

**BigFix
Profile Management User's Guide V1.0**

Special notice

Before using this information and the product it supports, read the information in [Notices \(on page 25\)](#).

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Profile Management Overview.....	1
Operator permissions and associated profile actions.....	2
Chapter 2. Profile Management tasks.....	5
Profile compliance behavior.....	8
Profile attributes for Windows 10 devices.....	13
Profile properties for MAC OS X devices.....	17
Chapter 3. Troubleshooting profile deployments.....	22
Notices.....	25

Chapter 1. Profile Management Overview

BigFix Profile Management is a WebUI-based feature of BigFix Lifecycle.

Profile Management is referred to as the process of managing user personalization settings on a device. Typically the most sensitive settings to be managed are in the area of security. For example, administrators might define policies for password or passcode length and complexity, network access, storage management restrictions, permissions to run built-in or external applications. Additionally, they can enforce restrictions on specific user activities, registry key content, and other properties.

Organizations typically have several scenarios to consider when they deploy devices. In many organizations, both Bring Your Own (BYO) personal devices and Choose Your Own (CYO) company-owned devices are deployed. In both cases, the device must be registered with a system that can configure it with the required settings in compliance with the security requirements of the organization as a whole. Moreover, devices must also comply to specific role-based requirements of the employee and department.

BigFix Profile Management can deploy device configuration profiles based on the specific business needs and security requirements of an organization. Depending on the organizational structure and the specific employee roles, profiles can address the security requirements of the organization and ensure continuous compliance of all devices. Profile Management ensures a high degree of control and allows for flexibility in establishing different policies that depend on the type of device and who uses it. Security Administrators can define and implement policy settings on any corporate device that is registered to the BigFix server.

This feature provides Security Administrators profile management capabilities for Windows 10 and Mac OS devices.

Profile management terms

The following terms represent the core of the feature.

Profile

A Profile represents a set of security settings that you want to enforce on devices. Settings are grouped into four categories for user convenience. Each category corresponds to a tab in the profile page in the WeBUI. You can enforce the following categories:

Password//Passcode

Contains password or passcode requirements.

Device

Contains settings that restrict usage of hardware devices.

Application

Contains settings that limit application functions.

Restrictions

Contains settings that disable the use of specific applications or device features.

Save profile

Action that stores the profile in the Bigfix database and generates a Fixlet that checks the values set in the profile for relevance on devices for which this profile is not yet enforced.

Deploy profile

Creates an action that deploys the Fixlet associated to the Profile and which enables continuous enforcement of the configuration settings.

Supported Client Operating Systems


Profile Management is available in BigFix Lifecycle 9.5 and supports Windows 10 and MAC OS X 10.12 Sierra, available with BigFix Platform Version 9.5.3. For a list of supported Windows 10 Editions, see [Detailed system requirements](#).

Operator permissions and associated profile actions

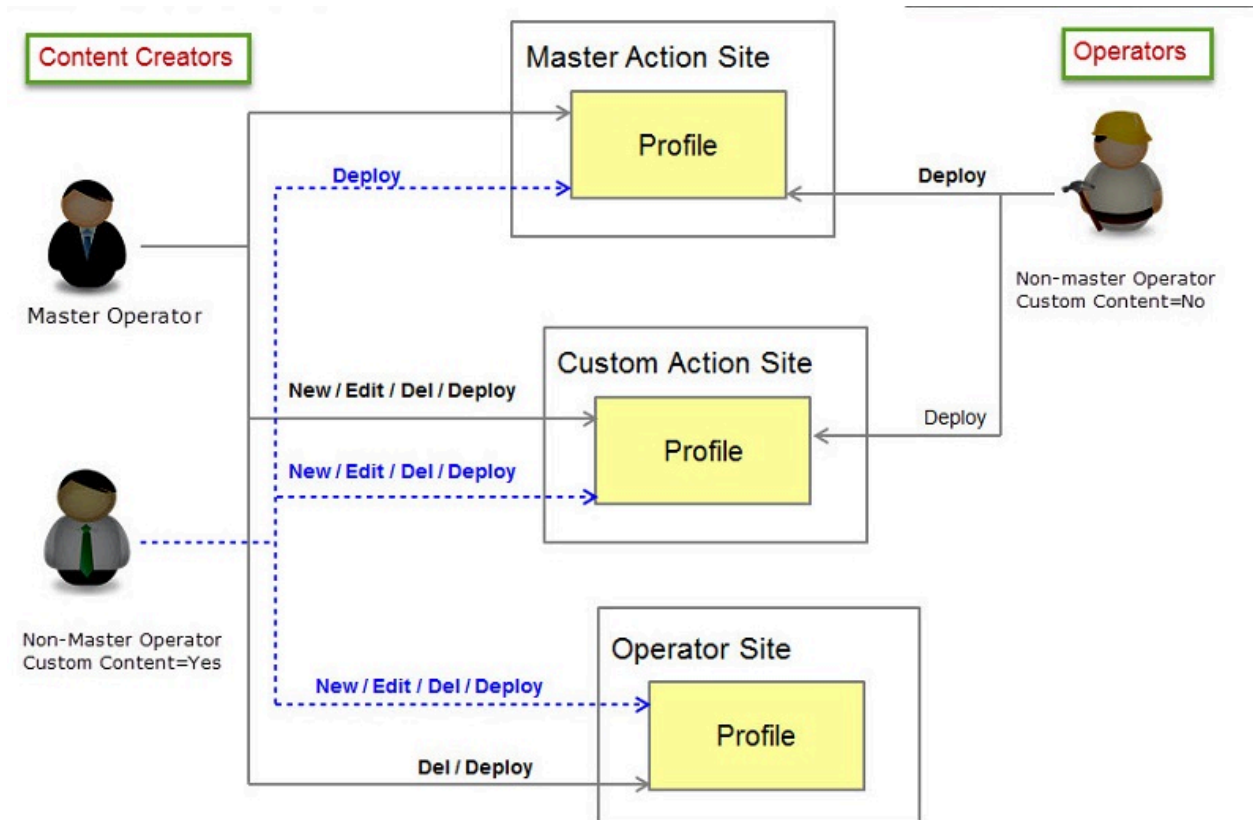
The profile actions that operators can complete depend on their roles and authorizations.

