Step 2 - Requesting a license certificate and creating the masthead and Customizing the masthead parameters (root server installation on Windows and on Linux, respectively).

8. If you are installing the WebUI on a remote server and configuring WebUI to work with SAML, set the `_WebUI_AppServer_Hostname` key of the BigFix server computer to the host name of the computer where the WebUI is installed.
9. Deploy the Fixlet.



Post-installation Notes:

- If the Fixlet fails, revoke the certificates that it generates and sends to the target machine.
- If you have encryption enabled for your MSSQL server, you will need to apply the client setting `_WebUIAppEnv_MSSQL_CXN_ENCRYPT = 1` on the remote WebUI server.
- If WebUI is installed on a Linux machine, to display all localized messages correctly, on the machine where WebUI is installed, create the client setting `_WebUIAppEnv_LANG` *(on page 71)* and set the preferred language; for example, **ja_JP.UTF-8** for Japanese.
- If the Fixlet is successful, the *WebUI port* on the root server is used to allow the communication between the root server and the WebUI. All network firewalls between the two machines must also allow using the *WebUI port*.

- Start, stop, and restart the WebUI process on a remote machine using services.msc on Windows, or through the terminal in Red Hat Linux. If stopped, the Fixlet **2562 - BES WebUI Service not Started** can also be used to start the WebUI.
- Inline Reporting feature is disabled by default in WebUI running on versions earlier than BigFix 10 Platform. To enable Inline Reporting capabilities, set the client setting `(_WebUIAppEnv_ENABLE_INLINE_REPORTING)` to 1. This is because this feature is not extensively tested in WebUI running on versions earlier than BigFix 10 Platform.

DB Schema Upgrade Procedure

Use the DB Schema Upgrade procedure on BigFix Platform versions 9.5.5 or later to upgrade an existing WebUI installation to use the WebUI with Microsoft SQL Server or the IBM DB2.

Allow adequate time for the WebUI service to start following the installation; index construction and other process need to complete before you can use the WebUI.

Before you start:

- Review the WebUI deployment *(on page 2)* and hardware *(on page 4)* requirements, and verify that your environment is ready. For example, if the database account permissions are not correct, the WebUI will not start correctly.
- Complete the BigFix Platform installation to V9.5.5 or later, including the WebUI service. For more information, see the BigFix Installation Guide.

DB Schema Upgrade Procedure

Before you deploy the database schema update Fixlet, make sure that there are no delayed updates pending for any WebUI applications. The Fixlet will not be relevant if you do not have the current sites. This is a particularly important check for customers with air gapped deployments, or who use the Delayed Update function.

1. On the BES Support site, locate and run the Fixlet **Deploy/Update WebUI Database Configuration**.

Change Ports

Use the Fixlet **Change Ports for WebUI Service and Web Reports** to change the communication ports.

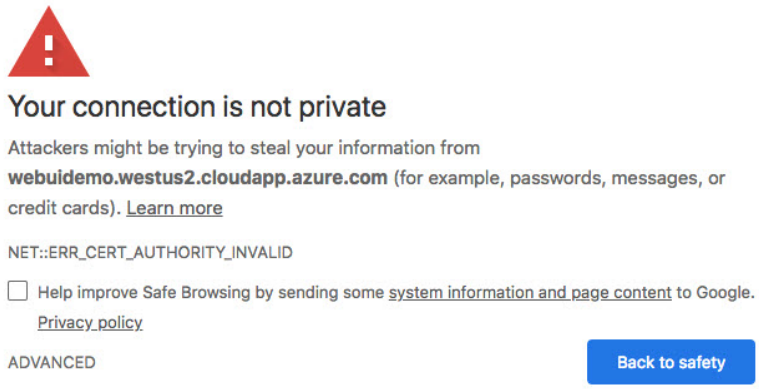
On BigFix Platform V9.5.3 and above, use the Fixlet **Change Ports for WebUI Service and Web Reports** on the BES Support site to change the communication ports on either the BigFix server or a remote machine. Use the Fixlet description to enter the port numbers you want to use.

Configure SSL certificates

Secure Sockets Layer (SSL) certificates enable secure communication between the BigFix WebUI server and all users that access it. Use this procedure to configure SSL certificates for BigFix WebUI.

Using self-signed SSL certificates

The WebUI uses self signed certificates generated by the BigFix Platform. These self signed certificates encrypt traffic, but are not trusted by web browsers (unless the corresponding CA certificate is added to the trusted certificate store on the endpoint). People running in this configuration will see this screen and can safely click through, ignoring the message:



Consider purchasing officially signed SSL certificates by a certificate authority (CA) such as Verisign, Entrust, or ZeroSSL. The advantage of using an external CA is that root certificates of known public CAs are imported by default into modern web browsers.

Using SSL certificates from a trusted Certificate Authority

Configure certificates from a trusted certificate authority (CA) to use in your BigFix WebUI deployment. When generating a private key and a certificate signing request (CSR) for a CA signed certificate, ensure that the private key and the certificate files have the following format and structure:

Private key format

PEM-encoded and without a password protection. The pvk format is not supported. Ensure that the private key (*private.key*) is enclosed between the following statements:

```
-----BEGIN PRIVATE KEY-----
<<base64 string from private.key>>
-----END PRIVATE KEY-----
```

X509 certificate format

PEM-encoded. If you have also received the intermediate and root certificates as separate files, you should combine all of them into a single one. For example, if you have the primary certificate file (*certificate.crt*) and the intermediate certificate file (*ca_intermediate.crt*), ensure that you combine them in the following order, primary certificate first followed by the intermediate certificate:

```
-----BEGIN CERTIFICATE-----
<<primary certificate: base64 string from certificate.crt>>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<<intermediate certificate: base64 string from ca_intermediate.c
rt>>
-----END CERTIFICATE-----
```

If you received the root certificate (*ca_root.crt*) in addition to the intermediate certificate, combine them as follows:

```
-----BEGIN CERTIFICATE-----
<<primary certificate: base64 string from certificate.crt>>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<<intermediate certificate: base64 string from ca_intermediate.c
rt>>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<<root certificate: base64 stringfrom ca_root.crt>>
-----END CERTIFICATE-----
```

Deploying SSL certificates

To deploy the SSL certificates to the BigFix WebUI server:

1. Rename SSL private key to `ssl.pvk`.
2. Rename the SSL certificate to `ssl.crt`.
3. Copy both files to the following location on your WebUI server:

Table 2. WebUI server directory for storing the certificate and private key

Operating System	WebUI Server	WebUI Server Directory
Windows	BigFix Root Server	`C:\Program Files (x86)\BigFix Enterprise\BES Server\WebUI`
	Remote Server	`C:\Program Files (x86)\BigFix Enterprise\BES WebUI\WebUI`
Linux	BigFix Root Server	`/var/opt/BES Server/WebUI`
	Remote Server	`/var/opt/BESWebUI/WebUI`

4. On the WebUI machine, ensure that the following client settings are added and that their values are the paths specified in Step 3:

- _WebUIAppEnv_WEB_CERT_FILE
- _WebUIAppEnv_WEB_KEY_FILE

For example, if your WebUI directory is `C:\Program Files (x86)\BigFix Enterprise\BES WebUI`:

- The value of WEB_CERT_FILE should be `C:\Program Files (x86)\BigFix Enterprise\BES WebUI\ssl.crt` and
- The value of WEB_KEY_FILE should be `C:\Program Files (x86)\BigFix Enterprise\BES WebUI\ssl.pvk`

5. Restart the BES WebUI Service.

Revoke WebUI Certificates

You must revoke your certificates if they have been compromised or if they are no longer valid for the intended purpose.

To revoke a certificate, use the `BESAdmin` tool on the root server.

- Windows deployment

```
BESAdmin.exe /revokewebuicredentials /sitePvkLocation:<pvklocation>
/sitePvkPassword:<pvkpassword> /hostname:<hostname>
```

- Linux deployment

```
./BESAdmin.sh -revokewebuicredentials
 -hostname=<hostname_of_the_instance>
-sitePvkLocation=<pvk_loc> -sitePvkPassword=<pvk_password>
```

For more information about the `BESAdmin` tool, see: Additional administration commands.

Send Notification

This section describes the Send Notification service.

Use the BigFix Send Notification service to trigger an email alert when a deployment completes on all devices, or fails on a specified number of devices.

To use the Send Notification service:

- An operator's **Custom Content** permission must be set to *"Yes."*
- An operator's **Can Create Actions** permission must be set to *"Yes."*
- BigFix Web Reports must be installed, running, and reachable via the REST API.

For more information on enabling the email notification service, see the BigFix Configuration Guide. For more about permissions, see Permission Effects in the WebUI.

Access the WebUI

This section shows how to access the WebUI interface.

To access the WebUI from a web browser, navigate to:

```
<http_or_https>://<IP_or_FQDN>:<port_if_not_80/443>
```

Depending on the size of the deployment, WebUI index creation can take one to two hours, and up to 12 to 16 hours for large deployments. During index creation the WebUI is not available.

Chapter 4. Remove the WebUI Service

Use this procedure to remove the WebUI from BigFix Platform.

1. Run **Fixlet 2557 - Remove WebUI Service** to remove the WebUI from the BigFix Server or a remote machine. The server instance, including client settings, the ETL directory, and the working WebUI directory will be removed.

   Note: If you need to move the WebUI or reinstall it, the next step is not mandatory. Perform the actions described in step 2 only if you want to do a cleanup into the BigFix Server database or if you do not want to reinstall the WebUI.

2. Copy the SQL statements for your database platform from BES WebUI DB Cleaner and run them on the BFENT database server. You must have access to BFENT and permission to run the SQL to complete this task. For example, SA level for SQL Server users, and DB2inst1 or dbadmin level for DB2 users.

Chapter 5. Provisioning Users

Use permission settings in the WebUI and the BigFix Console to control access to the WebUI and its functions.

Use Console permission settings to:

- Establish site, device, operator, and role permissions.
- Control which applications operators see on the **WebUI Apps** menu.
- Disable access to the **WebUI login** page for an operator or role.

Use the WebUI's Permission service to:

- Set content target limits, to restrict the amount of content an operator can deploy.
- Set device target limits, to restrict the number of devices an operator can deploy to, or query against.
- Grant unlimited targeting to a role.

Master operators retain full access to all WebUI elements, functions, and controls at all times. WebUI applications that are intended for master operators only (such as the Permissions service) do not appear on operators' screens. All WebUI operators have access to deployment information. For example, operators can see the list of all the patches deployed to an endpoint whether they have permission to patch or not. The ability to view this information does not imply the permission to act on it, for example, to stop a deployment in progress.

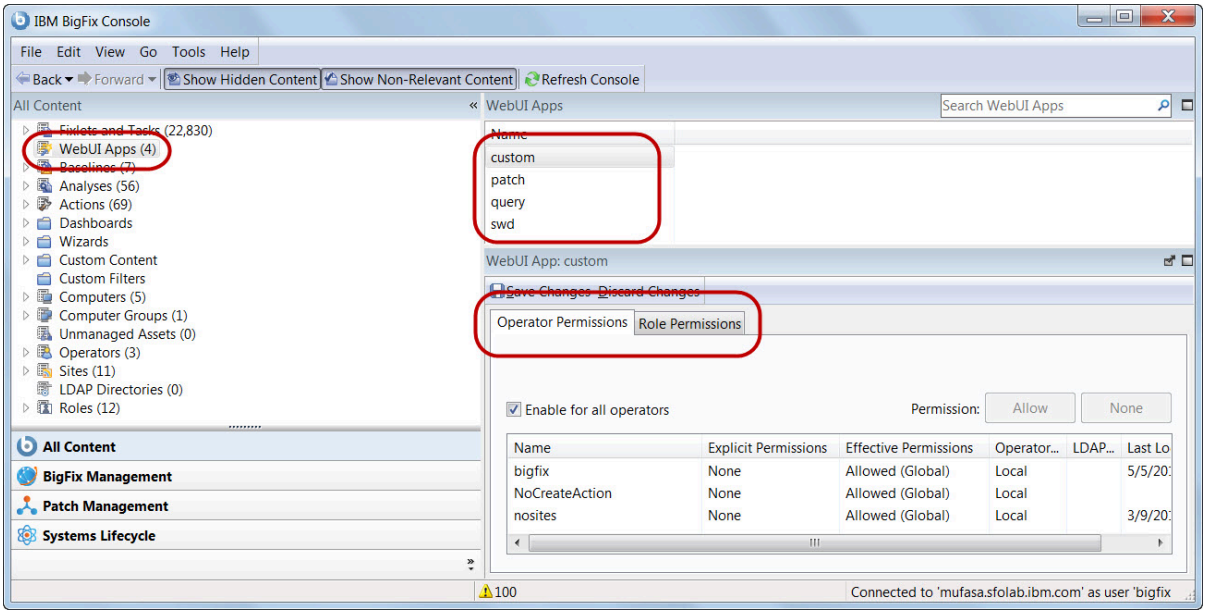
Procedures for setting WebUI permissions appear below. To read more about BigFix permissions see the BigFix Site Administrator and Console Operators. To learn more about managing operators and roles, see the BigFix Console Operator's Guide.

Permissions Set in the BigFix Console

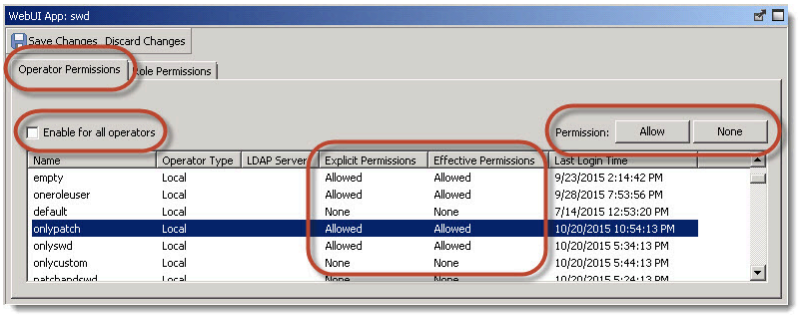
In this page, you can fine instructions to manage the WebUI permissions set in the BigFix Console.

Detailed procedures, including a description of how explicit and effective permissions work, appear below. To summarize: use the Console's **All Content > WebUI Apps** screen to set permissions for operators and roles. Or manage the same settings from the **All Content > Operators > WebUI** and **All Content > Roles > WebUI** screens. To control access to the WebUI log-in page, use the **All Content > Operators > Details** and **All Content > Roles > Details** screens.

Set Permissions: WebUI Apps Screen



1. Select a WebUI application.
2. Select the **Operator** or the **Role** tab, and then an operator or role.



3. Click the **Allow** button to grant access, or the **None** button to disable access.
4. Click **Save Changes**.

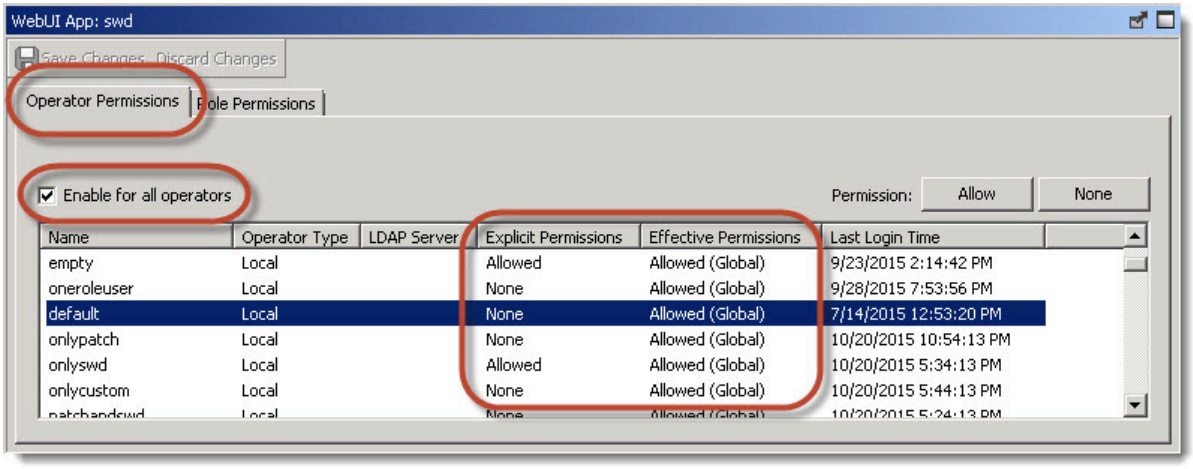
To grant access to all operators with one click check the **Enable for All Operators** box.

Permissions granted directly to an operator are called *"explicit"* permissions. Permissions granted indirectly to one or more operators (for example, through a role) are known as *"effective"* permissions. What happens when there is a conflict between an operator's explicit and effective permissions? For example, what happens when access to the Patch application is enabled for Operator A, but disabled for a role to which Operator A is assigned? When this happens BigFix applies the least restrictive of the two settings, and the result is the effective permission. The table shows the result for each set of explicit permissions.

Table 3. Explicit and Effective Permissions

Explicit Permissions	Effective Permission
Yes – Granted to operator. Yes – Granted to operator through a role. Yes – **Enable for All Operators** box checked.	Yes Allowed
No – Disabled for operator. No – Disabled for assigned role. No – **Enable for All Operators** box clear.	No None
Yes – Granted to operator. No – Disabled for assigned role. No – **Enable for All Operators** box clear.	Yes Allowed
No – Disabled for operator. Yes – Granted to operator through a role. No – **Enable for All Operators** box clear.	Yes Allowed
No – Disabled for operator. No – Disabled for assigned role. Yes – **Enable for All Operators** box checked.	Yes Allowed (Global)

When permissions are granted through the WebUI Apps setting's **Enable For All Operators** check box, the Effective Permissions value changes from *"Allowed"* to *"Allowed (Global)."*



Set WebUI Permissions: Operators Screen

To grant or remove access to WebUI components for an operator:

1. Go to **All Content > Operators > WebUI Apps** tab.
2. Select an operator.
3. Select a WebUI application.
4. Click the **Allow** or **None** to grant or disable access.
5. Click **Save Changes**.