Profile Management implements the standard BigFix Platform authorization model. This model establishes the rules that define what an operator is authorized to do based on:

- The Operator Role: Master Operator (MO) or Non-Master Operator (NMO)
- Operator permissions on Sites
- Specific operator permissions:
 - Create custom content.
 - Create actions

 **Important:** To work with Profile Management, operators must have the WeBUI Interface login privilege set to "yes". For more information about Operators, roles and permissions, see the *BigFix Console Operator's Guide* at this link: [Adding Local Operators](#).

The following figure summarizes operator roles and authorizations and corresponding profile actions:



Profile list view

The profile list view displays the profiles that the currently logged-in operator is authorized to access. The filtered list includes profiles that were created in sites that the operator has access to, even if the profiles were created by a different operator.

Add (create), edit, copy, and delete profile actions

To create a new profile, you must have the Custom Content permission set to Yes. When you create the profile, you must specify the site where the profile is created. The site list that you can choose from contains sites that you have access to. A Non-master operator can edit and delete profiles he created and can also edit any profile created in a site for which he has writer permissions.

Master operators are always authorized to edit or delete profiles, unless the profile is created in an Operator site that is not owned by the currently logged-in operator.

Deploy profile

To deploy a profile, you must have the Can Create Actions permission set to Yes. The deploy action is always possible for the currently logged-in operator, on the profiles that are displayed in the profile list.

The operator is authorized to deploy profiles to targets subscribed to the sites to which he is authorized, unless further restrictions apply.

Stop profile deployments

Master operators can stop all deployments except for ones that were created in specific operator sites.

Non-master operators can stop deployments that they submitted.

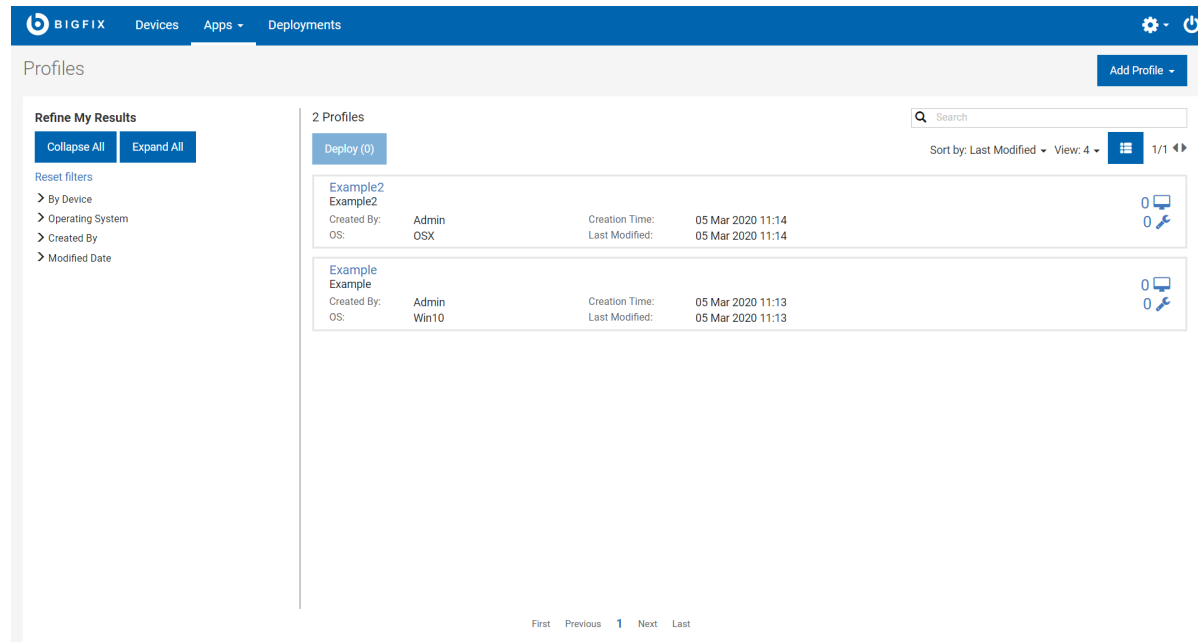
Chapter 2. Profile Management tasks

You can enforce device compliance by creating and deploying profiles.

Operators can work with Windows 10 or MAC OS profiles by selecting **Profile** from the content list.

Profile List View

The list displays the profiles that the logged-in operator is authorized to manage. Depending on the specific user role and permissions, some profile actions might not be available. For more information, see [Operator permissions and associated profile actions \(on page 2\)](#).



In the Profile list, the profiles are displayed in order of creation time. You can also sort profiles by name, or by Last modified. On the left, you can set more filters, such as selecting to display only those profiles that have applicable devices, displaying profiles that are created only for Windows 10 or MAC OS devices, filtering for profiles that are owned by you or another operator, or viewing profiles that were modified within a specified time interval.

For each profile, you can view how many devices are relevant (currently not compliant) for that profile. Directly below, you can view the number of open deployments for the profile. For information about profile deployments and how they work, see [Profile compliance behavior \(on page 8\)](#).

Create a profile

To create a new profile, from the Profile list view click **Add Profile**, and select the the Operating System. You must specify a Profile Name, Description, and select the Site in which the profile is created. For

details about the profile properties, see [Profile attributes for Windows 10 devices \(on page 13\)](#) and [Profile properties for MAC OS X devices \(on page 17\)](#). When you save the profile, a Fixlet is created. When you deploy the profile, the Fixlet is run on the computers that are subscribed to the specified site. The Fixlet checks if the current settings on the devices meet the security settings that are specified in the profile. If the settings on the devices are less restrictive, they are marked as relevant for the profile and are considered not compliant.

View or edit a profile

To view or edit profile properties, click the profile name. The Profile Overview page is displayed.

The screenshot shows the Profile Overview page for a profile named 'SBWin_02'. The page has three tabs: 'Overview', 'Noncompliant devices', and 'Deployments'. The 'Overview' tab is active. On the left, there is a summary box with the following information:

- 9 devices are noncompliant (26%)
- 0 open deployments
- 0 deployments with > 10% failed
- 0 deployments in the last 24 hours

Below this summary is a box labeled 'Windows 10 Profiles Group 2'. On the right side, there is a 'Deploy Profile' button and a 'Details' section with the following information:

Name	SBWin_02
OS	Windows 10
Created By	Administrator
Modified By	Administrator
Modified	10/11/16 9:30 AM

At the bottom of the details section, there is an 'Edit Profile' link with a red arrow pointing to it.

In the Overview page you can drill down to view detailed information pages by using the summary links. You can view details about which devices are noncompliant, the list of open or failed deployments, and which deployments occurred in the last 24 hours. The percentage of noncompliant devices is calculated from the total number of subscribed computers to the site where the profile is stored.

On the right, you can view the login name of the operator that created the profile, the operator that last modified the profile, and the date and time of the last modification. From this page, you can also deploy the profile.

Several checks are completed to determine whether the profile can be edited or not. A lock icon indicates that the profile cannot be edited because there are open deployments for it, or because the currently logged in operator does not have permission to create (edit) custom content. The link text View Profile is displayed after the lock symbol. A warning message indicates the reason. When you open the profile, the

Save option is disabled. If the profile is editable, when you click the link the profile page is opened in edit mode. Make the required changes and click **Save**.

Open deployments and profile updates

When there are open deployments for a profile, the profile is locked and cannot be edited. If you want to change policies in a profile, you must first stop any open deployments for that profile before you can edit and make the required changes. When the new profile attributes are saved, you must redeploy the profile to activate enforcement.

Copy a profile

You can make a new copy of a selected profile. From the Profile List view, click the profile that you want to copy. On the Overview page, click **View Profile** or **Edit Profile** depending on whether the profile can be edited or not. In the profile properties page, click **Copy**. A new profile page is displayed with the settings of the source profile. The new profile name contains the source profile name followed by `- Copy`. For example, If you are copying a profile that is named `Winprfl1`, the new profile name is `Winprfl1 - Copy`. You can change the name, site, description, and any other category settings as required. Click **Save** to create the profile.

Delete a profile

You can delete a profile from the edit profile page, only if no open deployments exist for it. Select the corresponding action and confirm your choice.

Deploy a profile

1. From the Profile List view select a profile and click **Deploy**. Alternatively, you can click the Profile name and deploy it from the Profile Overview page.
2. The list of devices for which the profile is relevant are displayed. Select one or more devices, or device groups and click **Next**. You can use filters to select devices that satisfy specific criteria, such as by Operating system, or IP address.
3. In the Configure section, by default, the deployment is open-ended. If you clear this option, you can specify an End Time. Click **Next**. Review your options and click **Deploy**, or **Cancel** to return to the profile list.