Set WebUI Permissions: Roles Screen

To grant or remove access to WebUI components for a role:

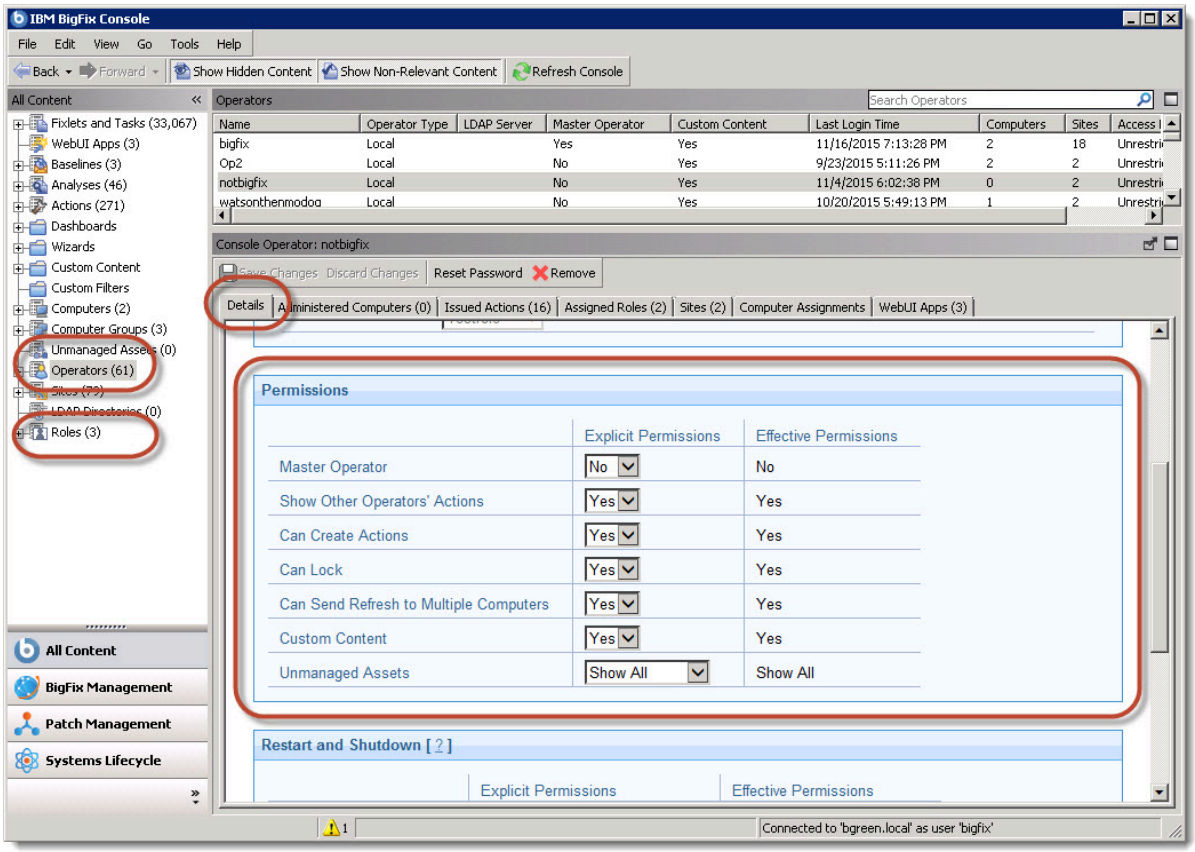
1. Go to **All Content > Operators > WebUI Apps** tab.
2. Select a role.
3. Select a WebUI application.
4. Click the **Allow** or **None** to grant or disable access.
5. Click **Save Changes**.

The Create Actions Privilege

An operator whose **Can Create Actions** permission is set to No cannot deploy content, but can still see deployments made by others.

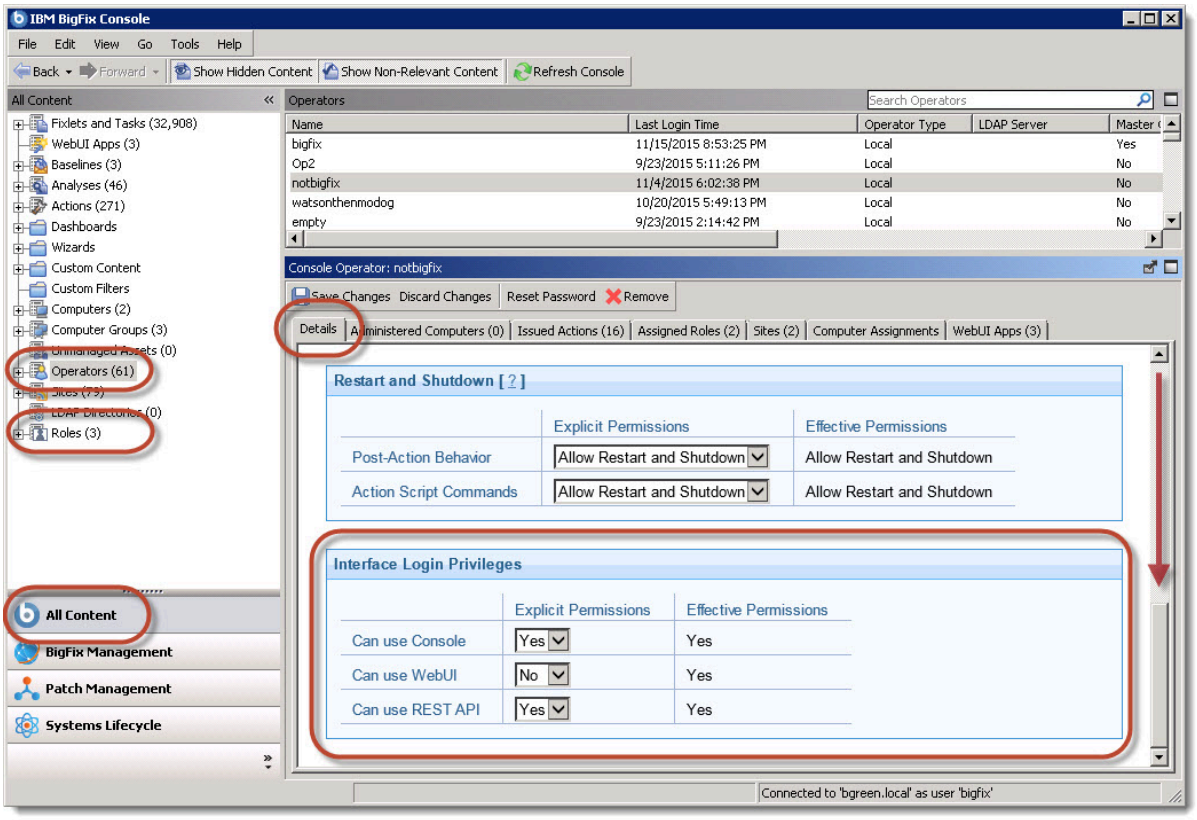
To set Create Action permissions to No:

1. Go to **All Content > Operators > Details** or **All Content > Roles > Details**.
2. Scroll down to the Permissions pane and set **Can Create Actions** to *"No"*.
3. Click **Save Changes**.



Disable Log-in Access to the WebUI

To disable WebUI access for an operator or role completely, turn off access to the log-in page. This option rejects a user's log-in credentials.



To grant or remove WebUI login access for an operator:

1. Go to **All Content > Operators > Details** tab.
2. Scroll down to **Interface Login Privileges**.
3. Set **Can Use WebUI** to *"Yes"* or *"No"*.
4. Click **Save Changes**.

To grant or remove WebUI login access for a role:

1. Go to **All Content > Roles > Details** tab.
2. Scroll down to **Interface Login Privileges**.
3. Set **Can Use WebUI** to *"Yes"* or *"No"*.
4. Click **Save Changes**.

Notes on Specific Applications

In this page, you can find important notes on specific applications.

Permissions and the Send Notification Service

The Send Notification option allows operators to issue an email alert when a BigFix deployment completes or fails. To use it:

- The Send Notifications service must be enabled.
- An operator's **Can Create Actions** and **Custom Content** permissions must both be set to **Yes**.

Permissions and the Executive Dashboard

The information that is displayed on the Overview dashboard reflects the permissions of the person who is logged in. For example, operators who do not have permission to use the Software application do not see software package data. Device totals reflect operator device assignments. For example, operators who work on a subset of devices, such as Windows machines only, see device totals for Windows machines only.

Permissions and BigFix Query

Use the **Can Submit Queries** and **Custom Content** permissions to fine-tune what operators can see and do in the Query application. They are both set in the Console and can be configured for operators and roles.

Permission to Submit Queries

Use the **Can Submit Queries** permission to control access to the REST API that supports queries. Operators with **Can Submit Queries** set to **Yes** see the results of their queries. Operators with **Can Submit Queries** set to **No** see no query results and the message, *"The logged in user is not allowed to submit queries."* For more information about BigFix Query and its APIs, see Getting client information using BigFix Query in the *BigFix Platform Configuration Guide*.

Permission to Create Custom Content Set to No

Operators with **Can Submit Queries** set to **Yes** and **Custom Content** set to **No** can:

- Run queries in the custom sites they have permission to use. Query targets include individual machines, manual groups, and dynamic groups.
- Filter and search for queries.
- Assign values to query variables.
- Save query results to a file.

These operators cannot add or edit queries, or see the Relevance expressions that they contain.

Permission to Create Custom Content Set to Yes

Operators with **Can Submit Queries** set to **Yes** and **Custom Content** set to **Yes** can:

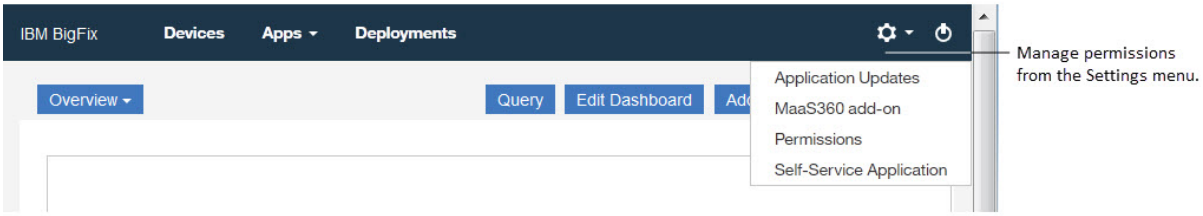
- Run queries in the custom sites they have permission to use. Query targets include individual machines, manual groups, and dynamic groups.
- Filter and search for queries.
- Create and edit queries and query categories.
- Load sample queries.
- Create, edit, and assign values to query parameters.
- See and edit query Relevance expressions.
- Save query results to a file.

The WebUI Permissions Service

Use the WebUI Permissions service to control the amount of content operators can deploy, and the number of devices they can deploy to or query, at one time.

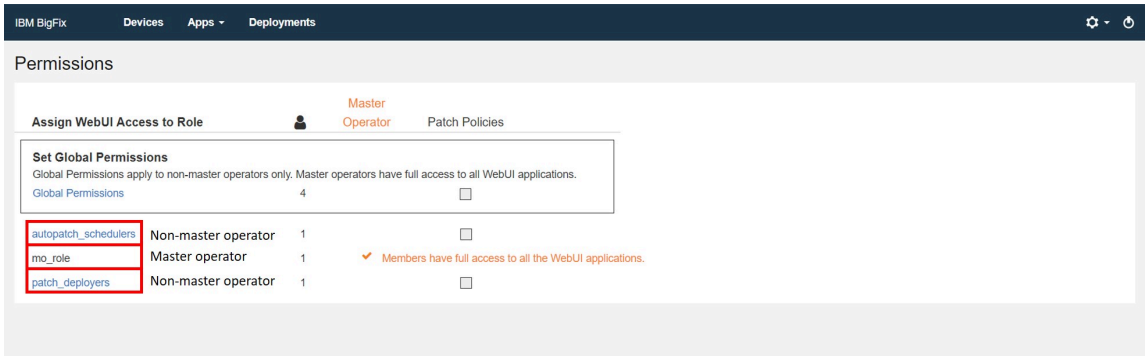
You can also use the Permissions service to grant unlimited targeting permissions to a role. The service will provide increasingly fine-grained control over permissions and preferences in WebUI applications. You can also grant permissions to non-master operator roles to

perform various actions in patch policies. Open the Permissions service from the **Settings** menu.



Global Permissions in WebUI Permissions service apply only to non-master operators. Master operators have full access to all WebUI application.

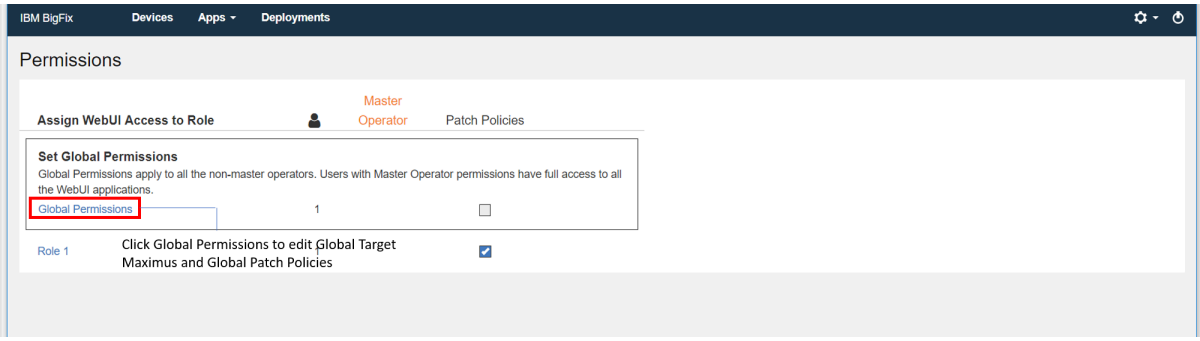
Important: For the below scenarios, two non-master operator roles and one master operator role is taken into account.

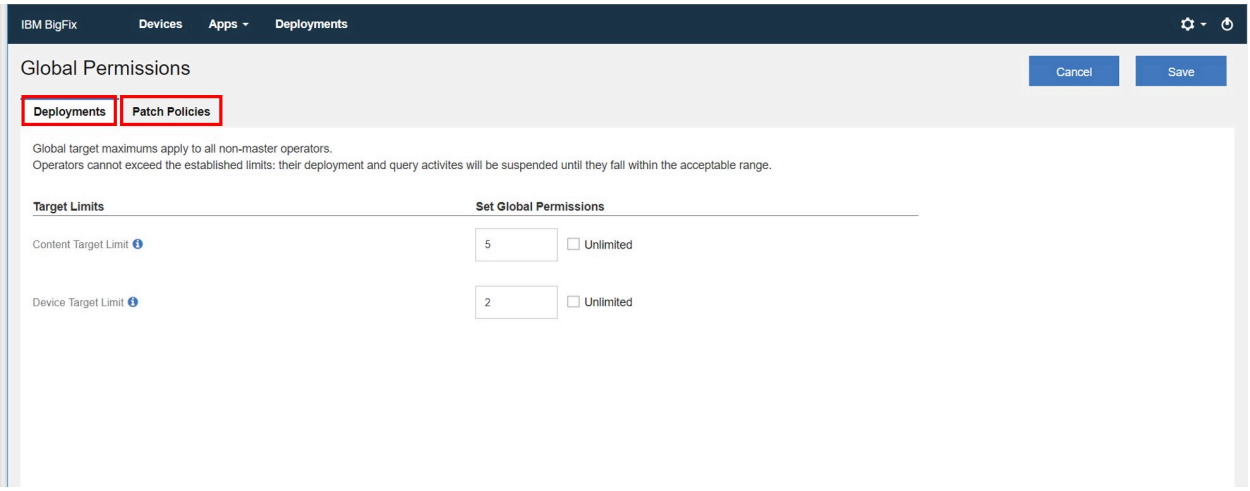


1. When Patch Policies check box of Global Permissions is selected, the non-master operator roles will inherit the access to Patch Policies app from Global Permissions and master operator role will have full access to all WebUI applications by default.
2. When Patch Policies check box of Global Permissions is not selected, the non-master operator roles will not have access to Patch Policies app and master operator role will have full access to all WebUI applications by default.

3. When Patch Policies check box of Global Permissions is not selected, the non-master operator roles can still be granted access to Patch Policies app by selecting the patch policies check boxes of the roles manually, and master operator role will have full access to all WebUI applications by default.

Click **Global Permissions** to edit global target maximums and global patch policies permissions. In the **Deployments** tab, the administrator can set the content target limit and device limit for all non-master operators. Non-master operators cannot exceed the established limits. In case of violations, their deployment and query activities will be suspended until they fall within the acceptable range. Global target maximums apply to all non-master operators except the members of a role that has been granted unlimited target permissions. In the **Patch Policies** tab, the administrator can grant permissions which allow non-master operators to perform different actions.





When certain patch policy check box in **Patch Policies** tab is selected, other patch policies check boxes will be auto selected and disabled. This is due to permission dependencies on each other.

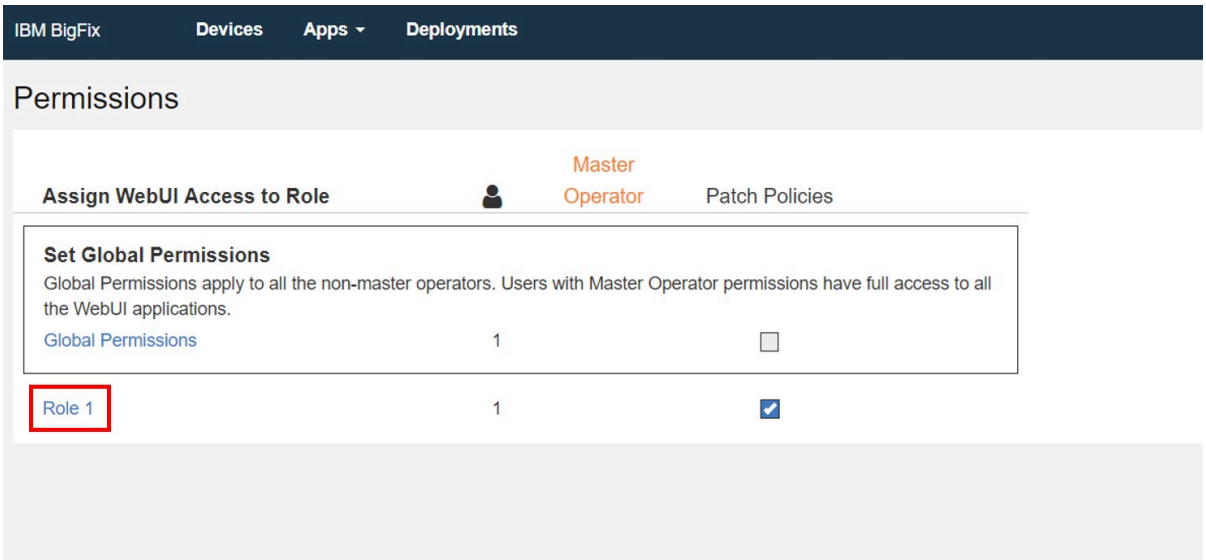
1. When Delete Policy permission is granted, non-master operators will also have permissions to Create/ Edit Policy, Delete Schedule, Create/ Edit Schedule, Add/ Remove Your Own Targets and Remove Other Operator's Targets.
2. When Create/ Edit Policy permission is granted, non-master operators will also have permission to Refresh Policy.
3. When Delete Schedule permission is granted, non-master operators will also have permissions to Create/ Edit Schedule, Add/ Remove Your Own Targets and Remove Other Operator's Targets.