When you deploy a profile. In the **DEPLOYMENTS** view, the profile state is **Open** indicating that continuous compliance checking and automatic enforcement are active. By default, if a device becomes noncompliant, meaning that the device is relevant again for the selected profile, the profile is automatically reapplied, except if the current configuration on the target is more restrictive than the configuration enforced in the profile.

 **Important:**

- The profile is automatically reapplied indefinitely when it becomes relevant again. This behavior is always valid unless you stop the deployment, or clear the open-ended deployment option, in which case, the profile is reapplied only until the specified End Time.
- If a deployment fails for any reason, the status of the associated task remains in *Waiting* in the WeBUI. This behavior is implemented by the "Retry on Failure" mechanism, explained in [Retry on failure \(on page 8\)](#).

For information about troubleshooting deployments, see [Troubleshooting profile deployments \(on page 22\)](#).

Retry on failure

BigFix Profile Management implements a "Retry on Failure" mechanism. If a deployment fails, the corresponding task remains in *Waiting* state in the WebUI, and every 15 minutes the feature attempts to reapply the profile for 999 times. The deployment state changes when profile is reapplied successfully or when the retry interval counter expires. In the first case, the deployment status changes to **Fixed**, while in the second case the deployment status changes to **Failed**.

To check what is happening when the deployment status is still in *Waiting*, you can log in to the BigFix Console. There are exit codes for the failed action that is associated to the deployment. For exit codes relative to Mac OS X profile deployments, see [Troubleshooting profile deployments \(on page 22\)](#).

Stop a deployment

From the deployments view, select the open deployments that you want to stop and click the corresponding action. You can apply one or more filters to the deployments list, such as by Failure rate, issuer, deployment type, and others. You are asked to confirm the stop request.

Profile compliance behavior

The security posture of devices in your organization is enforced by deploying profiles.

Within an organization, different levels of Security can be implemented, depending on the overall Security requirements. A common level of security policies might be applied to all devices in the organization, at the Master Action site level, while at the department level, more restrictive policies might be necessary depending on the organizational structure and on the criticality of single devices. Based on the organization's desired Security posture, the Security Administrator creates a "Corporate" profile that enforces the minimal set of required security policies that must be common to all devices. At the department level, depending on the required security level and criticality of the devices, operators can

create specific "Department" profiles that enforce more restrictive policies on specific sets of devices. The final result is that on the device the combined parameters from the deployed profiles are always the most restrictive.

Operationally, profile management is implemented as a two-step process. In the first step, Security Administrators define the Security posture of the organization by identifying the policies that must be enforced on the devices. These policies are defined by creating one or more profiles. When an operator creates and saves a profile in a specified site, all computers that are subscribed to that site are checked for relevance regarding the policies set in the profile. If a device becomes relevant for that profile, it means that it is not compliant. When a device is checked against a profile, if more restrictive settings are found, the device is not relevant.

In the second step, when the profile is deployed to the targets that must comply to the policies, the configurations that are defined in the profile are enforced on all targeted devices. This step is completed by a Fixlet that sets the required profile configurations on the selected targets. If the configuration parameters are changed locally on the target, the configuration is reapplied automatically, unless the parameters set locally on the target are more restrictive than the ones currently enforced with the deployed profile. When the profile is deployed successfully, the status on the device for the profile is **Fixed**.

Managing multiple profiles on a target - profile layering

Profiles are divided into categories. You can enable individual categories that contain one or more settings that you want to enforce on your targets. On Windows 10 targets, each parameter in the categories that are enabled in the profile is mapped to specific device settings according to the WMI infrastructure. On Mac OS X targets, a new OS X profile is created for each enabled category. A maximum of four OS X profiles are created on a Mac device, one for each enforced category in the BigFix profile. You can view OS X profiles from the Profile graphical user interface available in System Preferences on the device.

Operators can define multiple profiles that enforce one or more categories of settings. When the profile is deployed on a target, each setting in every enforced profile category is evaluated against the corresponding setting on the target. If at least one setting in the profile is more restrictive than the corresponding setting on the target, the target is considered relevant (noncompliant) and the profile is applied. You can deploy multiple profiles on a target, and the evaluation is always completed by comparing the individual settings. The final security configuration (security posture) of the target is made up of the union of more profiles where the most restrictive values are enforced.

If policies change either centrally or locally, Administrators can stop the deployments of the currently enforced profiles, and reset the profile configurations on all devices in the organization or in a specific

department. New profiles can then be deployed on targets. For more information, see [Resetting the Profile Management Configuration \(on page 12\)](#).

 **Note:**

On Mac OS X devices, if one or more profiles that are not deployed by BigFix Profile Management exist, when you deploy a BigFix profile that sets parameters that belong to the same category of the existing profile, the deployment fails after the "Retry on Failure" counter expires. To solve the problem, you must first remove the existing profile from the device and then redeploy the BigFix profile. For more information about the specific error codes, see [Mac OS X Profile Deployment errors \(on page 24\)](#)

On Windows 10 devices, if one or more parameters in the profile have more restrictive settings than those currently on the device, the profile is always applied.