Click a role to edit role specific permissions:

- In the **Deployments** tab, administrator can set the content target limit and device limit for the selected role. Operators cannot exceed the established limits. In case of violations, their deployment and query activities are suspended until they fall within the acceptable range.

- In the **Patch Policies** tab, administrator can grant permissions which allow specific role to perform different actions.

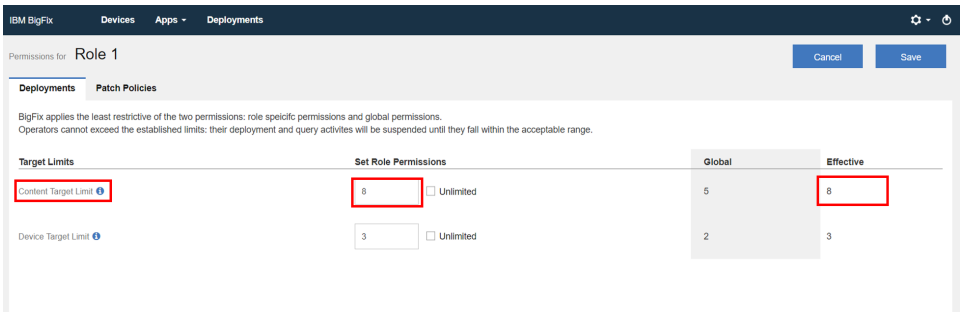
  Note: The Patch Policies tab is visible only if the selected role has permission to access the Patch Policies app.



Important: The effective permissions for a role are the least restrictive of the global permissions and role permissions.

Example: Content Target Limit

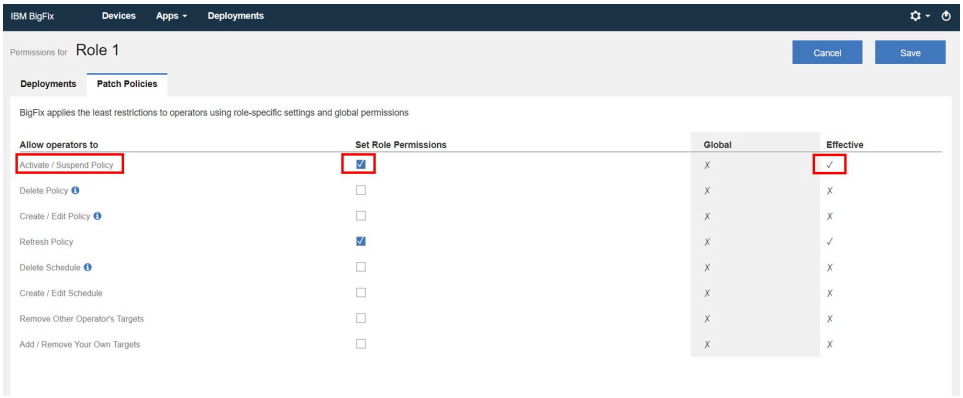
The global permission is set to 5 and the role permission to 8 for Content Target Limit. The least restrictive of the global permission and role permission is 8. The effective permission is set to 8 as it is the least restrictive.



In case the **Unlimited** check box is selected, the effective permissions is set to unlimited.

Example: Patch Policies

Activate/ Suspend Policy check box is not selected for global permission and selected for role permission. The least restrictive of the global permission and role permission in this case would be to allow operators in this role to Activate/ Suspend Policy.

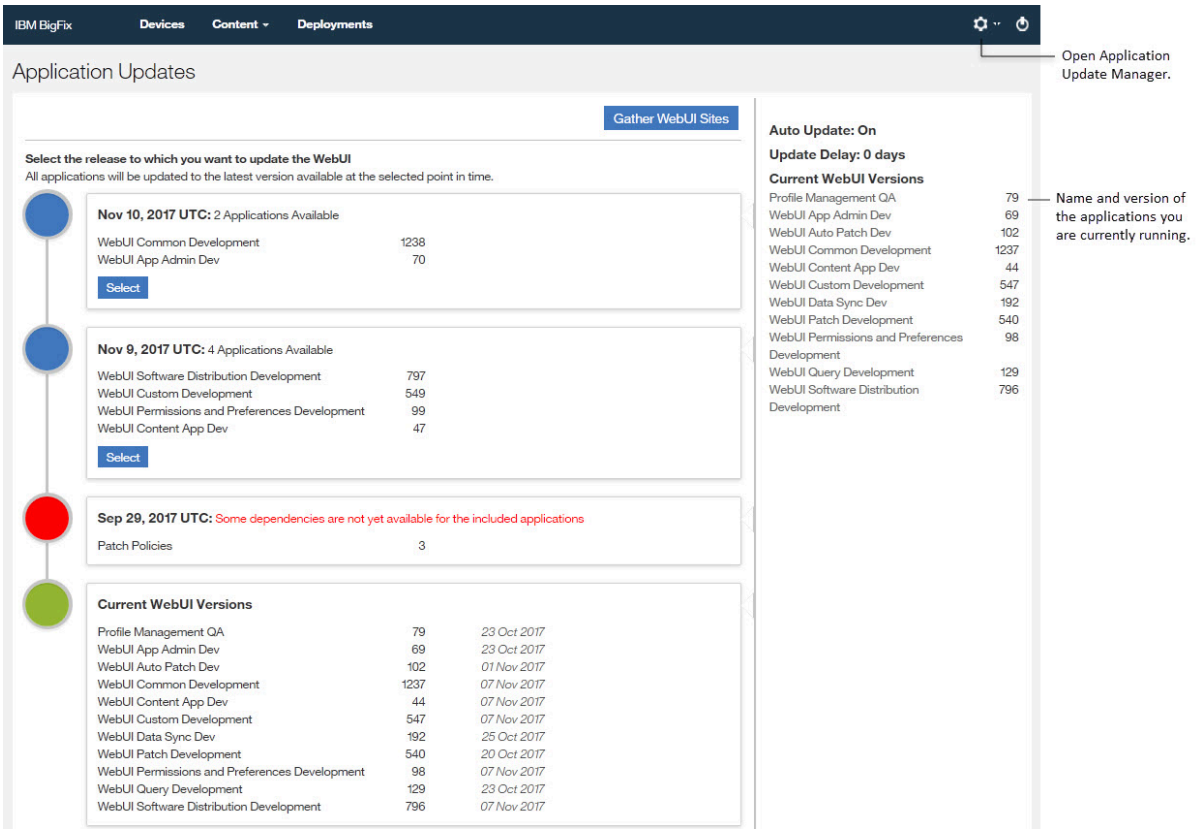


Chapter 6. Managing Application Updates

Use the **Application Update Manager** to:

- Display version information for each WebUI application.
- View and apply available updates.
- Run an ad hoc gather of WebUI sites.
- View AutoUpdate settings.

To display the **Update Manager**, click the **Settings** icon on the navigation bar. Only Master Operators see this icon.



Version numbers reflect an application's site. For example, the Patch application resides in the WebUI Patch site; the WebUI application, which includes the Common application and the Login application, resides in the Common site.

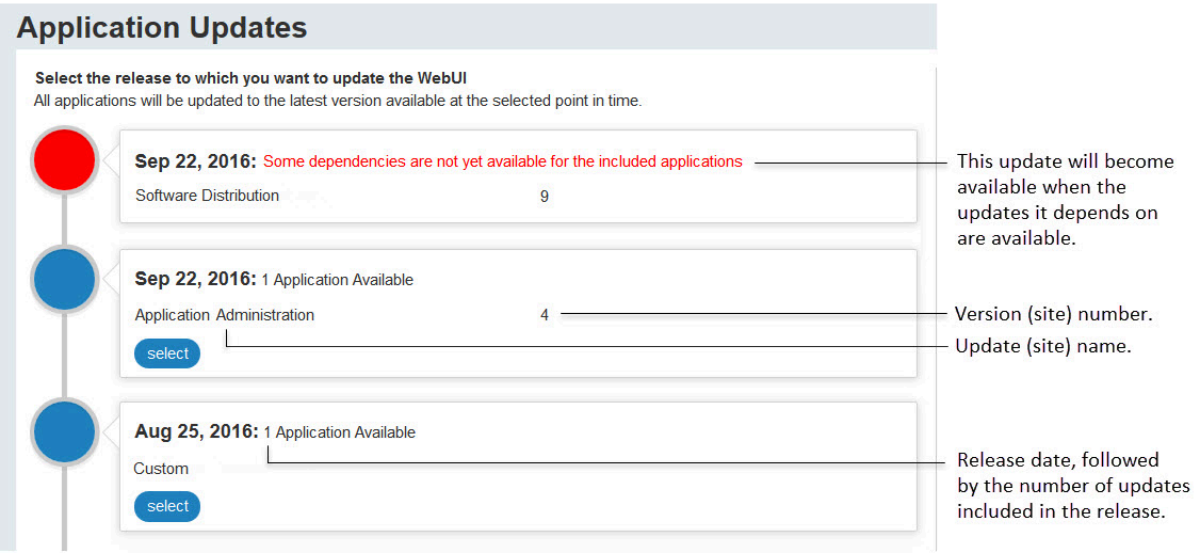
On BigFix platform versions 9.5.7 and above the **Gather** button appears on the Update Manager. On V9.5.7 the BigFix server checks for new versions of WebUI sites every 6 hours. Use **Gather** button to retrieve any new versions that have been released since the last gather occurred.

When you update an application, the selected update and all the preceding updates are applied. Internal dependency checks prevent you from updating an application that depends on a version of another application that is not yet available. For example, you cannot install a version of the WebUI Patch application that depends on features in the Common Application that have not yet been released.

WebUI services remain available during updates. To update an application:

1. Click **Select**. A confirmation dialog shows the version you will be running following the update.
2. Click **Update Now** to complete the operation, or **Cancel** to return to the **Update Manager**.

   Take into account that the WebUI service will be automatically restarted if you are updating the **WebUI Common** application.



Notes

- You cannot roll back to an earlier version once an update has been applied.
- When AutoUpdate is on and the delay period is set to 0, the number of available updates in the Update Manager will be 0, because updates are automatically applied. When AutoUpdate is on and the delay period set to 30 days, the number of available updates will extend back 30 days (because updates older than 30 days have been applied).
- When AutoUpdate is off, the number of available updates will extend back in time for an indefinite period.
- The attended restart of the WebUI service after updating the **WebUI Common** application is available only starting from Patch 17.

AutoUpdate and AutoUpdateDelay

Use the AutoUpdate feature to automatically apply new versions of WebUI applications as they become available. When AutoUpdate is on, WebUI application updates are automatically applied. When AutoUpdate is off, updates to WebUI applications must be applied manually. Use the AutoUpdateDelay setting to control the timing of automatic updates when AutoUpdate is on. Set them to install immediately (Update Delay = 0 days), or delay them for up to 30 days. Reasons to delay automatic updates might include:

- Providing time to update a procedure that will change as a result of new features.
- Trying a new version of an application on a test deployment before installing in on a production system.
- Staying on a specific WebUI version for these or other reasons.

When the WebUI is installed the AutoUpdate function defaults to on, and the AutoUpdateDelay defaults to 0 days. To adjust the AutoUpdate and AutoUpdateDelay settings, use the BigFix console on the computer where the WebUI service is installed.

1. On the BigFix Console, select **Computers**.
2. Right-click the WebUI server (either the BigFix server, or a remote machine).
3. Select **Edit Computer Settings**.
4. Select the setting that you want to change.

- For AutoUpdate, select `_WebUIAppEnv_APP_UPDATE_ENABLE_AUTO`. When set to 1, WebUI applications automatically update to the most recent versions in the Pending Sites cache. When set to 0, AutoUpdate is Off.
- For AutoUpdateDelay, select`_WebUIAppEnv_APP_UPDATE_DELAY_DAYS`. Enter the number of days to wait between updates. The Delay range is 0 - 30 days; the default is 0 days.

Note: The first time that you change the AutoUpdate and AutoUpdateDelay defaults following installation of the WebUI, you will be adding the client settings specified below, not updating them. To add a setting for the first time, in Step 3 of the procedure select **Add Computer Setting**, rather than **Edit Computer Settings**, and enter the required setting name and value. Then make subsequent adjustments to the AutoUpdate and AutoUpdateDelay settings using the **Edit Computer Setting** option.

Disaster Recovery

To quickly restore specific versions of your WebUI applications after a system crash, schedule regular backups of the **Sites** and **Pending Sites** folders, which are located in the **WebUI** folder on your WebUI server. The **Sites** folder stores the versions of the WebUI applications you are currently running. The **Pending Sites** folder (within the **Sites** folder) stores the versions that have become available but have not yet been installed.

- To restore your system by using backups, drop the backed-up files into the **Sites** and **Pending Sites** folders.
- To use the latest versions of the WebUI applications after a crash, restart the WebUI server.
- To generate a list of the most recent versions of each application you were using before the crash, check the dashboard variable by using the Relevance statement:

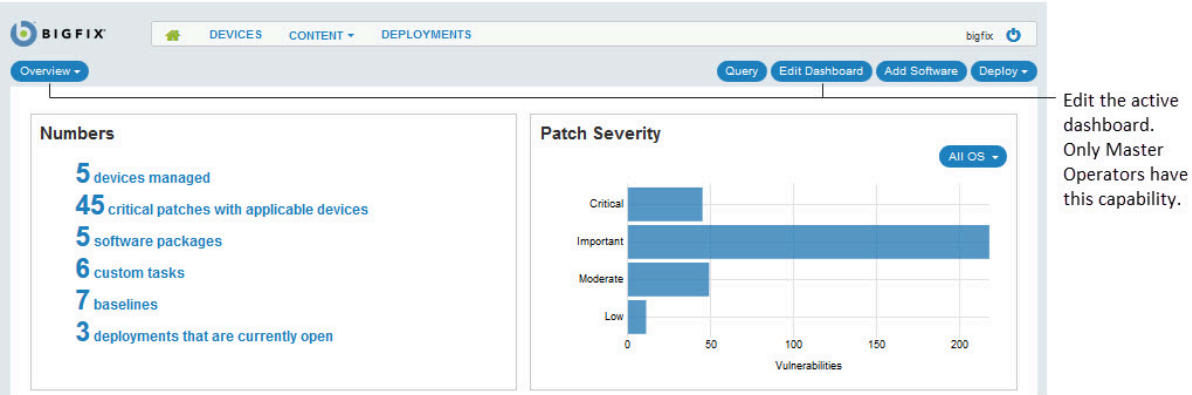
```
shared variable (“WebUIAppAdmin”, “Current_Sites”)
```

If the backups become unavailable, contact Technical Support; they will be able to provide additional options.

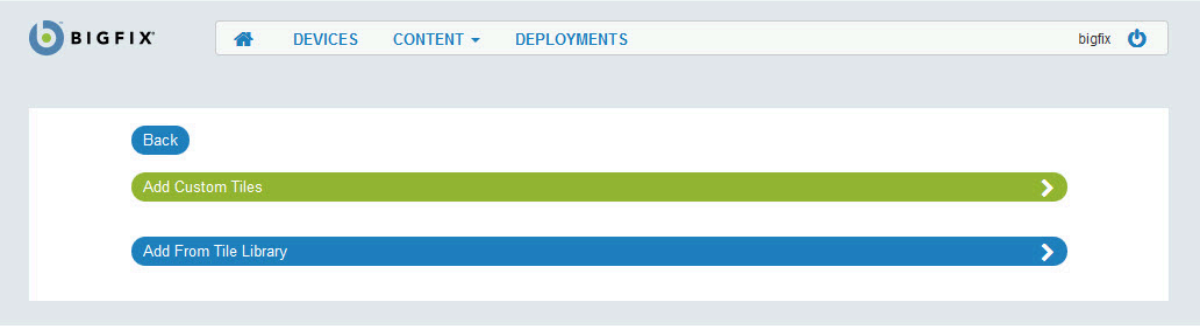
Chapter 7. Editing Dashboards

Use the WebUI's editing tools to customize the WebUI Overview and Executive Overview dashboards.

Extract and present BigFix data in an array of formats to summarize key information from across your enterprise. Only Master Operators can edit the active dashboard to customize.