Use Case Example - Organization with Windows 10 devices

In this example, a corporation has 30 departments and several thousand Windows 10 devices that are distributed in several geographic locations. The Security Officer establishes the security posture of the entire corporation that comprises a set of common policies that all devices must comply to, regardless of their specific department membership. Administrators in each department, based on the devices and the roles of the users, can define specific security settings that are valid only for their specific department and deploy them locally.

In this example, Windows 10 device *Win10_DeptB_SWAdm* belongs to Department B in the organization, which is geographically located in London. The device is used by the Software Administrator, in charge of installing the required software on the devices in his/her department. To illustrate the layering behavior, three profiles are created and deployed to the device: a corporate profile, a department profile, and a profile that is specific to Software Administrators in the organization. Profile layering checks each setting in each category, and ensures that the most restrictive setting is always enforced.

The Security posture at the corporate level, establishes that all passwords in the organization be at least 8 characters long, and expire after 20 days. Moreover, the use of Cortana is not allowed.

To enforce this posture, the Security Administrator creates a corporate profile with the following settings:

Table 1. ProfileCorp_Win10 - Profile for all Windows 10 devices in the company

Profile Category	Setting
Password Settings	Password expires after 20 days
	Minimum Password Length is 8 characters
Restrictions	Cortana is disabled

The profile is deployed and applied to all devices in the organization, including *Win10_DeptB_SWAdm*. When the profile is deployed successfully to the devices, they are compliant.

The Security Administrator defines a profile that must be deployed to all devices used by Software Administrators across the organization, including *Win10_DeptB_SWAdm*. The profile enforces the following settings:

Table 2. Profile_Corp_SWAdmins - Profile for all devices used by Software Administrators in the corporation

Profile Category	Setting
Password Settings	Minimum Password Length is 15 characters
	Device is put on BitLocker Recovery mode after 3 incorrect password attempts.
	Password Expires after 10 days
Restrictions	Telemetry Level set to Security

The Local Security Administrator in London defines a cross-department profile for departments A, B, and C in that location. This Profile has the following settings:

Table 3. Profile_London_DeptABC - Profile for all Windows 10 devices in London

Profile Category	Setting
Password Settings	Minimum Password Length is 12 characters
App Security	Allow App Store Auto Update is disabled
Restrictions	Cortana is enabled (default)
	Location Service set to OFF
	Telemetry Level set to Basic

This profile is deployed on all devices belonging to departments A, B, and C in London, including *Win10_DeptB_SWAdm*

The resulting Security configuration on device *Win10_DeptB_SWAdm* combines the most restrictive settings from all three profiles, as displayed in the following table

Table 4. Security configuration on target Win10_DeptB_SWAdm

Category	Settings
Password Settings	Minimum Password Length 15 characters - from profile <i>Profile_Corp_SWAdmins</i>
	Password Expires after 10 days - from profile <i>Profile_Corp_SWAdmins</i>
	Device is put on BitLocker Recovery mode after 3 incorrect password attempts - from profile <i>Profile_Corp_SWAdmins</i>
App Security	Allow App Store Auto Update is disabled - from profile <i>Profile_London_DeptABC</i>
Restrictions	Cortana is disabled - from profile <i>ProfileCorp_Win10</i>
	Location Service set to OFF - from profile <i>Profile_London_DeptABC</i>
	Telemetry Level set to Security - from profile <i>Profile_Corp_SWAdmins</i>

Resetting the Profile Management Configuration

In each site where at least one profile exists, a corresponding task for resetting the profile configuration on the device is available for Windows 10 and Mac OS X devices. When you run the task on Windows devices, it removes all parameters of the categories that were enabled by Profile Management, also those parameters that were set manually or by other applications,

On MAC OS X devices, the task erases all profiles that are created by Profile Management (a maximum of four profiles, one for each enforced category, is erased). Run this task in the following situations:

- Corporate Security policies have changed and you want to enforce new policies on all your devices.
- You are moving some devices from one department to another, and the new department has different security requirements.
- You want to enforce less restrictive policies on one or more devices, either temporarily or on a permanent basis.

Select **Content > Custom**, and type **Reset** in the search field. A list of available reset tasks for Windows and MAC OS X is displayed. You can also use filters to restrict the search to specific sites or operators. Before you run a reset task, you must stop all open deployments of the profiles that are currently enforced on the targets where you want to reset the profile management parameters.

Depending on the operator login authorizations, you might view more than one Reset task. Deploy the task stored in the Site where the devices you want to reset are subscribed.

Profile attributes for Windows 10 devices

To enforce security compliance on your Windows 10 devices, create one or more profiles with the required settings. To complete this task, you must have the correct authorizations. See [Operator permissions and associated profile actions \(on page 2\)](#).

1. Specify a **Profile Name** , a **Description** and select the **Site** where the profile is created. The sites that are available are those that your operator login is authorized to. These fields are mandatory. You can enforce security policies for the categories that are displayed in the left pane. To change or specify attributes in a category you must first enable it by clicking **On**. If you enable a category without changing any settings, the greyed values are not enforced on the devices when the profile is deployed. You must enable at least one category to save the profile.