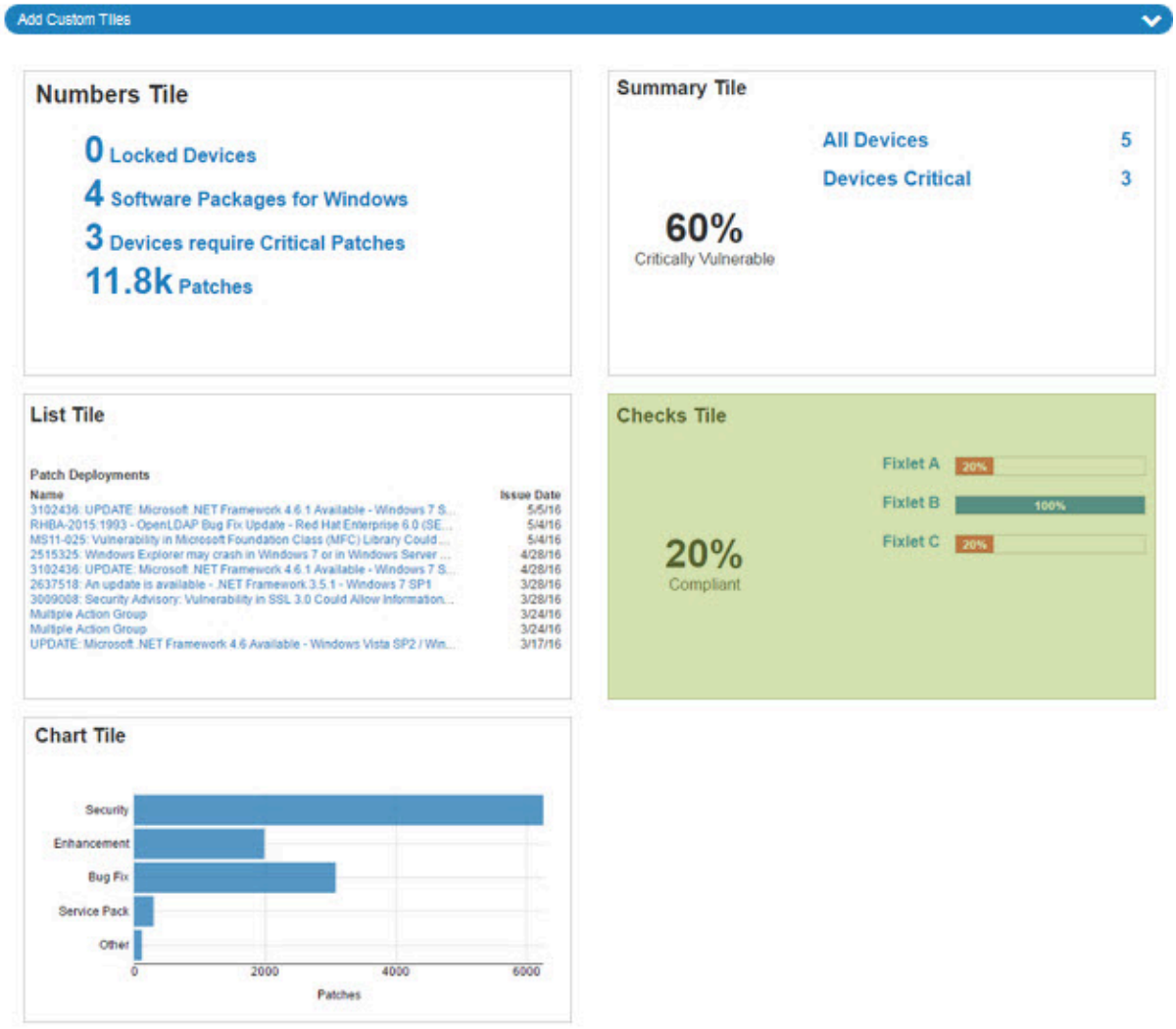


Drag tiles to arrange them, and preview dashboard designs as you build. Draw from a library of pre-defined tiles, or design your own.



Pre-defined tiles include Environment Overview, Patch Compliance, Patch Severity, New Releases, and Deployments in the last 30 Days.

While the WebUI's default overview tiles are useful to many users, the custom tiles enable you to place critical information specific to your own deployment on the WebUI and Executive overviews. Use the five custom tile types to design and build your own tiles: Key Numbers, Summaries, Lists, Checks, and Charts.



All users can see and use the WebUI dashboards, but only Master Operators can edit them. Changes made to either dashboard become the default design for that overview for all users. Dashboard elements and data are adjusted to reflect the BigFix permission levels and assignments of Non-Master Operators.

Four screens are involved in editing and building tiles:

- **Edit Dashboard** - Arrange, delete, and add tiles.
- **Select Tile** - Select pre-defined tiles and custom tile templates.
- **Build Tile** - Select top-level data objects, arrange tile elements, and preview designs.
- **Define Filters** - Refine tile data and perform complex joins.

General Editing Techniques

To edit a dashboard, click the **Edit Dashboard** button.

Use the **Edit Dashboard** page to:

- Add and delete tiles.
- Reposition tiles on the page.
- Turn the Tile Performance Monitor message on and off.

The Tile Performance Monitor displays a message across WebUI dashboard tiles that load slowly: *"The filters used in this tile took over 10 seconds to load. Operators with access to a smaller set of BigFix data will see better performance. Creating a new tile with more efficient filters should improve performance. Performance monitoring can be disabled by an administrator."* Set the **Performance Monitor** switch to **On** to display the message when tiles load slowly. The Performance Monitor defaults to **Off**.

To delete a tile, click the **X** in the upper right corner.

To reposition a tile, drag it to a new location.

To add a tile:

1. Click the **Add Tile** button. Place up to six tiles on a dashboard. To add a tile to a dashboard that already has six, delete one first.
2. Select a tile from one of the tile libraries.

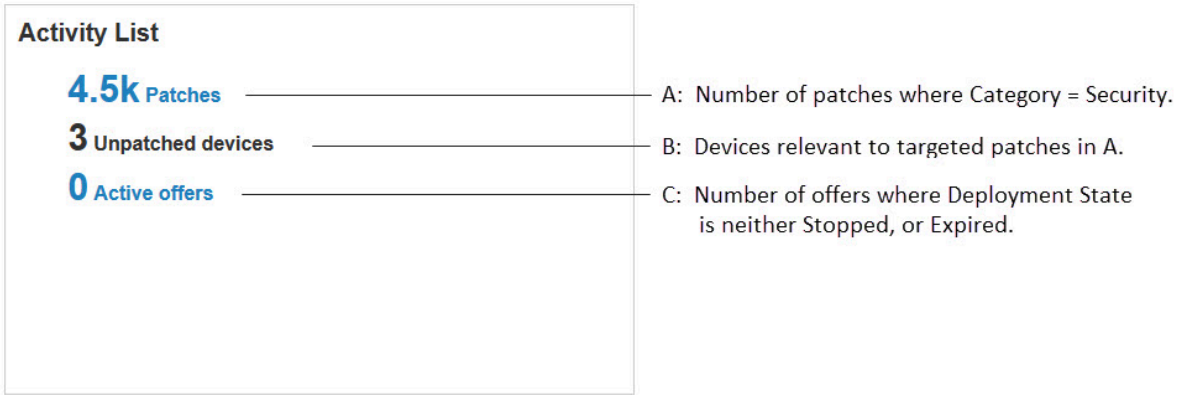
- To add a custom tile, click the **Add Custom Tiles** bar. For instructions on building custom tiles, see Working With Custom Tiles *(on page 46)*.
- To add a predefined tile, click the **Add From Tile Library** bar. Select a tile and drag it to the required location. For a description of each tile and its elements, see Working with Predefined Tiles *(on page 41)*.

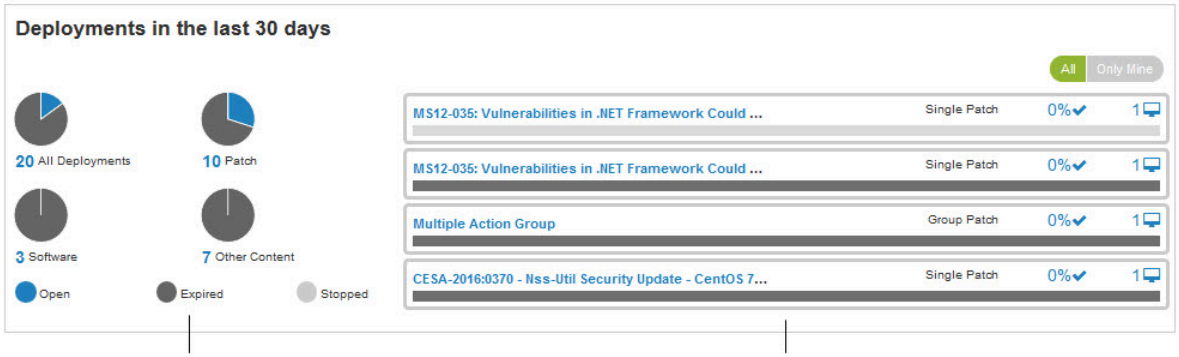
Working with Predefined Tiles

The tiles on the WebUI's default dashboards can be used in any combination.

To add a predefined tile to a dashboard:

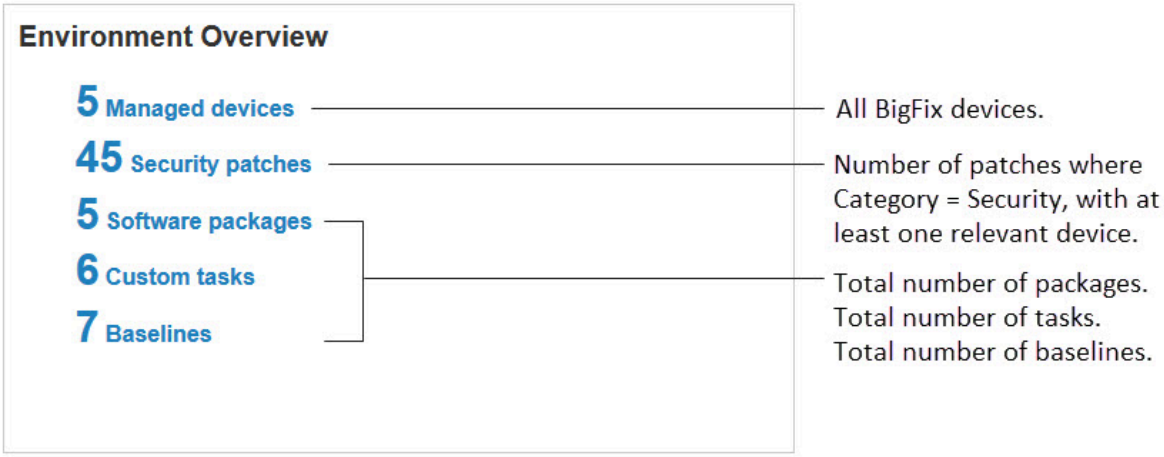
1. Click the **Edit Dashboard** button.
2. On the **Edit Dashboard** page, click **Add Tile**.
3. On the **Select Tile** page, click **Add From Tile Library**.
4. Click a tile to add it. The new tile is placed on the page below any existing tiles.
5. Drag tiles to arrange them on the page.
6. Click the **Save** button in the upper right corner of the page or **Cancel** to exit without making changes.

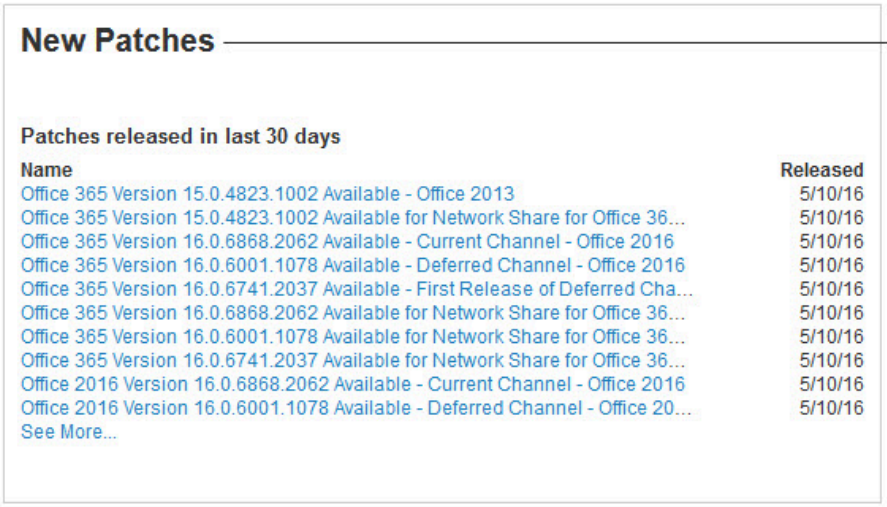


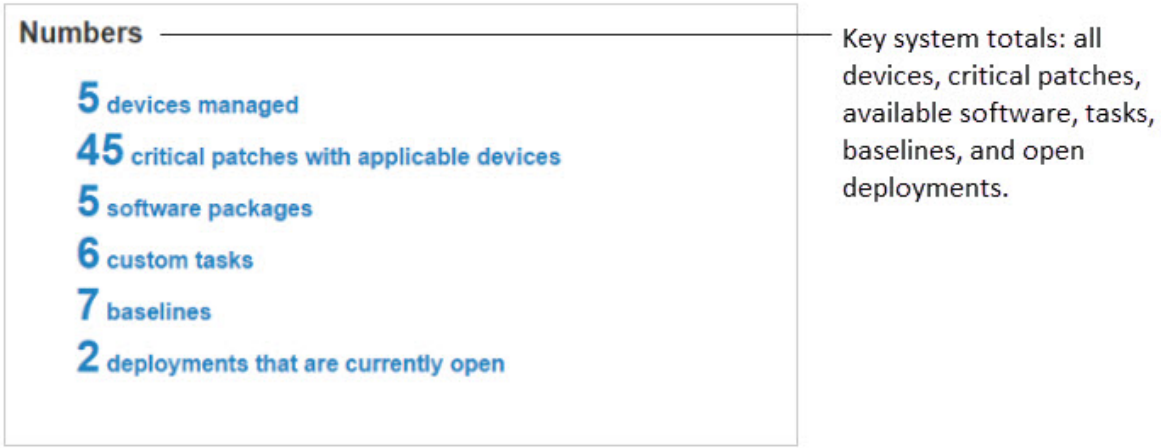


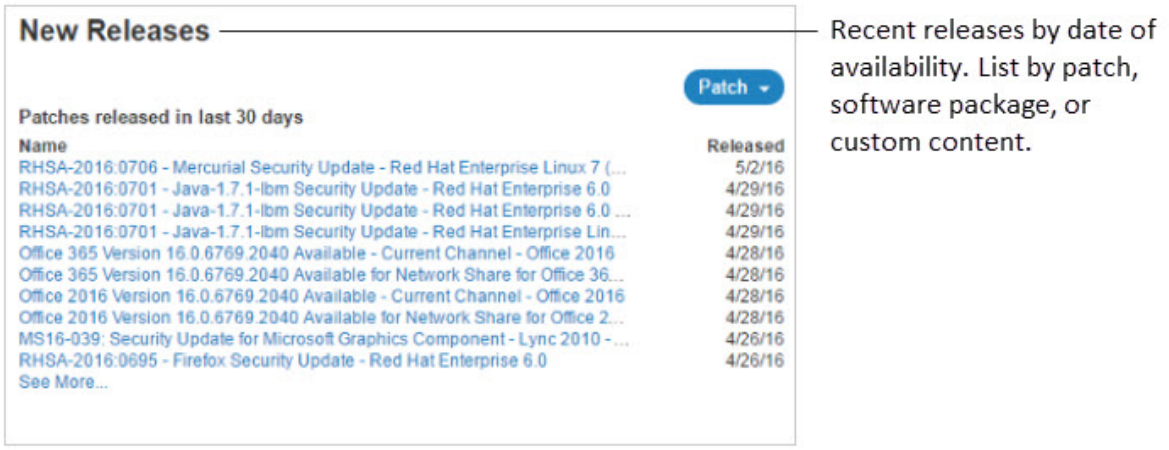
Deployment totals by type (all, patch, software, other) and their status (open, stopped, expired).

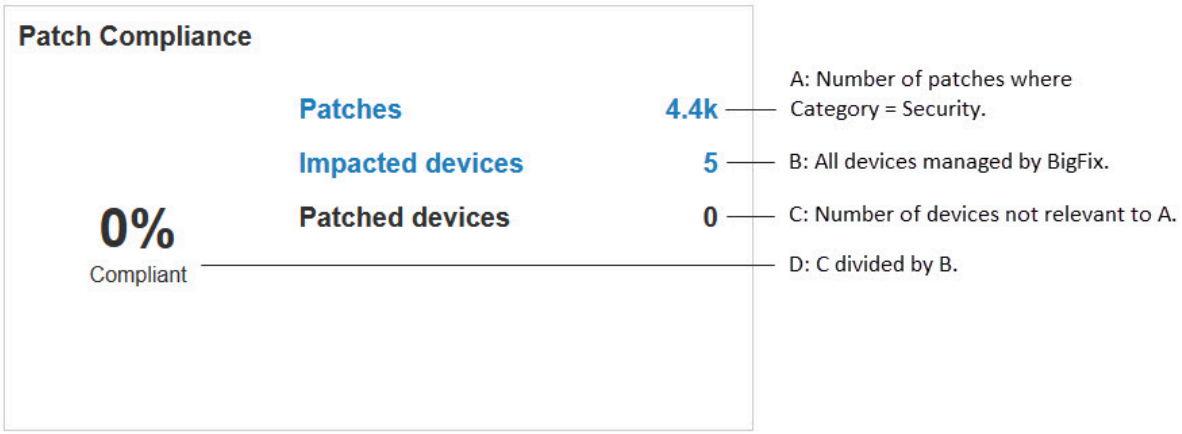
The last four deployments, with process status and device information.



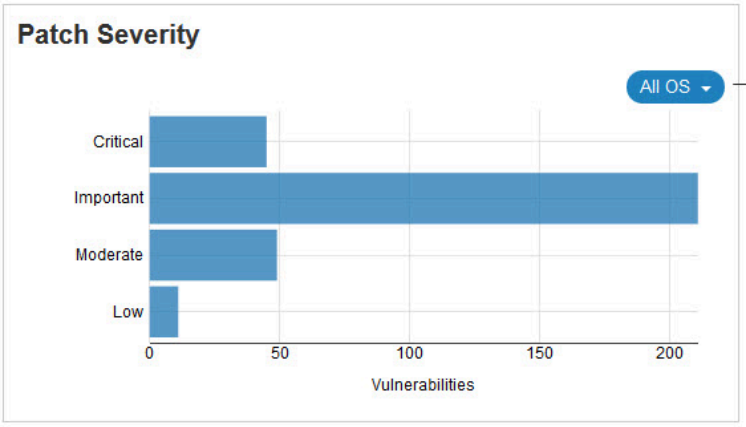

New Patches
Patches released in the past 30 days, and their release date.
Patches released in last 30 days
Name
Released
Office 365 Version 15.0.4823.1002 Available - Office 2013
5/10/16
Office 365 Version 15.0.4823.1002 Available for Network Share for Office 36...
5/10/16
Office 365 Version 16.0.6868.2062 Available - Current Channel - Office 2016
5/10/16
Office 365 Version 16.0.6001.1078 Available - Deferred Channel - Office 2016
5/10/16
Office 365 Version 16.0.6741.2037 Available - First Release of Deferred Cha...
5/10/16
Office 365 Version 16.0.6868.2062 Available for Network Share for Office 36...
5/10/16
Office 365 Version 16.0.6001.1078 Available for Network Share for Office 36...
5/10/16
Office 365 Version 16.0.6741.2037 Available for Network Share for Office 36...
5/10/16
Office 2016 Version 16.0.6868.2062 Available - Current Channel - Office 2016
5/10/16
Office 2016 Version 16.0.6001.1078 Available - Deferred Channel - Office 20...
5/10/16
See More...