Note: You cannot specify double quotation marks " in the Profile Name and Description fields.

2. Select the **Password Settings** tab to change authentication settings for your Windows 10 devices. You can specify the following properties:

Password expires after [0] days

Specify the length of time in days after which a user password must be changed. Allowed values are in the range from 0-730 where 0 (zero) means that the password never expires. The most restrictive value is 1.

Enforce password history for the last [0] passwords.

Specify the number of previous passwords that cannot be reused. Allowed values are in the range 0-24, where 0 (zero) means that this check is not enabled, and the most restrictive value is .24.

Activate Password Controls

Selecting this option automatically enforces a strong password scheme requiring that passwords have at least 3 complex element types including uppercase and lowercase letters, and numbers. Optionally, you can also specify special characters. If PINs are used, the same complexity rules apply. This policy is the most restrictive. Additionally, you can set or change the following controls:

Device is put on BitLocker recovery mode after [0] incorrect password attempts

Allowed values are in the range 4-16, or 0 (zero). the default value of zero means that the policy is not enforced. If BitLocker is enabled on the device, when the value set by this policy is reached, the device is rebooted and put on BitLocker recovery mode, and the user must

specify the BitLocker recovery key. If BitLocker is not enabled, the device is only rebooted. The most restrictive value is 4.

Device is locked after [0] minutes of inactivity.

Specify how many minutes to wait in the absence of any user input, before the device is locked. After the specified time, the device becomes PIN or password locked. The allowed values are in the range 0-999, where a value of 0 means that no timeout is active and the device never locks. The most restrictive value is 1.

Minimum password length is [4] characters

Specifies the minimum length required for a password or PIN. Allowed values are in the range 4-14, and the default value is four. However, local accounts will always enforce a minimum password length of six characters. The most restrictive value is 14.

Allow use of simple device passwords

This option allows accounts on the device to sign in using picture passwords or biometric methods (such as fingerprint or iris recognition), if the device is equipped with the corresponding readers. This option is enabled by default.

3. Select the **Device Security** tab to change the following properties:

Allow Storage Card

Controls whether the user is allowed to use removable storage cards for device storage. Default is allow. Deselect this value to prevent the use of removable SD cards and to disable USB drives on the device.

Allow Device Discovery

This policy controls whether a device can discover other devices when the lock screen is displayed. The Default is allow. It enables the use of shortcuts such as **Win+P** to project on another screen, or **Win+K** to search for wireless display and audio devices. Deselecting this option will disable use of these shortcut keys.

Both options are selected by default.

4. Select the **App Security** tab to specify security options for Windows Applications:

Allow App Store Auto Update

This setting enables automatic updates of Windows Store apps.

Install Trusted Apps

This policy setting enables the installation on the device of non-Windows Store applications that are trusted by a certificate. Select one of the available settings:

Not Configured

This is the default value, and it means that the policy is not used.

Explicitly Allow

Enables the installation of trusted non-Windows Store apps on the device.

Explicitly Deny

Installation of non-Windows store apps on the device is not permitted. This is the most restrictive option.

Developer Mode

Specifies whether development, deployment and debugging of installed non-packaged applications is allowed. Select one of the available settings:

Not Configured


This is the default value, and it means that the policy is not used.

Explicitly Allow


Enables the development and deployment of non-packaged apps on the device.

Explicitly Deny

Development and deployment of non-packaged apps is not allowed on the device. This is the most restrictive option.

 **Note:** The values you select in the **Install Trusted Apps** and **Developer Mode** policy settings affect how the following Developer Features in the Update and Security page on the device are handled:

- Windows Store Apps
- Sideload apps
- Developer Mode

 **Important:** If you select “*Explicitly Deny*” for **Install Trusted Apps** and select “*Explicitly Allow*” for **Developer Mode**, the latter parameter value overrides the first, so that the installation of non-Windows Store trusted apps is also allowed.

Select the **Restrictions** tab to disable access to one or more specific resources. The resources you can restrict are general purpose, such as speech, typing, account, email, and notification settings. All options are enabled by default. Click **Select All** to disable all resources in the list.

Camera

Disables the use of camera on the device.

Microsoft Account Connection

When selected, it prevents Microsoft accounts from performing non-email related connection authentication and services. This restriction might affect the use of Cortana, depending on the Windows 10 build that is installed on the targeted device.

Adding Non-Microsoft Accounts Manually

When selected, users on the device cannot add non-Microsoft email accounts.

Sync My Settings

Disables all Windows sync settings on the device.

Cortana

Specifies whether users on the device can access Cortana.

Toasts

Disables toast notifications above the device lock screen.

Input Personalization

Disables the automatic learning component of input personalization that collects speech, inking, typing, contacts, and calendar information required by Cortana. When selected, automatic learning is stopped on the device, and all previously collected learning information is cleared. Cortana and Dictation are also disabled.

System Telemetry level

Defines the level of telemetry events and data (such as diagnostics, usage, and reliability information) that the device is allowed to send. You can specify four different levels. Levels are cumulative.