Numbers
Key system totals: all devices, critical patches, available software, tasks, baselines, and open deployments.
5 devices managed
45 critical patches with applicable devices
5 software packages
6 custom tasks
7 baselines
2 deployments that are currently open





Note: In larger deployments, the Patch Compliance tile can be slow to load. If your deployment has over 10,000 endpoints, you might experience dashboard delays in loading data with this tile. Administrators building dashboards may want to refrain from using this tile.



For the selected Operating System: (All, OS X, Linux, Windows, Other)

The number of patches relevant to at least one device where Category = Severity and Severity value = Critical, Important, Moderate, or Low.

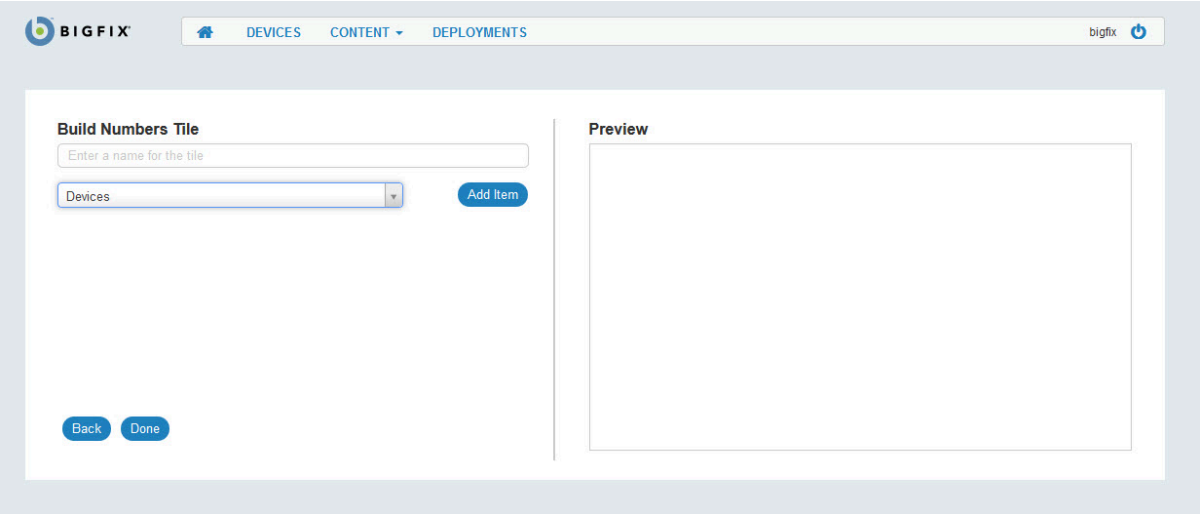
Recent deployments and device totals. List by patch, software package, or custom content.

Working With Custom Tiles

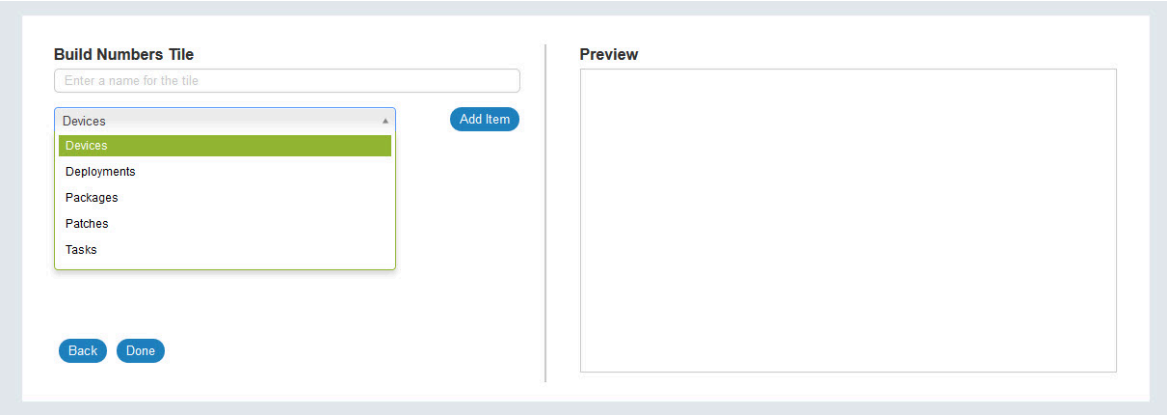
Use the **Build Tile** and **Define Filters** screens to create five types of custom tiles. The basic process for creating custom tiles is described here, and instructions for creating each type follow.

- Key Number
- Summary
- List
- Check
- Chart

Select a custom tile from the **Edit Dashboard** page to display the **Build Tile** page.

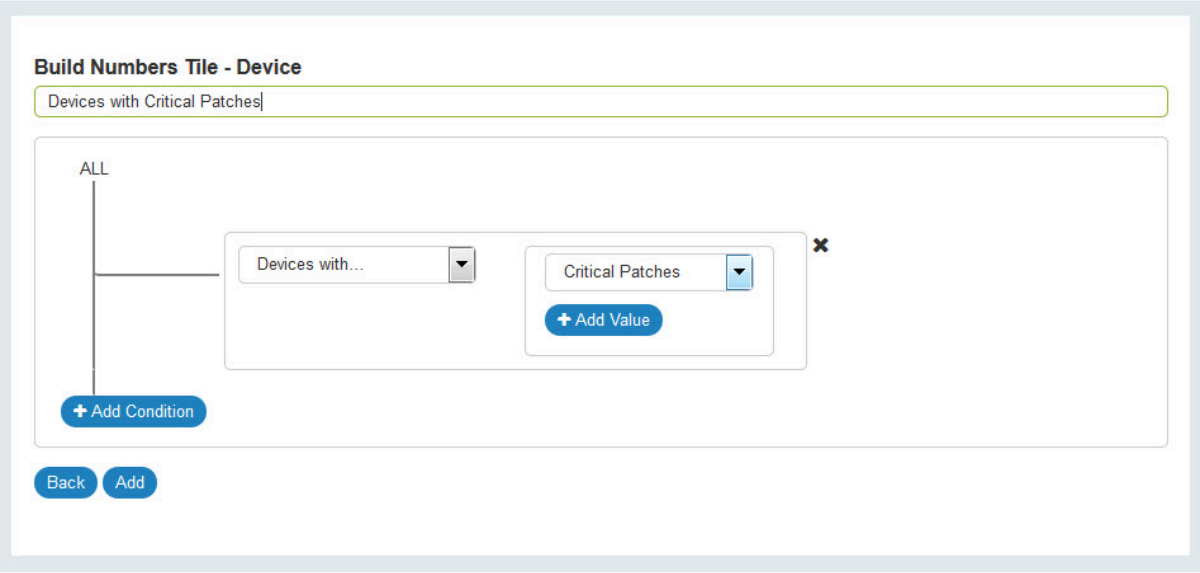


1. Entering a title for the tile. The Preview area on the right side of the page shows the tile-in-progress.
2. Select a BigFix object from the **Build Tile** drop-down list:
    - Devices
    - Deployments
    - Packages (Software)
    - Patches
    - Tasks (Custom Content)

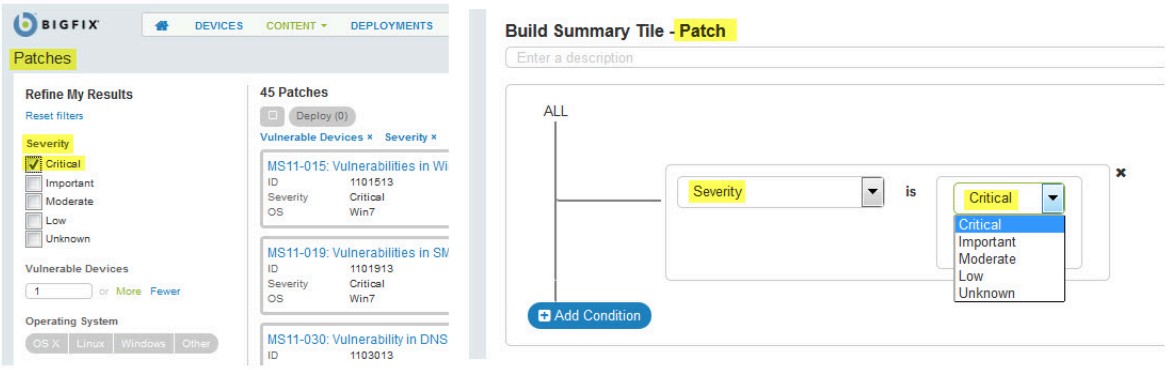


3. Click **Add Item** to display the **Define Filters** page.

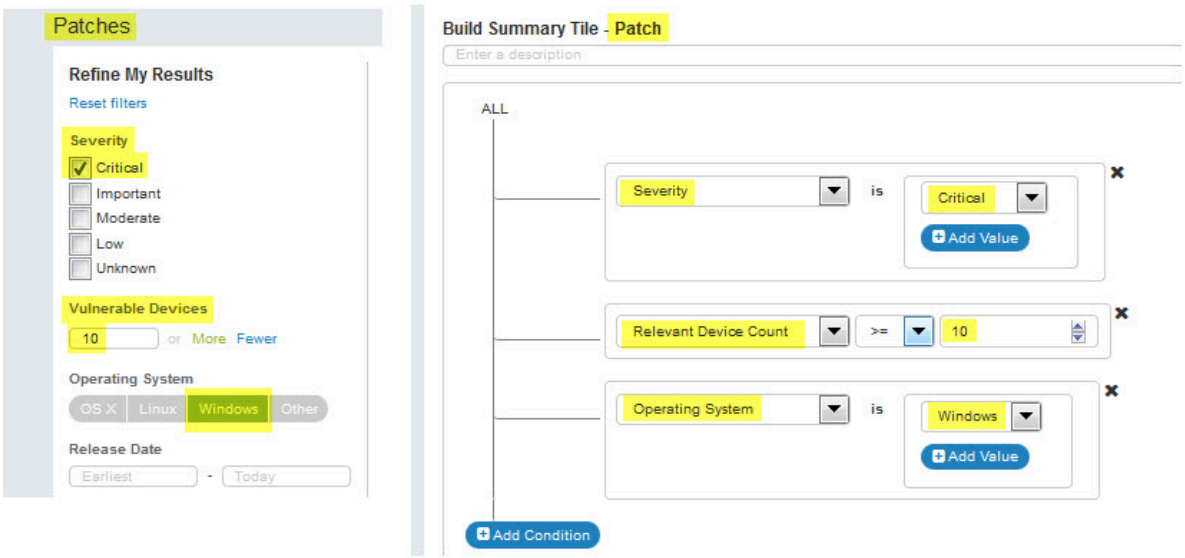
4. Use the **Define Filters** screen to select object-specific conditions and values.
    - To display a value for every instance of a top-level object (ALL devices), click the **Add** button, next to **Back**, at the lower left corner of the page.
    - To further refine the filter, for example, to return Devices with critical patches, click **Add Condition** and **Add Value**.



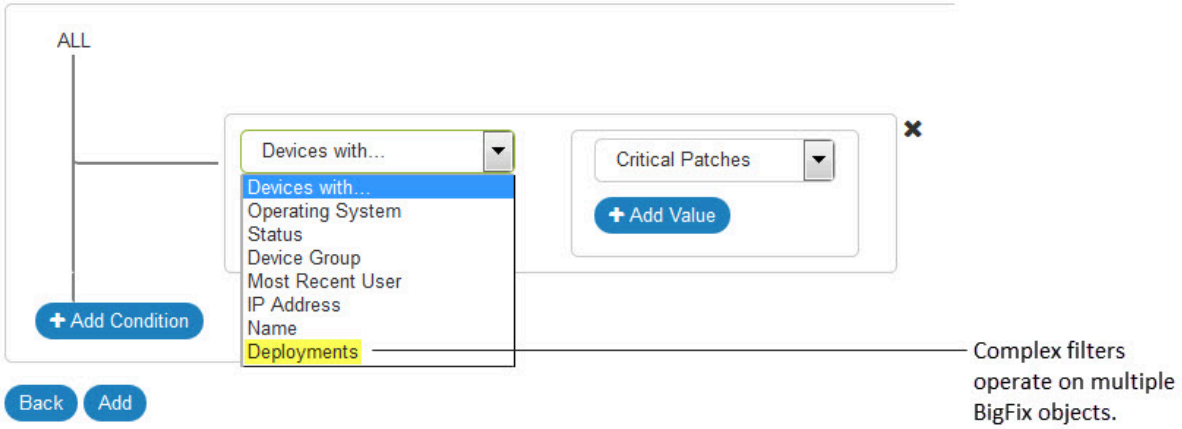
Working with conditions (object properties) and their values on a tile is analogous to working with filters on WebUI list screens. In the diagram below the image on the left shows a patch list filtered to show critical patches. On the right, the same operation is shown on the **Define Filter** page. Patch is the top-level object. Severity is the condition (object property), and Critical is the Severity value.



The next example illustrates the use of multiple filters. On the left: critical patches with 10 or more vulnerable devices on Windows machines. On the right: the same operation in a tile filter.



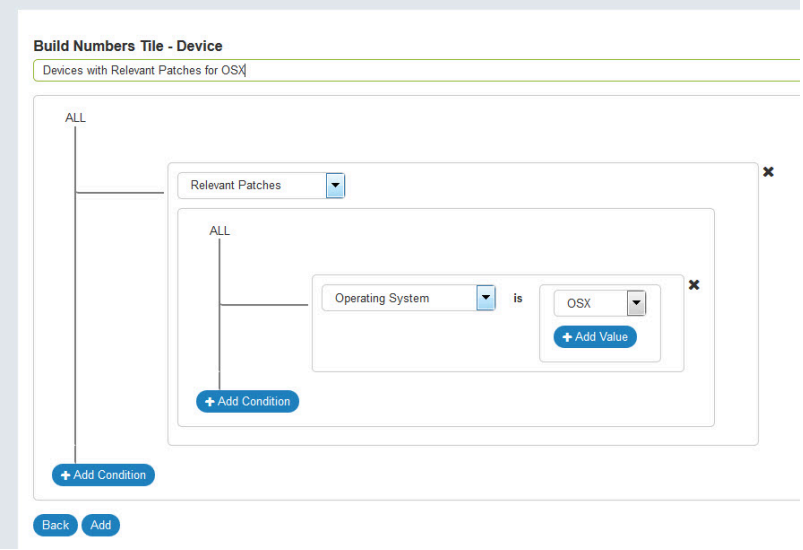
You can display data on a tile based on more than one high-level object using a complex filter. Complex filters appear at the end of an object's Condition list.



The complex filters for each object:

- Devices: Deployments
- Deployments: Targeted Devices, Source Tasks, Source Packages, Source Patches.
- Packages (Software): Deployments
- Patches: Deployments
- Tasks (Custom Content): Deployments, Targeted Devices.

In a complex filter the condition box is nested inside the top-level object.



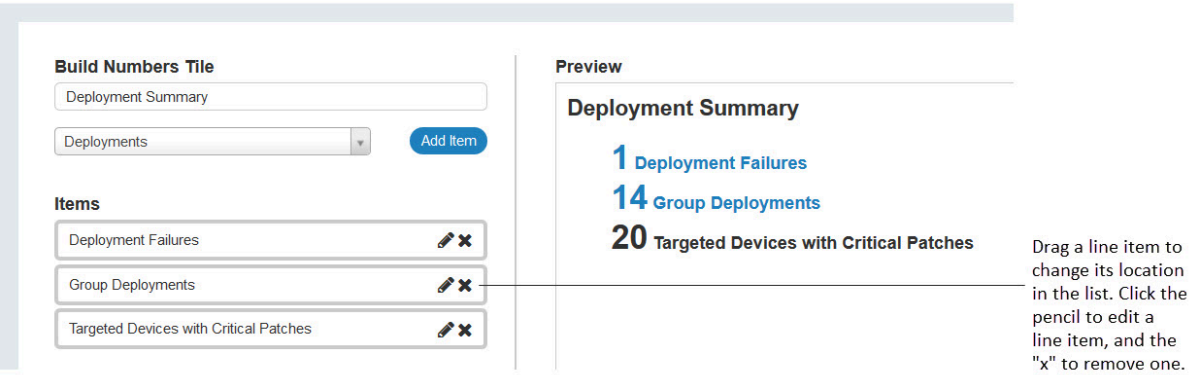
A basic understanding of how complex filters are processed will help you use them effectively.

1. A query is performed on each top-level object: some combination of Devices, Patches, Software Packages, Tasks, and Deployments. Every instance of each condition specified is found.
2. A set intersection on the results of both queries is created using an identifier common to both, and the results are returned to you. For example, a complex filter that involves devices creates a list of Device IDs that meet the conditions specified for each object. The set of Device IDs common to both lists is returned.

Examples of efficient complex filters include:

- How many Windows 7 machines are vulnerable to the critical patches released by Microsoft in the last 5 days?
- How many actions has the operator *"Dexter"* taken against devices in the device group *"Watson"* in the last 10 days?
- How many Adobe software package installations failed between May 1, 2016 and May 31, 2016?"

Tile Editing Tips



- On the **Build Tile** page, drag a line item to change its order in the **Items** list. Click the **X** to delete it.
- Click the pencil icon to edit a line item.
- The **Define Filters** page prevents you from accidentally selecting the same condition twice (they are inactive in subsequent drop-down lists).
- Tile results that are derived from complex filters are not clickable (hyper-linked to related data).
- Filters that are concise and limited in scope run more efficiently. Broad, general filters that return large data sets take longer and use more resources. Performance is not static, and various factors can influence it, including hardware changes, changes in the number of endpoints, and the amount of data an operator has access to.
- If a complex filter returns unexpected results, check for:
    - An empty set. If one of the filters returns 0 (for example, because you did not specify a condition), any intersection with that set will also return 0.
    - A very large set. If one of the filters returns every instance in the set, for example, all devices that have an applicable patch, the results will contain all instances. While accurate, they might be so broad as to be meaningless.

Create a Key Numbers Tile

Use key numbers tile to display the total count of every item that satisfies your conditions.