Security

Send security data only. Only data pertaining to security updates is sent.

This value is the most restrictive.

Basic

Send a limited set of system configuration and health data for problem determination. This level also includes data from the Security level.

Enhanced

Send data about application usage, performance, device-specific events, some diagnostics. This level also includes data from the Basic and Security levels.

Full

Send all necessary data to identify and resolve problems, and reliability and usage data. This level also includes data from the Basic, Enhanced, and Security levels.

Location

Specifies whether to allow app access to the Location service.

Location Service is allowed

The Location Service is enabled. This is the default value. Users on the device can control and change the Location Privacy settings (on or off).

Force Location Off

All Location Privacy settings are greyed out. Users on the device are not allowed to change settings, and no apps can gain access to the Location service, including Cortana.

Force Location On


Location Service is allowed, and Location Privacy settings are greyed out. Users on the device are not allowed to modify the Location settings.

Profile properties for MAC OS X devices

To enforce security compliance on your MAC OS X devices, create one or more profiles with the required settings. To complete this task, you must have the correct authorizations. See [Operator permissions and associated profile actions \(on page 2\)](#).

1. Specify a **Profile Name**, a **Description** and select the **Site** where the profile is created. The sites that are available are those that your operator login is authorized to. These fields are mandatory. You can enforce security policies for the categories that are displayed in the left pane. To change

or specify attributes in a category you must first enable it by clicking **On**. If you enable a category without changing any settings, the greyed values are not enforced on the devices when the profile is deployed. You must enable at least one category to save the profile.

 **Note:** You cannot specify double quotation marks " in the Profile Name and Description fields.

2. Select the **Passcode Settings** tab to set or change the following properties:

Allow simple values

The passcode can contain sequential or repeated characters, such as AAAA, or 1234. This option is selected by default.

Minimum passcode length is [0] characters

Specify the minimum length of the passcode. Allowed values are in the range 0-50. The default value of 0 indicates that passcode length is not checked. The most restrictive value is 50.

Password requires at least [0] complex characters

Specifies the number of non-alphanumeric characters (such as \$ and !) that the passcode must contain. Allowed Values are in the range 0-50, where 50 is the most restrictive value.

Passcode expires after [0] days

Allowed values are in the range 0-730, where 0 means that the passcode never expires. The default is 730. The most restrictive value is 1.

Enforce passcode history for the last [0] passwords

Specify the number of previous passwords that cannot be reused. Allowed values are in the range 0-50 , where the value 0 indicates that this check is not enabled. When you enter a new passcode, it is compared against the specified number of previous passcodes. If a match is found, the passcode is refused. The most restrictive value is 50.

Lock screen after [0] minutes of inactivity.

Allowed values are in the range 0-5. The default value of zero means that the screen never locks. The most restrictive value is 1.

Lock device after [10] failed login attempts .

The device is locked after the specified failed login attempts. Allowed values are in the range 0-11. The default value 0 indicates that the device is never locked. The most restrictive value is 1.

Set a Delay of [0] minutes before the login window is re-displayed

When the device is locked because after the defined number of failed login attempts was reached, the device waits the specified number of minutes before displaying the login window again. The default value of zero means no delay. If the value specified in the Lock Device parameter is 0 or 1, this option is greyed out and cannot be changed.

Set a Grace period of [730] minutes before requiring a passcode when the device is locked

Valid values are in the range 0-730, where 0 means no grace period, and a passcode must be entered immediately. This is the most restrictive value.

3. Select the **Device Security** tab to change the following settings:

Allow use of external disks

You can use external disks (for example USB keys) on the device. This option is enabled by default. If you select to disable this option, and the target system already has a mounted external disk, for the restriction to take effect you must reboot the system after you deploy the profile.

Allow use of removable media

You can use any type of removable media (such as CD or DVD) on the device. This option is enabled by default. If you select to disable this option, and the target system already has a mounted CD/DVD, for the restriction to take effect you must reboot the system after you deploy the profile.

Eject media at logout

Select this option to eject all removable media when the user logs out. By default this option is not selected.

Enable AirDrop

You can use AirDrop on the device to share items. This option is enabled by default.

4. Select the **App Security** tab to change the following settings:

Enable Game Center

Specifies whether you can use Game Center on the device. This setting is enabled by default. You can disable one or more of the following Game Center options:

Allow multiplayer gaming

Allow multiple players

Allow adding Friends

You can add friends to your player list

Allow modification of account credentials

You can modify the user id and passcode for accessing Game Center

Restrict adoption of preinstalled apps by App Store

When this option is selected, any free application included in the installed operating system on the device cannot be updated through App Store.

Restrict App Store usage

Select this option to use App Store only for updating applications installed by MDM and Apple software.

Require Administrator password to manage apps

If you enable this option, you must always specify the Administrator password every time you install or update any application on the device.

Enable Gatekeeper

Gatekeeper protects devices by checking for malware before apps are installed.

Allow sending diagnostic data to Apple

Sends diagnostic and usage data to Apple. This option is enabled by default.