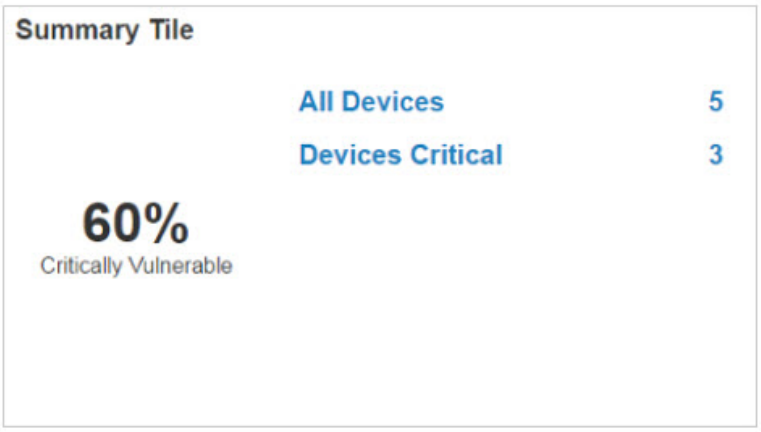
To create a key numbers tile:

1. From the **Overview** page, select **Edit Dashboard** > **Add Tile** > **Add Custom Tiles**.
2. Select List.
3. Enter a name for your tile.
4. Select an item (BigFix object) from the drop-down list, and click **Add Item**.
5. Enter a description for this line item on the tile.
6. Specify data conditions and values (filter criteria).
    a. Click **Add Condition**.
        i. Select a condition from the drop-down list.
        ii. Select a condition value. Click **Add Value** again to further refine your conditions.
        iii. Use the **Add Condition** and **Add Value** buttons to specify more conditions as required.
    b. To include every instance of an object (for example, ALL Software Packages), proceed to Step 7.
7. Click **Add** to add this line item to your tile and return to the **Build Tile** page. Or click **Back** to exit without saving.

8. Repeat Steps 4 – 7 to create up to five more line items for the tile. Check the **Preview** pane to see how your tile looks as you build. Drag and drop line items to rearrange them, or click the **X** to delete a line item.
9. Click **Done**. On the **Edit Dashboard** page, move the new tile to the place you want it on the dashboard.

Create a Summary Tile

Use summary tile to express an item as a percentage of another.



To create a summary tile:

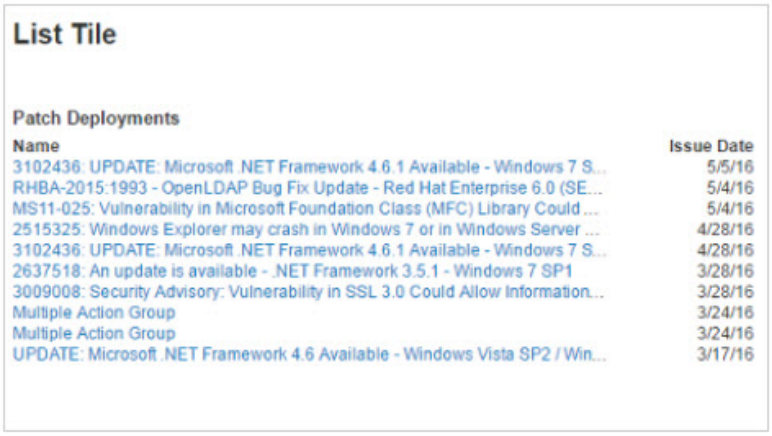
1. From the **Overview** page, select **Edit Dashboard** > **Add Tile** > **Add Custom Tiles**.
2. Select Summary.
3. Enter a name for your tile.
4. Select an item (BigFix object) from the drop-down list, and click **Add Item**.
5. Enter a description for this line item on the tile.
6. Specify data conditions and values (filter criteria).

a. Click **Add Condition**.
    i. Select a condition from the drop-down list.
    ii. Select a condition value. Click **Add Value** again to further refine your conditions.
    iii. Use the **Add Condition** and **Add Value** buttons to specify more conditions as required.
b. To include every instance of an object (for example, ALL Software Packages), proceed to Step 7.

7. Click **Add** to add this line item to your tile and return to the **Build Tile** page. Or click **Back** to exit without saving.
8. Repeat Steps 4 – 7 to create up to five more line items for the tile. Check the **Preview** pane to see how your tile looks as you build. Drag and drop line items to rearrange them, or click the **X** to delete a line item.
9. Define a summary for the tile. Using the drop-down lists, select two line items to express one as a percentage of the other. For example, a percentage of all devices with patches that are critical. Enter a description for your summary.
10. Click **Done**. On the **Edit Dashboard** page, move the new tile to the place you want it on the dashboard.

Create a List Tile

Use list tile to list items that satisfy your conditions.

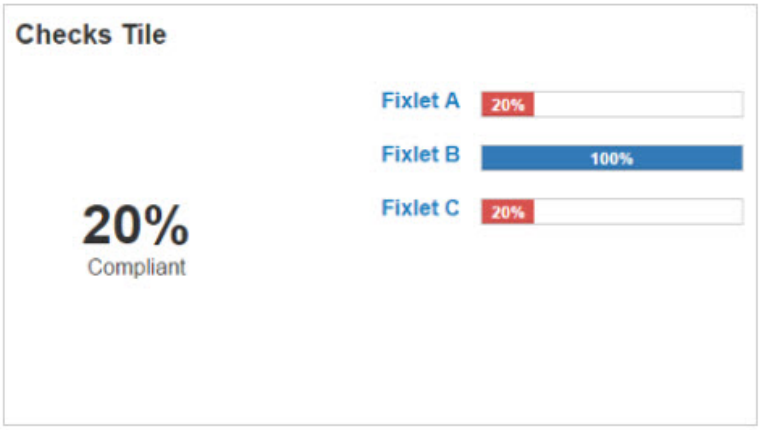


To create a list tile:

1. From the **Overview** page, select **Edit Dashboard** > **Add Tile** > **Add Custom Tiles**.
2. Select List.
3. Enter a name for your tile.
4. Select an item (BigFix object) from the drop-down list, and click **Add Item**.
5. Enter a description for the list.
6. Specify data conditions and values (filter criteria).
    a. Click **Add Condition**.
        i. Select a condition from the drop-down list.
        ii. Select a condition value. Click **Add Value** again to further refine your conditions.
        iii. Use the **Add Condition** and **Add Value** buttons to specify more conditions as required.
    b. To include every instance of an object (for example, ALL Software Packages), proceed to Step 7.
7. In the field **Sort the list by**, select a sort option.
8. Click **Add** to add the list to your tile and return to the **Build Tile** page. Or click **Back** to exit without saving.
9. Repeat Steps 4 – 8 to create more lists for this tile as required. To preview a tile with multiple lists, use the button in the **Preview** pane to select the list you want to see. A similar control is used to select between multiple lists in the completed tile.
10. Click **Done**. On the **Edit Dashboard** page, move the new tile to the place you want it on the dashboard.

Create a Checks Tile

Use checks tile to track device compliance for specific patches and custom content (tasks and baselines).



Percentages for each bar are calculated by dividing the number of unique non-relevant devices by the total number of devices. The tile total is calculated by dividing the number of unique non-relevant devices by the total number of devices for all line items on the tile. For example, in the sample tile pictured, 20% of all devices are compliant with Fixlets A, B, and C.

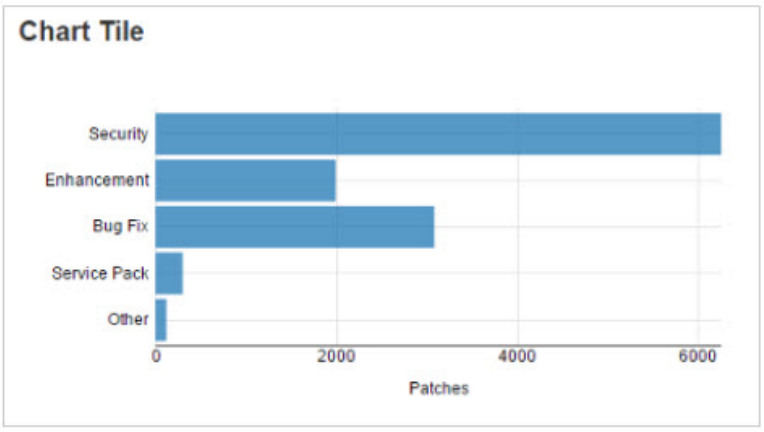
To create a checks tile:

1. From the **Overview** page, select **Edit Dashboard** > **Add Tile** > **Add Custom Tiles**.
2. Select Checks.
3. Enter a name for your tile.
4. Select *"Patches"* or *"Custom Items"* from the drop-down list, and click **Add Item**.
5. Enter a label for this line item on the tile.
6. Select a compliance threshold value for this item. Expressed as a percentage, compliance rates equal to or above the threshold are shown on the tile in blue. Compliance rates below the threshold value are shown on the tile in red. The default is 80 percent.
7. Hover the mouse over a patch or task name to display the **Select** button. Click **Select** to add a compliance line item to the tile. To find a specific patch, task, or baseline, enter its name in the **Search** box. Click a name in the list to open its document in a separate browser window.

8. Repeat Steps 4 – 7 to add up to 5 more compliance line items to the tile. Check the **Preview** pane to see check tile design as you work. On the Build Tile page, drag compliance line items to arrange them, or click the **X** to delete a line item.
9. Click **Done**. On the **Edit Dashboard** page, move the new tile to the place you want it on the dashboard.

Create a Chart Tile

Use chart tile to visually represent data of various components.



When you work with bar charts on the **Define Filters** page, start by gathering the data for your chart by using the **Add Condition** and **Add Value** buttons. Then, use the fields in the **Set Bars** pane to visually represent the components of that data. The **Create chart bars based on** field prevents you from inadvertently duplicating the conditions used in the filter by disabling them in the drop-down list.

To create a bar chart:

1. From the **Overview** page, select **Edit Dashboard** > **Add Tile** > **Add Custom Tiles**.
2. Select Chart.
3. Enter a name for your tile.
4. Select an item (BigFix object) from the drop-down list, and click **Set Bars**.

5. Specify the data conditions and values (filter criteria) for the chart.
    a. Click **Add Condition**.
        i. Select a condition from the drop-down list.
        ii. Select a condition value. Click **Add Value** again to further refine your conditions.
        iii. Use the **Add Condition** and **Add Value** buttons to specify more conditions as required.
    b. To include every instance of an object (for example, ALL Software Packages), proceed to Step 6.
6. In the **Set Bars** pane, select a category for your chart from the **Create chart bars based on** drop-down list. For example, categories for patches include *"Severity"*, *"Operating System"*, *"Issue Date"*, *"Category"*, and *"Name or ID"*.
7. Click the **Add Bar** button to create bars for the values in that category. For example, in a chart that shows patch severity, make bars for *"Critical"*, *"Important"*, *"Moderate"*, *"Low"*, and *"Unknown"*. Type the bar's name in the field to the right of its value to label it. To delete a bar, click the **X**.
    - Bar names must be unique.
    - To specify a date range, click in the bar field to display a calendar and select start and end dates.
    - When you enter values for *"Issued By"*, type the operator's BigFix user name.
8. Click **Add** to add the chart to the tile and return to the **Build Tile** page. Or click **Back** to exit without saving.
9. On the **Build Tile** page, drag the bars to rearrange them, or click the **X** to delete a bar. Check the **Preview** pane to see your changes.
10. In the field below the tile title, type a description of the chart's X axis.
11. Click **Done**. On the **Edit Dashboard** page, move the new tile to the place you want it on the dashboard.

Chapter 8. Performance

This chapter provides an introduction to some tools for managing performance problems you might encounter with the WebUI. For a detailed discussion of BigFix and WebUI performance topics and tools, including planning, monitoring, and maintenance, see the *BigFix Capacity Planning Guide*.

For the best performance, install the WebUI service on a dedicated machine. Running BigFix services and the WebUI database on a single machine will slow response times.

Optimizing User Permissions

In the WebUI, if non-master operators have similar permissions, WebUI is able to take advantage of that fact and use shared values for caching (see section on Caching).

Specifically, if non-master operators have identical permissions with regards to:

- Visible sites
- Visible Computers
- Assigned Roles

Non-master operators are able to share caches. Thus, to optimize WebUI performance, best practice is that the deployments must have groups of non-master operators that have their permissions defined via groups and roles. Try to avoid assigning individual operators, individual site or computer permissions. Also, try to avoid having content be assigned to individual operator sites as much as possible.

Operator Performance

Use these techniques to minimize operator-related delays.

- Balance Operator Load - Concurrence, or the number of operators using the WebUI at the same time, can affect performance. Response times may slow when a large number of operators are all using the WebUI at once. This can be minimized this by scheduling operators effectively, and ensuring that you have sufficient system resources to support concurrent operator load. If an operator is experiencing slow

response times, taking a break and returning to the WebUI when system load decreases might help. If this becomes an ongoing problem, Operator and Role shaping can help.

- Shape Operator Access - You can decrease system load by managing operators' access to content and endpoints. Use the BigFix Operator and Role permissions to limit individual operators to specific content, specific endpoints, or both. For example, if an operator is only concerned with a specific set of endpoints, such as Windows endpoints, define their role accordingly. Shaping can significantly reduce processing overhead.
- Remove Extraneous Content - Removing unnecessary content can also reduce the load on the server.

Environment Upgrades

The *BigFix Capacity Planning Guide* provides guidelines for CPU allocation, CPU scaling, virtualization and many other aspects of system planning and maintenance to ensure the resources allocated to the WebUI are balanced and healthy. For example, use system monitoring to determine whether system stress is due to operator workloads, or inadequate resource allocation.

Database Management

Database maintenance is critical to WebUI health. See the *BigFix Capacity Planning Guide* for information and tools specific to your platform.

1. Backups - Backups are an established best practice for database recovery. Every BigFix installation should have suitable backup policies in place to address their recovery needs in the event of failure.
2. Database Reorganization - With constant use the information in a database can become widely distributed; tables and indexes fragment over time. Use your platform's reorganization tools to reclaim space ensure query efficiency.
3. Database Statistics - Database statistics ensure that the DBMS optimizer makes wise choices for database access plans. The BigFix databases feature cost based

optimizers that use database statistics to determine the most efficient way to run a query. If the statistics are not maintained properly, inefficient query plans will be created and WebUI performance will degrade. Use your platform's tools to maintain these statistics.

Caching

Caching is used to improve WebUI response times. Cached data is processed, stored, and refreshed at a specific interval.

(While most WebUI data appears in real time, a few WebUI counters, such as the number of applicable devices, require complex calculations.) Processing time goes up as device counts go up, and large deployments can be affected. The cached values are:

- Applicable Patch count on the Device list
- Applicable Device count on:
    - the Patch list
    - the Software Package list
    - the Custom Content list
    - Document Overviews for individual patch, software, and custom content.
- Open Deployment count on:
    - the Content list
    - the Custom Content list
    - the Patch list
- Deployment information on the device list

_WebUIAppEnv_SP_QUEUE_CONCURRENT The setting _WebUIAppEnv_SP_QUEUE_CONCURRENT also affects WebUI caching. It limits the number of stored procedures that run simultaneously per App in the background that update cache values while users are browsing the WebUI. The default value is 5.

Cached values are flagged. For example, the relevant patch count on the Device list may display a message, *"Last updated 4 minutes ago. Click here to see the most up-to-date data."* Refreshing the browser retrieves the latest data from the cache.

The default refresh interval is 10 minutes. This interval, also called the cache Time To Live (TTL) value, determines how often cache results are invalidated. Ten minutes is considered a good trade-off between cache freshness and response time impact.

To change the interval, use the client setting **_WebUIAppEnv_CACHE_TTL**. Modifying the TTL value requires significant understanding of system load and operator concurrency, and is only recommended for administrators willing to monitor and tune the configuration. Enter the wanted interval period in seconds. The default interval is 600; the minimum interval is 180 (3 minutes).

Increase the interval to establish longer periods between cache refreshes. Customers with large deployments and lots of activity can lengthen the interval for fewer refreshes and lower impact on system resources. Activities that change applicable counts will consume more resources. These include:

- Increasing the number of devices reporting in to BigFix.
- Intensive patching activities, for example, on Patch Tuesday.

Chapter 9. Log Locations

All WebUI logs are stored in one default location. Logs are stored on the WebUI Server in the following locations (unless changed by the server setting _WebUI_Logging_LogPath).

Windows Deployment

```
c:\Program Files (x86)\BigFix Enterprise\BES Server\WebUI\Logs\
```

Linux Deployment

```
//var/opt/BESServer/WebUI/Logs/
```

An additional log in the WebUI directory that contains startup information for the WebUI process.

```
service-wrapper.log
```

It is possible to change the location of where logs are written as well as alter the verbosity of the log files. These options can be performed by creating or editing several server settings as described in WebUI Server Settings *(on page 65)*. Note that these settings should not be altered under most circumstances and should be reserved for very specific situations.

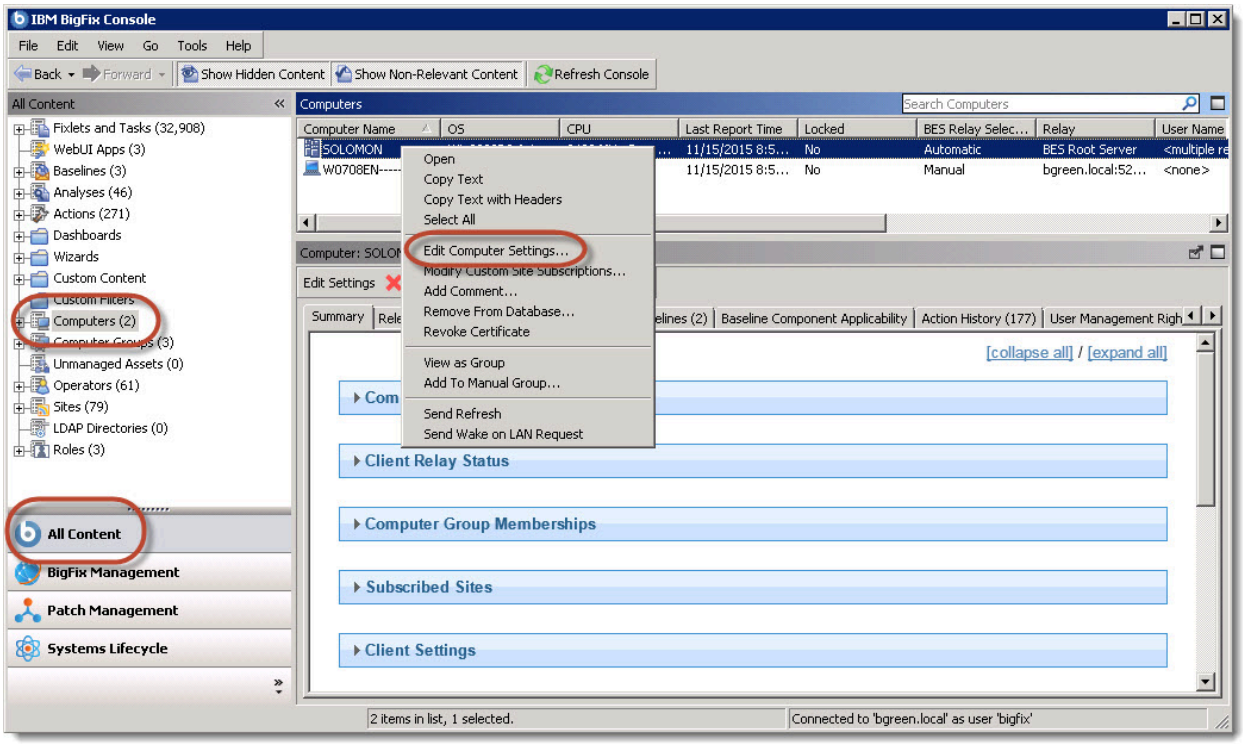
Chapter 10. WebUI Server Settings

Create or modify server settings on your WebUI server to control advanced aspects of the WebUI. These settings are for advanced users only and can be used to help troubleshoot problems or adjust behaviors to optimize performance. As a rule, these settings should not be changed unless specifically required; some of these settings can drastically affect the behavior and performance of your deployment.

The **BesRootServer** service must be restarted to apply any of these settings.

Access WebUI Server Settings

The WebUI Server Settings are accessed through the BigFix Console as a function of your WebUI server.



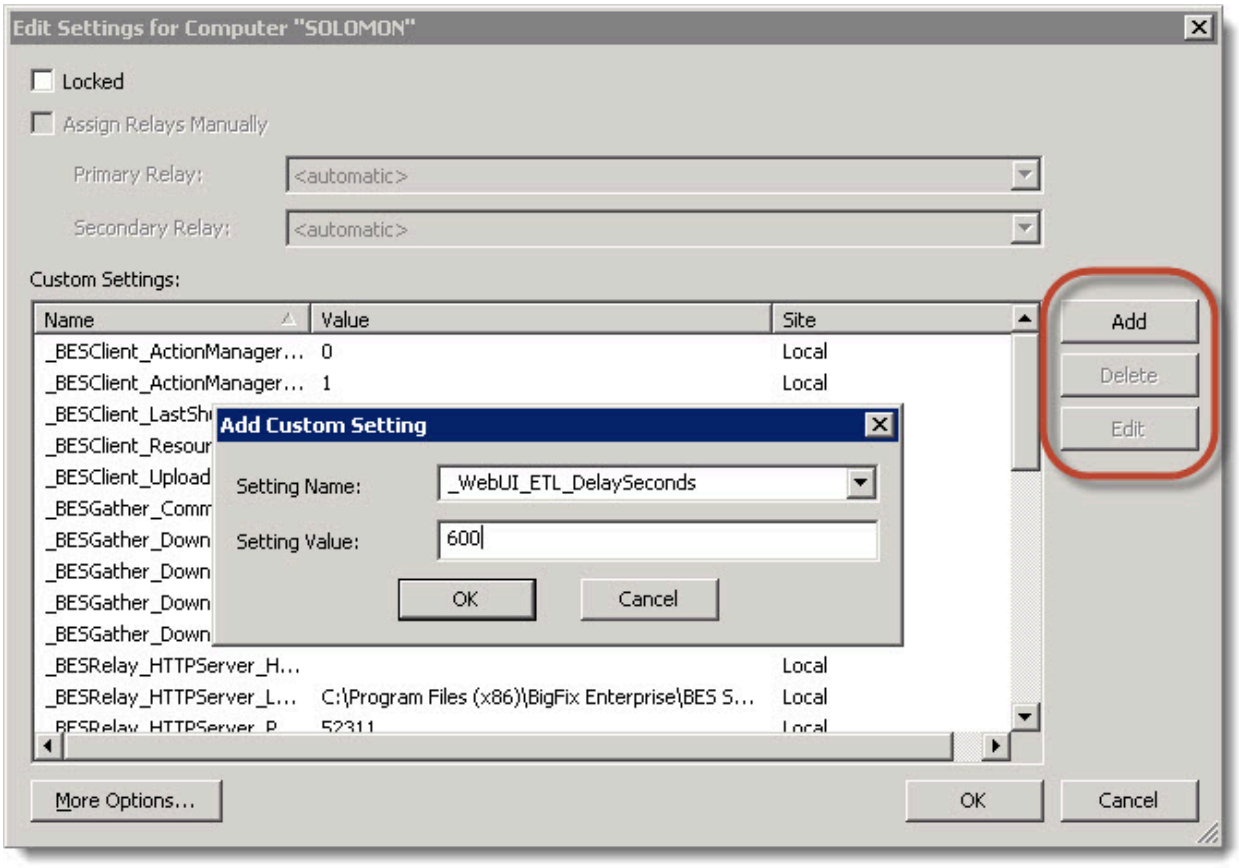
Locate your WebUI Server by navigating to **All Content > Computers**. Select your server computer and right click. Select **Edit Computer Settings** to display the **Edit Settings**

dialogue box. For detailed instructions on adding or editing server settings, see the BigFix Console Operator's Guide.

Server settings are written in the following format:

`<server_setting_name>=<value>`

Click **Add** or **Edit** to create or edit a new server setting. All server setting names begin with an underscore. Any WebUI setting that gets applied requires a WEBUI service restart.



Server Settings Definitions

WebUI Server settings

The WebUI Server settings are listed below. Any default settings are noted. If a setting has no default the parameter might not appear in the BigFix Console unless you create it.

Note: You must start the WebUI service for these settings to take effect.

_WebUIAppEnv_MSSQL_CXN_ENCRYPT A string value of `1` indicates that the user's MSSQL Server is configured to encrypt all traffic, either via *"Forced Encryption"* or a connection to an Azure Cloud virtual machine. Default is `0`.

_WebUIAppEnv_WEB_CIPHERS The set of web ciphers we start the WebUI with are detailed here: https://wiki.mozilla.org/Security/Server_Side_TLS. The cipher list must be colon-delimited. For example:

```
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256
-GCM-SHA384:
ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SH
A256:
DHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA384:ECDHE-R
SA-AES256-SHA256:
DHE-RSA-AES256-SHA256:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!SRP:
!CAMELLIA:
!kRSA:!DSS:!DSA
```

_WebUIAppEnv_APP_PORT Configures the port to be used by the WebUI. If you are going to use SAML, remember to set the *_WebUI_Monitor_Port* key of the BigFix server computer to the very same port.

_WebUIAppEnv_APP_PORT_MIN Sets the min port range to use for express apps (set by bfappmonitor).

_WebUIAppEnv_APP_PORT_MAX Sets the max port range to use for express apps (set by bfappmonitor).

_WebUIAppEnv_CACHE_TTL Value is in seconds. Datasync will invalidate things in WebUI.COMPUTED_FIXLET_COUNTS, WebUI.COMPUTED_DEVICE_COUNTS, Webui.SWD_COMPUTED_FIXLET_COUNTS, and Webui.CUSTOM_COMPUTED_FIXLET_COUNTS after the delta between when we cached and the current time exceeds AppEnv_CacheTTL in seconds. The value defaults to 600 if **_WebUIAppEnv_CACHE_TTL** is not set or the setting is malformed. The polling interval at

which Datasync checks to see if CACHE_TTL has elapsed is 60 seconds, so the minimum CACHE_TTL time is 60 seconds. Actual invalidation can occur anywhere from CACHE_TTL seconds up to CACHE_TTL+60 seconds. The minimum value is 180. Anything lower will default to 180.

_WebUIAppEnv_LOGIN_CACHE_TTL_HOURS Value is in hours. At login, it uses this value to determine whether it should repopulate caches or not. Default is 24 hours, minimum is 1 hour. There is no maximum value.

_WebUIAppEnv_NOTIFICATION_EXPIRATION_DAYS Enter the number of days after which the message sent through WebUI to target devices is expired; and hence, the message will be automatically deleted from the SSA Messages tab of the target device. The default value is 3 days.

_WebUIAppEnv_SAML_ONLY When set to 1, sets WebUI to run only in SAML only mode. Disables all other apps except for common and login to allow WebUI to configure SAML but not have anything else run.

_WebUIAppEnv_SAML_SSO_ENABLE When set to 1, will enable Web-based Single Sign-On (SSO) authentication method with SAML. Without the flag set, the default value is Disabled.

_WebUIAppEnv_SAML_AUTHNCONTEXT Defines the authentication context specified on the SAML exchange. In general, the allowable values are listed in section 3.4 of the SAML 2.0 specification (https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf), but the value must be allowed/understood by the SAML Identify Provider (IdP) being used. Most IdPs accept a subset of the values listed in the spec but might also have their own additional values. See your IdP documentation to confirm the required value for your environment. (For example, for ADFS, see https://msdn.microsoft.com/en-us/library/hh599318.aspx). If not set, `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` is used, which results in FORMS-based authentication requiring a user name and password to be entered. For two-factor authentication using smart cards, most IdPs require the use of `urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient`, or `urn:federation:authentication:windows`.

_WebUIAppEnv_QueryOnly When set to 1, sets WebUI to run in Query only mode. Disables all other apps except for common and login to allow WebUI to configure Query but not have anything else run.

_WebUIAppEnv_ENABLE_WEBUI_METRICS A value of 1 turns on logging for all of the webUI route requests. Default location in runapps: <app>/app/dev.out production/site: <app>/dev.out

_WebUIAppEnv_METRICS_PATH Specify path for when ENABLE_WEBUI_METRICS flag is enabled within which sql files and metrics details are generated. Default: <app>/app/dev.out in runapps or <app>/dev.out in production/site

_WebUIAppEnv_APP_UPDATE_ENABLE_AUTO If set to 1, WebUI Apps will auto update to the earliest versions in the pending sites cache. If set to 0, auto update is disabled. By default, auto updates are enabled.

_WebUIAppEnv_APP_UPDATE_DELAY_DAYS When a new site version is released, WebUI will wait this many days before it will replace the currently running version. Only applies when auto updates is enabled. Defaults to 0.

_WebUIAppEnv_LOGIN_SESSION_TIMEOUT_SECONDS Specifies the amount of time before a user is logged out of WebUI due to inactivity. The default timeout is 900 seconds (15 min).

_WebUIAppEnv_PLATFORM_HOST The value is set at install time using the host name specified in the masthead. Change this setting when deploying the WebUI against a non-primary server to configure the client setting on the WebUI host machine to connect to the secondary server.

_WebUI_Logging_Filter The value of this parameter is a regular expression that filters events to be logged. The default is `bf*error,bf:bfetl:debug,bf:bfapp:debug,bf:appmonitor:debug,bf:datasync:initialize:debug`. To enable verbose logging for all BigFix events, use `bf*`. To log all debug events, including third party applications, use simply `*`.

_WebUI_Logging_LogPath This value defines the full file path of the service app log. It also defines the directory in which all other logs will be written. The default value is *`<server_dir>/WebUI/logs/service-app.log`*. If the value is changed to `<server_dir>/bananas/fruit.log` for example, the service app log will be named `fruit.log`. However,

all other logs will retain their default names, but they will be written in `<service_dir>/bananas/`. Note that it is not possible to define the names of any logs except the service app log.

_WebUI_Logging_LogMaxSize Defines the maximum size of each log file in bytes. The default is 5,242,880 or 5 MB (5*1024*1024). When a log file exceeds the limit set here, a second log file is created. This continues until 10 log files have been created, at which point, the first log file is overridden. Therefore the maximum log file size for each log is ten times the value defined here. Note that, depending on usage, log files for each WebUI Application may be written at very different rates. This parameter defines the size of all log files.

_WebUI_HTTPS_Port This parameter defines the port used for HTTPS. The default is 443. This parameter is written by Fixlet 2252 during WebUI Enablement. Fixlet 2250 can be used to change this value at any time.

_WebUI_Redirect_Port This parameter defines the HTTP port used by WebUI if port 80 is not used. This setting does not exist by default. If a port other than 80 is required, this parameter must be defined in conjunction with **_WebUI_Redirect_Enable.** When Fixlets 2252 and 2250 define a port other than 80, this parameter is defined and enabled.

_WebUI_Redirect_Enable Controls HTTP port access. Use this setting if you don't want to redirect to the https port. The setting does not exist by default, allowing HTTP port access. To disable HTTP port access, the setting value must equal 0. This parameter works in conjunction with **_WebUI_Redirect_Port** setting.

_BESRelay_WebUISiteGather_IntervalMinutes Defines how often the WebUI Server gathers sites published by HCL. As the title suggests, this variable is an integer representing minutes between site updates. The default is 5.

_BESRelay_WebUISiteGather_Schedule Sets repeating times where the WebUI Server gathers sites published by HCL and overrides the setting in **_BESRelay_WebUISiteGather_IntervalMinutes**. It is best practice to change the interval minutes to the default of 5 if you have changed it previously. Enter comma-separated values in the following case-sensitive format `<Day>:<hh:mm>` where `<Day> = Mon, Tue, Wed, Thu, Fri, Sat, or Sun`. `<hh:mm>` is in 24 hour clock format. For example, the following value will schedule site updates every Sunday at 9am, Saturday at noon, and Friday at 10:30 PM: `_BESRelay_WebUISiteGather_Schedule=Sun09:00,Sat12:00,Fri22:30`

_WebUI_HTTPS_StrictTransportSecurity This setting prevents browsers from connecting to the WebUI using HTTP in favor of HTTPS. The default value is 0. Set this to 1 to enable this security feature.

_WebUIAppEnv_ENABLE_WEBUI_METRICS This setting can be enabled with a value of 1. The primary audience for this setting is WebUI developers, it has little value for administrators under most circumstances.

_WebUIAppEnv_APP_RESTART_DELAY_SECONDS This setting defines the number of seconds the App Monitor will wait before attempting to restart any applications that have stopped for any reason.

_WebUIAppEnv_DEPLOYMENT_DOC_REFRESH_RATE_MS This setting controls how frequently deployment status is refreshed on the deployment document. The default is 15000 ms (every 15 seconds).

_WebUIAppEnv_SP_QUEUE_CONCURRENT This setting sets a limit on the number of stored procedures per App the WebUI allows at any given time in the background (to improve performance). User logins cache requests bypass the queue and get executed immediately. The minimum and the default value is 5.

_WebUIAppEnv_LANG This client setting sets LANG environment variable in the WebUI node processes. This setting does not exist by default. When WebUI is installed on a Linux machine, the LANG environment variable is not set by default on node processes. As such, not all localized messages are displayed correctly. To set the LANG environment variable, this parameter must be defined and set to a preferred language; for example, **ja_JP.UTF-8** for Japanese.

_WebUIAppEnv_ENABLE_INLINE_REPORTING This client setting enables inline reporting feature. If WebUI is running on BigFix Platform versions less than 10, inline reporting feature is not enabled by default. To enable this feature, this parameter must be set to 1.

Chapter 11. SAML 2.0

BigFix supports SAML 2.0. SAML authentication is an application login mechanism that uses a configured Identity Provider (IdP) to authenticate users. While SAML authentication support is a feature of the BigFix platform, its configuration is implemented through the WebUI. The WebUI must be enabled in your deployment to take advantage of SAML. You can use the WebUI without setting up SAML, and use SAML without using the WebUI applications.

To activate SAML authentication without enabling the full set of WebUI components, start the WebUI in SAML-Only mode.

Enabling the WebUI in SAML-Only Mode

Starting the WebUI in SAML-Only mode allows you minimize resource consumption by activating the SAML authentication without enabling the full set of WebUI applications. In SAML-Only mode only those processes that are required to enable SAML authentication for the BigFix WebUI, the BigFix Web Reports, and the BigFix Console are created. All the other WebUI functions, other than the **SAML Administration** page, are unavailable.

Note: To use SAML with the full compliment of WebUI applications and functions do not use SAML-Only mode. Instead, use the standard enablement procedures explained in step 3 of the sequence listed below.

To start the WebUI in SAML-Only mode, use the computer setting `_WebUIAppEnv_SAML_ONLY` and the SAML Administration page. This is the procedure to follow, as BigFix Master Operator, to enable the WebUI in SAML-Only mode:

1. Open the BigFix Console, select the **All Contents** domain and then **Computers**. Click your WebUI server name and select **Edit Computer Settings**.
2. If not yet listed, add the computer setting `_WebUIAppEnv_SAML_ONLY` to the Settings list and set its value to `1`.
    a. From **Edit Settings**, click **Add** to open the **Add Custom Setting** dialog.
    b. In the **Setting Name** field type: `_WebUIAppEnv_SAML_ONLY`

c. In the **Setting Value** field type: `1`

d. Click **OK**.

Note: If the setting `_WebUIAppEnv_SAML_ONLY` is already present but set to `0` (disabled), change its value to `1`.

3. If not yet enabled, enable the WebUI as described in the Installation Procedure. If you already enabled the WebUI, restart the WebUI service to activate the changes.
4. For SAML to work correctly when you are installing the WebUI on a separate remote server, you must set the `_WebUI_AppServer_Hostname` key of the BigFix server computer to the hostname of the computer where the WebUI is installed.
5. Log in to the WebUI. Type your WebUI URL into a browser window to display the `/login` page. Once your credentials are authenticated, the SAML Administration page (`/administrator`) displays.
6. On the SAML Administration page, enter your SAML configuration settings, and click **Enable**.

Note: To enable SAML authentication for Web Reports, Web Reports must be enabled for SSL. (This is required whether WebUI is in standard or SAML-Only mode.)

7. Restart the BES Root Server, the Web Reports server, and the WebUI service to complete the process. SAML authentication is now enabled in SAML-Only mode for Web Reports, BigFix Console and WebUI.

After installing the WebUI, if you only want to switch from the full-WebUI to the SAML-Only mode, set the `_WebUIAppEnv_SAML_ONLY` setting to `1`, and then restart the BES Root Server and the WebUI service to make the change operational.

When either `_WebUiAppEnv_SAML_ONLY` is not present, or it is set to `0`, SAML-Only mode is not enabled.

For more information about the available settings affecting the WebUI configuration, see WebUI Server Settings *(on page 65)* for instructions.

Notes

- In SAML-Only mode, appending `/login` to your WebUI URL displays the standard WebUI login form.
- Logging in to the WebUI (using either SAML or the `/login` page) redirects users to the SAML Administration page. On this page Master Operators can configure SAML settings. Non Master Operators will see the “403 (Forbidden)" message, and will not be able to view or edit the SAML configuration.
- If a user attempts to manually access the `/` URL after logging in, they will see a blank WebUI dashboard. Only the **Home** and **Log Out** controls will be active. Logging out redirects the user to the Reauthenticate page, regardless of the method they used to log in. All other navigable WebUI URLs (except `/` and the SAML Administration page) return an "Access Forbidden" message.