5. Select the **Restrictions** tab to disable user access to specific resources in "System and Preferences" on the device. All preferences are enabled by default. Select one or more resources that you want to disable or click the **Select All** button to disable all resources. The panes for the options you select will be greyed out on the device. Resources are divided in two categories:

- System Preferences:

App Store

Bluetooth

CDs and DVDs

Desktop and Screen Saver

Extensions

iCloud

Internet Accounts

Network

Printers and Scanners

Profiles

Security & Privacy

Sharing

Sound

Spotlight

Startup Disk

Time Machine

Users and Groups

• Miscellaneous

Camera

Disables the use of the built-in camera, a built-in camera of a connected display, or a USB camera

iCloud documents & data

Disables the possibility to store presentations, spreadsheets, images, and other documents on devices that are set up for iCloud Drive.

iCloud keychain

Prevents iCloud Keychain from storing Safari website username and passwords, credit card information, and from keeping Wi-Fi network information up to date. This setting is found in **Safari > Preferences > Passwords**

iCloud password for local accounts

Prevents the use of an iCloud ID and password to unlock A MAC OS X device. This setting is found in OS X "System and Preferences" under "Users and Groups".

Spotlight internet suggestions

Disables the use of Spotlight to search fro apps, documents, images and other files.

Chapter 3. Troubleshooting profile deployments

When a deployment fails, you can determine the cause of the error by viewing the available logs and error code information.

Profile Management stores information about deployment actions on the BigFix server, on the WebUI Server, and on the devices to help you understand the cause of an error.

Unable to remove profile with restrictions via MCM Remove policy

If you have created and deployed restrictions profile through Profile Management application (deprecated) from WebUI, it installs the profiles locally on the endpoint. In this case, if you try to remove the restrictions through **WebUI > Apps > MDM > Remove Policy** action, it does not work. However, you can remove such policies from the endpoint, through the following local commands on the command line.

1. To list out profile identifiers

```
sudo profiles -P
```

2. To remove profiles with the given \$profile_identifier

```
sudo profiles -R -p $profile_identifier
```

WebUI Server Log files

On the WebUI server, you can view information about errors that occur when profiles are saved and the corresponding fixlet is created and submitted to the BigFix Server. Log files are stored in the following locations:

- Windows: \\Program Files (x86)\BigFix Enterprise\BES Server\WebUI\Logs\
• Linux: //var/opt/BEServer/WebUI/Logs

The specific log file for Profile Manager is `prfmgr.log`

How to set WebUI Server Site log levels for Profile Management

To change logging levels for the WebUI, you have to add the `_WebUI_Logging_Filter` client setting as described in [Server Settings Definitions](#). To set logging levels for Profile Management, you must add a specific token. The value you specify determines what is written in the `prfmgr.log`. You can also specify the logging level detail (debug, verbose, or error). The available tokens are:

```
bf:bfdata-prfmgr  
bf:bfdata-prfmgr:all-creators  
bf:bfdata-prfmgr:all  
bf:bfdata-prfmgr:get-applicable-count
```

```

bf:bfdata-prfmgr:get-deployment-count
bf:bfdata-prfmgr:profile

bf:prfmgr
bf:prfmgr:deployments
bf:prfmgr:devices
bf:prfmgr:profile_action_handler
bf:prfmgr:profile_fixlet_creator
bf:prfmgr:initialize
bf:prfmgr:tasks
bf:prfmgr:profiles

```

For example, to log all Profile Management traces, write the following value in the **_WebUI_Logging_Filter** client setting: `bf:prfmgr:*`.

If you also want to view all queries, you must add messages that are logged by the database by specifying: `bf:prfmgr:* ,bf:database:*`

Target log files

When a profile is deployed on a target device, you can find useful information in the log files that are created for each deployed profile.

Windows 10

In the path `\\Program Files (x86)\BigFix Enterprise\BES Client_BESdata_Global\PrfmgrLog` a file is created for each deployed profile. The name of the log file is made up of the profile name followed by extension `.log`. The profile log file contains the following information:

- Which security settings are enforced with the profile.
- The current settings on the target device.
- The final state of the device, and, in case of errors, the failure message or WMI exit code.

Mac OS X

The following log files are stored in the `/var/tmp/BES` directory on the target

- `PRF_Profile_WebUI_*`: This file contains the last imported profile for the specified category.
- `com.bigfix.profile.*`: Contains working files with error information.
- `profileLoad.output`: This file contains profile operation logs.

Mac OS X Profile Deployment errors

When you deploy a profile on a Mac OS X device where there are profiles that were not created by BigFix Profile Management that enforce the same category or categories of the profile you are deploying, the message `This action failed because another non-BigFix profile already enforces the category on this target` is displayed in the Device Results page with an exit code corresponding to the category that caused the error, as detailed in the following list:

- 91 - Passcode
- 92 - Device Security
- 93 - App Security
- 94 - Restrictions

Important:

These results are displayed in the WebUI only after the "Retry on Failure" counter is expired. When the counter is still active, the deployment remains in "waiting" state. During this time frame, you can log in to the BigFix Console to check the exit code for the associated action.

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.