Chapter 12. Troubleshooting

Read this section for information about any known issues using the WebUI application.

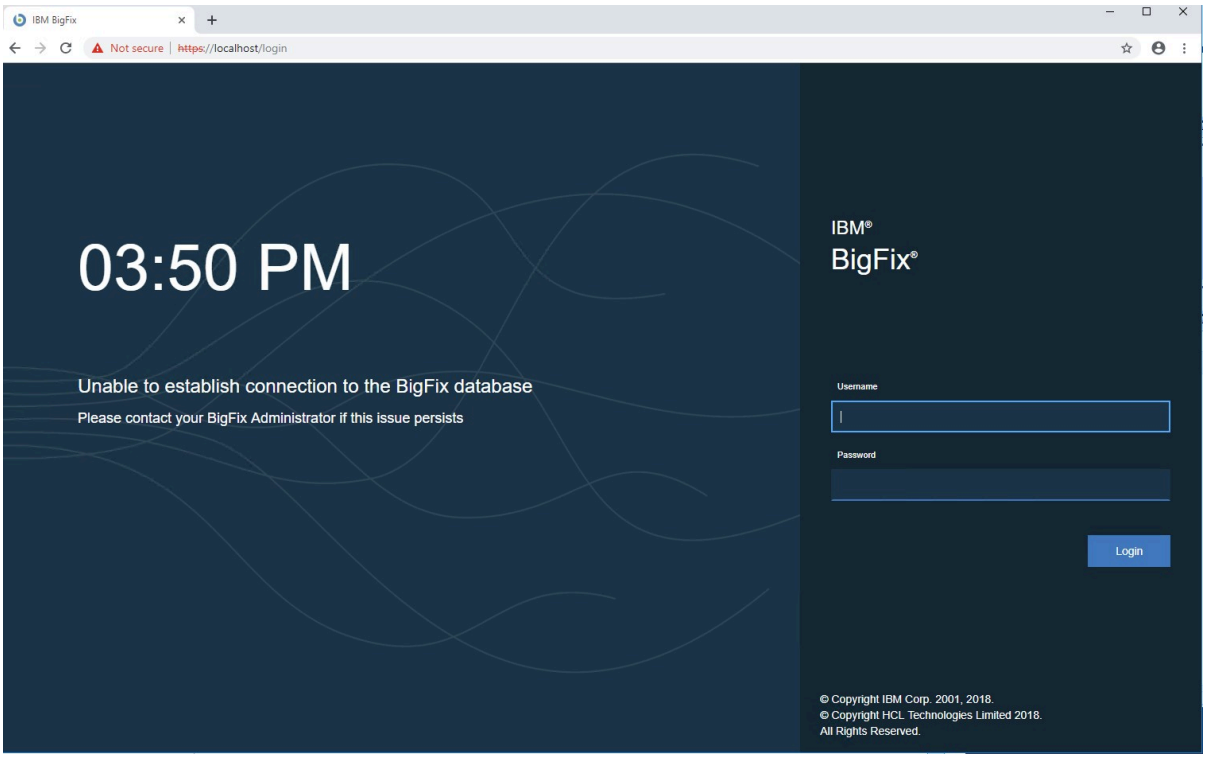
To help troubleshoot issues that operator might experience using the WebUI application, review the following troubleshooting tips:

Unable to establish connection to the BigFix Database

The WebUI application tries to connect to the BigFix Enterprise appropriately using the configuration details setup of the WebUI on the first install. Sometimes, communication can fail. Reasons include:

- If the database service is unreachable (the machine is off, firewall exception not granted).
- If the credentials used to communicate with the database is expired or changed.
- If the permissions for the user configured to communicate with the BigFix Enterprise gets revoked or changed.

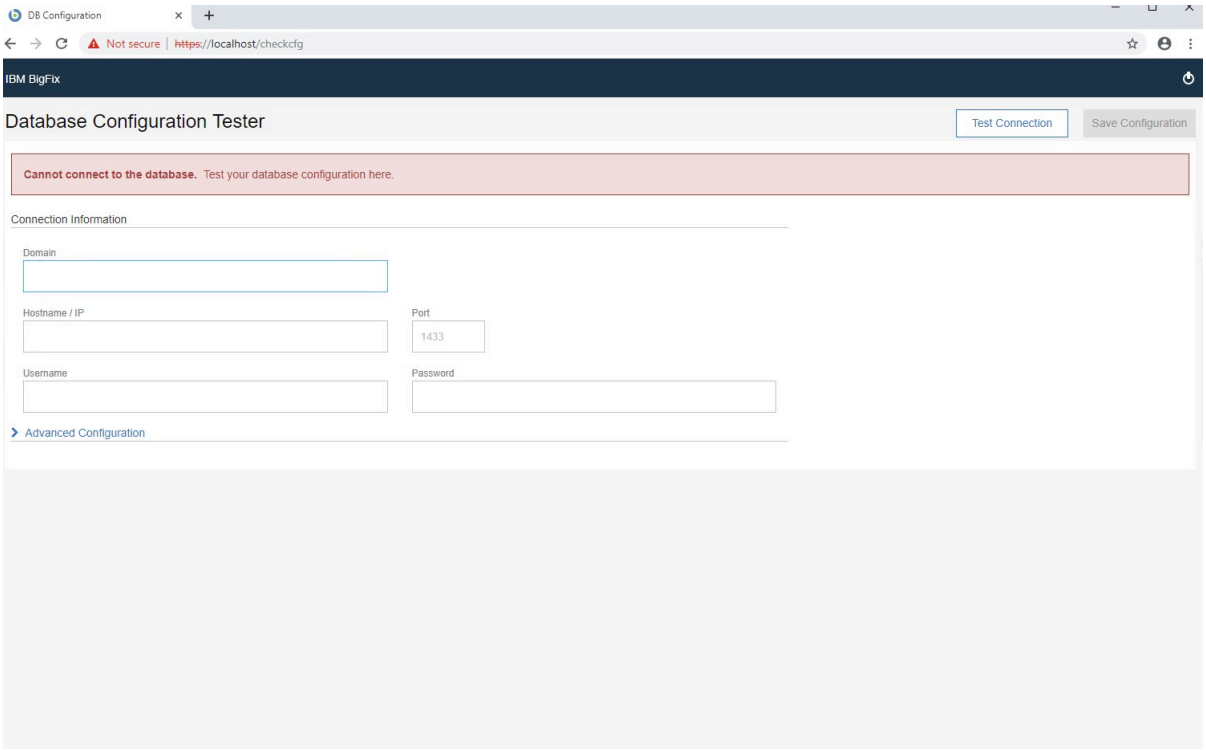
In cases of communication failure, the WebUI application will display the following message:



Note: If the WebUI is deployed on MSSQL, the operator will see the database configuration tester wizard. If the WebUI is deployed on DB2, the operator will not be able to see the database configuration tester wizard, and the operator must use BES Support Fixlet 2687 to resolve their database connectivity issues.

Important: The WebUI application allows master operators to authenticate the root server even if the communication fails. At this stage, the BigFix administrator (any Master Operator) needs to login to the WebUI application and reconfigure the WebUI. Non-master operators that attempt to log in will get an error message and will not be able to login to the WebUI until database connectivity is restored.

Once a master operator logs in, Database Configuration Tester screen appears:



Note: Master Operator can test the database configuration and save it without using the BigFix Thick Console.

After entering the relevant information, an operator can hit the **Test Connection** button to verify if the WebUI can communicate with BigFix Enterprise accurately.

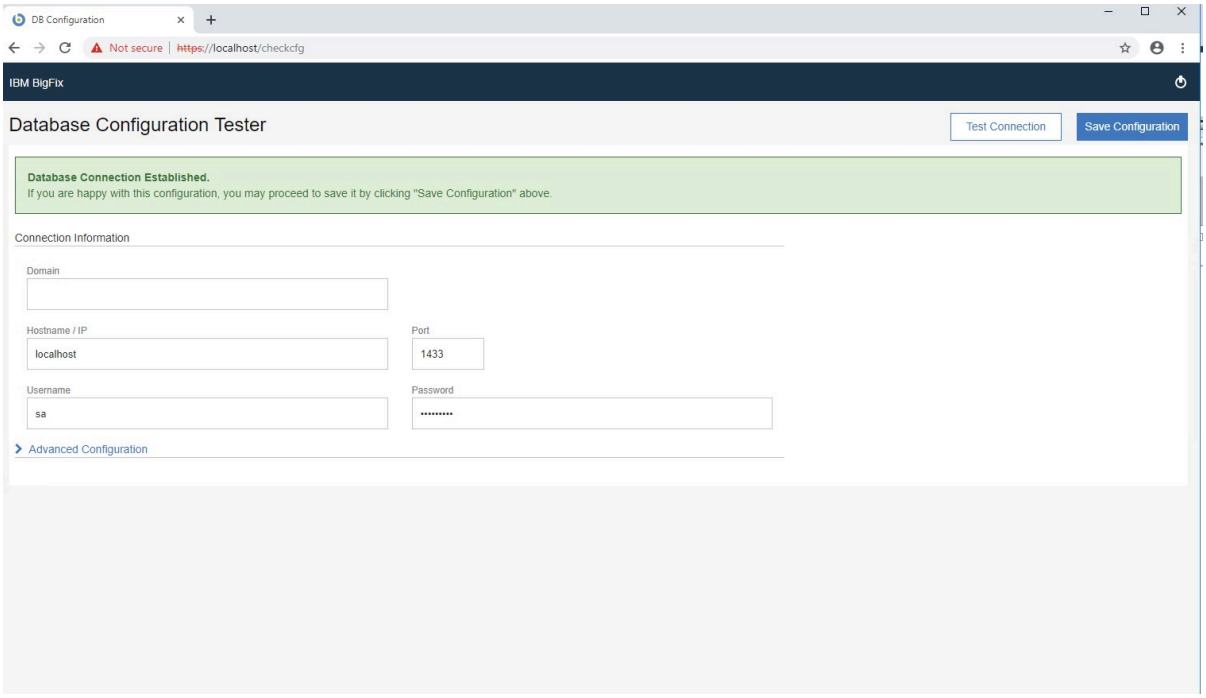
If the Test Connection returns with a failure message, check the following:

- The operator configured to communicate with the database has the right permissions to BigFix Enterprise. The WebUI operator must be able to:
  - Read and write to BigFix Enterprise.
  - Create and modify stored procedures in BigFix Enterprise.
  - Create and modify tables in BigFix Enterprise .
  - Create and modify indexes in BigFix Enterprise.
- Check whether the SQL Server is configured to force encryption on connections to BigFix Enterprise. If it is configured to force encryption, ensure that the **Encryption**

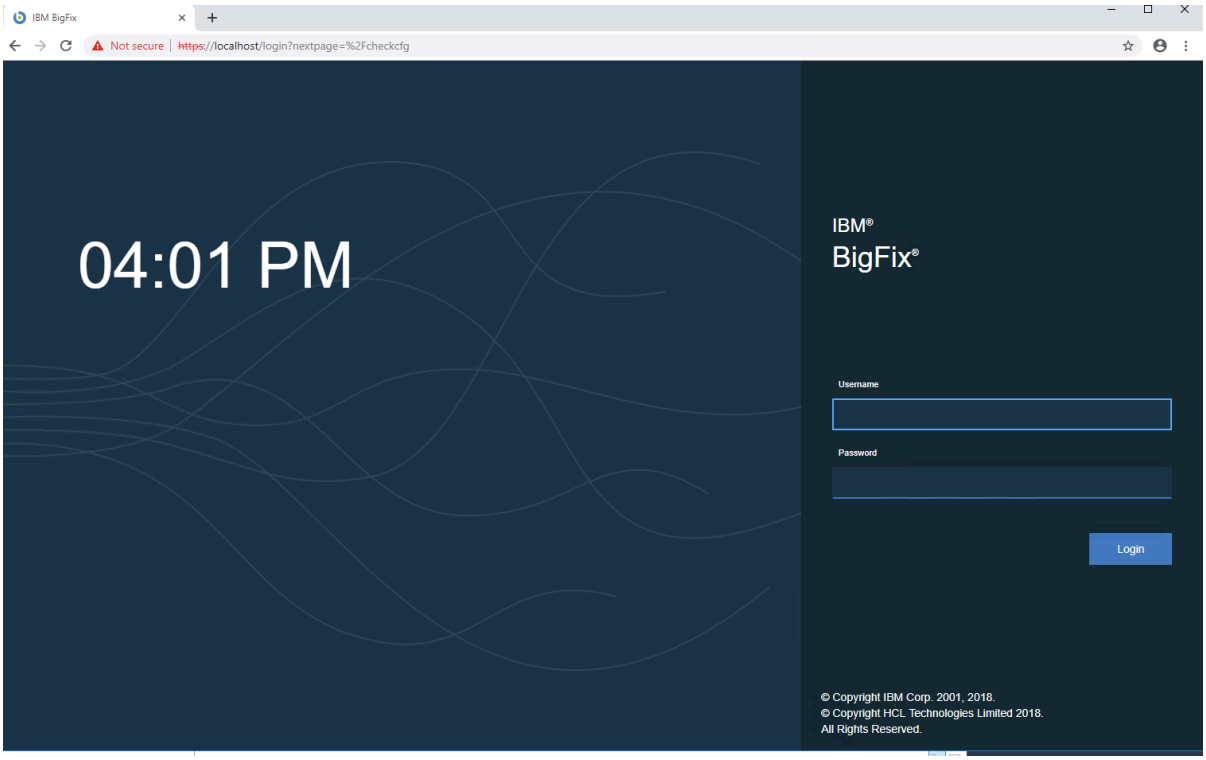
Enabled button is checked. (Encryption Enabled can be found in the Advanced Configuration section).

- If the MSSQL is installed in a non-default instance, make sure to enter the **Database Instance Name** in the configuration (Database Instance Name can be found in the Advanced Configuration).
- Check whether the configured operator is a local SQL operator or a domain user. If the domain user is necessary, ensure that **Domain** field is filled out correctly.

Upon testing the credentials, an operator can click the **Save Configuration** button to ensure that WebUI starts using the new set of credentials to communicate with the database.



The WebUI service must be restarted for the changes to take effect. The WebUI login screen must not display the error to operators, and operators must be able to resume the normal function of the application:


IBM BigFix
Not secure | https://localhost/login?nextpage=%2Fcheckcfg
04:01 PM
IBM®
BigFix®
Username
Password
Login
© Copyright IBM Corp. 2001, 2018.
© Copyright HCL Technologies Limited 2018.
All Rights Reserved.

Chapter 13. WebUI and Distributed Server Architecture (DSA)

Understand how to work with WebUI in Distributed Server Architecture (DSA).

Set up the environment for a smooth switch

If the WebUI server is directly attached to the BigFix Server:

- Set the DSA server as the Secondary Relay in WebUI computer client settings.

  When a failure on the primary BigFix server occurs and the WebUI client is unable to report, they use the secondary BigFix relay value during normal relay selection process to find and report to the secondary BigFix server.
- Set `_BESClient_RelaySelect_ResistFailureIntervalSeconds` to a low value. The setting `_BESClient_RelaySelect_ResistFailureIntervalSeconds` specified on the client system can have an impact on failover timing. Its value can range from 0 seconds to 6 hours, and it defines how many seconds the client ignores reporting failures before attempting to find another parent relay. The default value is 10 minutes. In case of a failover configuration, ensure that if defined, `_BESClient_RelaySelect_ResistFailureIntervalSeconds` is set to a low value.

If the WebUI server is attached to a Relay, ensure your environment has been set up following the instruction at Configuring relay failover

WebUI and DSA

If you are using DSA to provide redundancy and you have your WebUI installed on the primary server, when it fails, you will have to use the secondary server to install a new instance of the WebUI that connects to the secondary server.

When you deploy the WebUI against a non-primary server, configure the client setting on the WebUI host machine to connect to the secondary server using the WebUI server setting `_WebUIAppEnv_PLATFORM_HOST`. This prevents the WebUI instance from defaulting to using the host name specified in the masthead.

If the WebUI is installed on a separate server, there is no need to uninstall and reinstall it.

Follow these steps to properly switch the WebUI from the primary to the secondary Root Server:

1. Stop the WebUI server.
2. To make the chosen DSA server act as master server, assign `masterDatabaseServerID` to the DSA server ID you want to switch to. See Switching the master server on Linux systems.
3. On the WebUI Computer, change the setting `_WebUIAppEnv_PLATFORM_HOST` to point to the DSA server you want to switch to.
4. On the DSA server you are going to use as primary, use the BESAdmin tool to create new WebUI credentials and copy the new keys in the WebUI cert directory. See Additional administration commands.
5. Run fixlet `Deploy/Update WebUI Database Configuration` (ID 2687) to set the correct Database server for the WebUI, that is the Database server you are going to use after the switch.
6. Start the WebUI server.

When the failing DSA server will be back again, if you want to switch back both the DSA and WebUI configuration, repeat all the above steps and add the following between step #3 and step #4:

- On both the DSA servers (failing and current) revoke the old WebUI credentials using the `BESAdmin -revokewebuicredentials` command. See Additional administration commands.

Note: Multiple instances of the WebUI are not currently supported. If you are reinstalling the WebUI service on a machine, uninstall the WebUI service first.

DSA and SAML

BigFix supports SAML authentication in a DSA environment. In the event of a primary server failure, you will need to separately configure each BigFix instance you want to enable in SAML. For example, in Microsoft Active Directory Federation Services (ADFS), define SAML Assertion Consumer Endpoints for:

1. The primary WebUI server, the primary BES root server, and the primary Web Reports server (if you are using Web Reports).
2. The secondary WebUI server, the secondary BES root server, and the secondary Web Reports server (if you are using Web Reports).

Chapter 14. Supported Patch Sites

A subset of BigFix patch sites is supported in the WebUI. The supported patch sites are for the following operating systems:

- CentOS
- Debian
- Mac OS X
- Oracle Linux
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Ubuntu
- Windows

Future releases will include more patch sites.

Appendix A. Support

For more information about this product, see the following resources:

- Knowledge Center
- BigFix Support Center
- BigFix Support Portal
- BigFix Developer
- BigFix Wiki
- HCL BigFix Forum

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or

any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.