BigFix Compliance

Student Workbook

January 2024

HCL BigFix

For more information

To learn more about BigFix, contact your HCLSoftware representative, HCL Business Partner, or visit www.BigFix.com.

About HCLSoftware

HCLSoftware, a division of HCLTech, develops, markets, sells, and supports software for digital transformation, data, analytics and insights, AI and automation, and enterprise security. HCLSoftware is the cloud-native solution factory for enterprise software and powers millions of apps at more than 20,000 organizations, including more than half of the Fortune 1000 and Global 2000 companies. HCLSoftware's mission is to drive ultimate customer success through relentless product innovation. https://www.hcltechsw.com

Produced in the United States of America.

Contents

Student exercises

Overview

BigFix Compliance enforces continuous compliance with security policies throughout your organization for every endpoint both on and off the corporate network. It includes out-of-the-box support for most popular security benchmarks published by CIS, DISA STIG, USGCB and PCI-DSS. An intelligent agent on every endpoint monitors, enforces and reports on the security configuration status of the endpoints in real-time regardless of OS type or location. Any compliance drift is reported and can quickly be remediated to reduce the overall security risks.

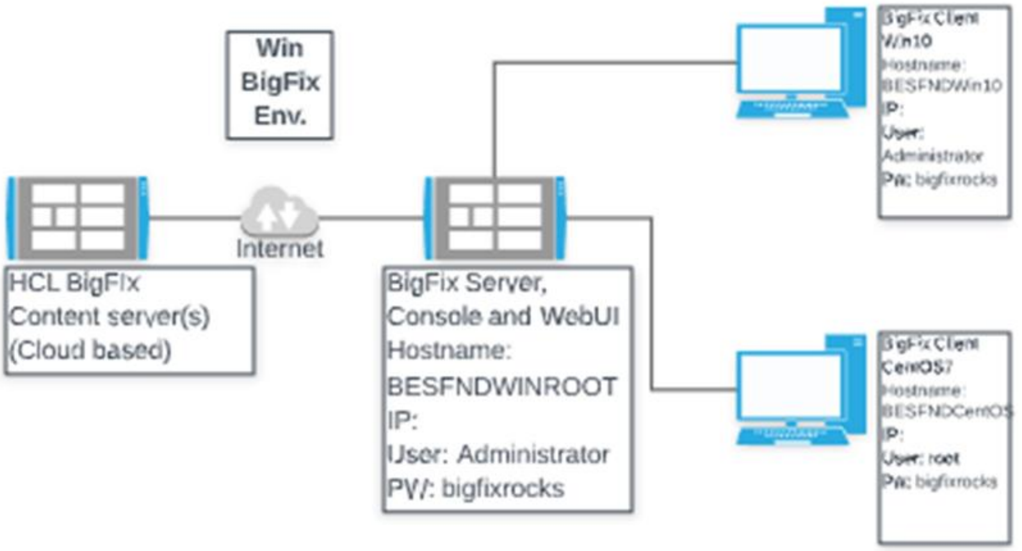
In this lab you will learn how to:

- Enable the Compliance content
- Install the BigFix Compliance Analytics Server
- Create Custom Checklists
- Import Checklists and Data into the Analytics Server
- Customize Compliance Checks
- Enforce Continuous Compliance
- Create a Saved Report in BigFix Compliance Analytics
- Create Computer Groups for Reporting
- Create a Custom Properties
- Enable Patch and Vulnerabilities Reporting
- Create Exceptions
- View the Exception Results Report
- Create and Deploy a Client Compliance Document
- Deploy the Compliance Assessment and Quarantine Policies
- View the Patch and Vulnerability Reports (optional)

The exercises in this lab guide focus on installing, configuring, and using the BigFix Compliance content.

These exercises are based on VMware Workstation v12, but other versions of VMware Workstation could also be used including VMware Fusion.

NOTE: This is not a deployment guide and it is not designed to show a secure implementation.



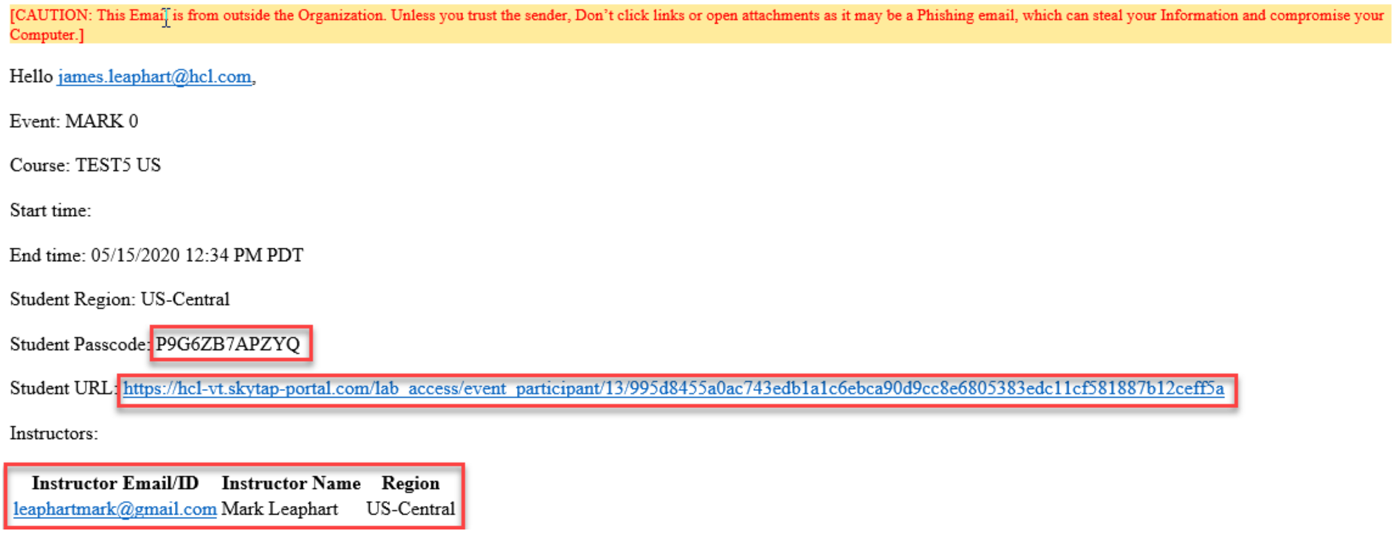
The below table contains a summary of the VM images used in this lab guide:

	Host Name	BigFix Components	OS	IP Address	Userid & Password
1	BESFNDWINROOT	BigFix Windows based Server, Console, WebUI, Web Reports, and Client	Windows 2019	10.0.0.1	Administrator bigfixrocks
2	BESFNDWIN10	BigFix Client, Console	Windows 10	10.0.0.2	tecuser bigfixrocks
3	BESFNDCENTOS	BigFix Client	CentOS7	10.0.0.3	root bigfixrocks
	All	BigFix Console creds			adminmo B1gfixrocks

Accessing Lab Environment

The BigFix Lab environment is currently being hosted in Skytap's (www.skytap.com). To access this environment, you will need the url, id, and password sent to your registered email address (this would be from Skytap.com). If you are a USA Federal customer – your instructor will provide you your credentials and access url(s).

Students will receive an email (this is the email address you provided when you registered for the course) from Skytap that contains the url to YOUR Skytap environment, the login id and password for this specific course. It will look something like this:



[CAUTION: This Email is from outside the Organization. Unless you trust the sender, Don't click links or open attachments as it may be a Phishing email, which can steal your Information and compromise your Computer.]

Hello james.leaphart@hcl.com,

Event: MARK 0

Course: TEST5 US

Start time:

End time: 05/15/2020 12:34 PM PDT

Student Region: US-Central

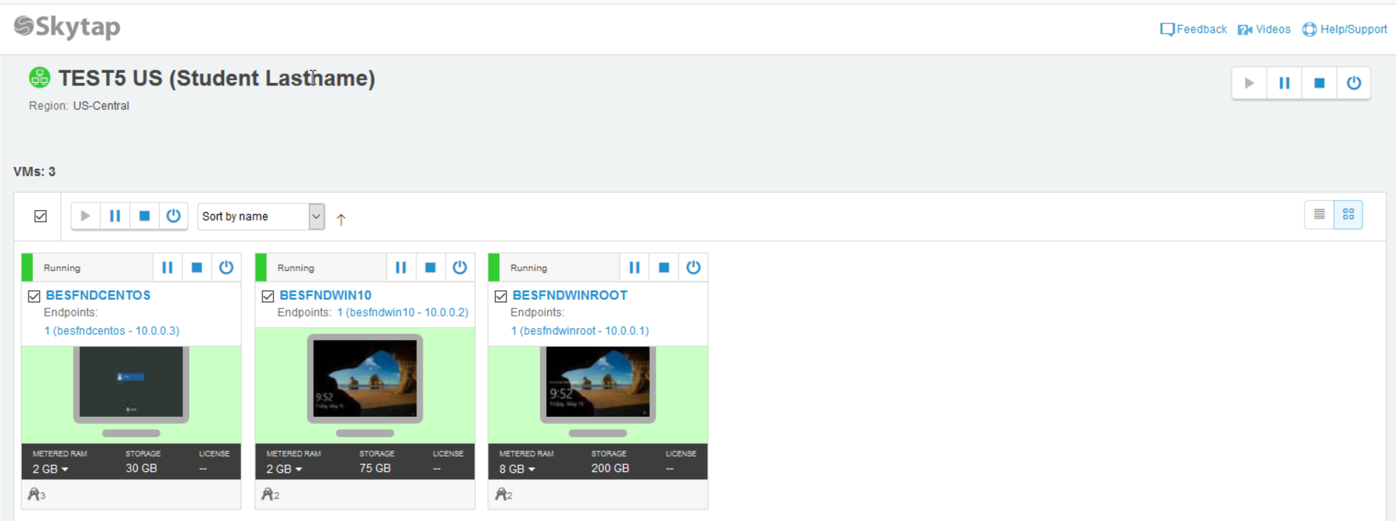
Student Passcode: P9G6ZB7APZYQ

Student URL: https://hcl-vt.skytap-portal.com/lab_access/event_participant/13/995d8455a0ac743edb1a1c6ebca90d9cc8e6805383edc11cf581887b12ceff5a

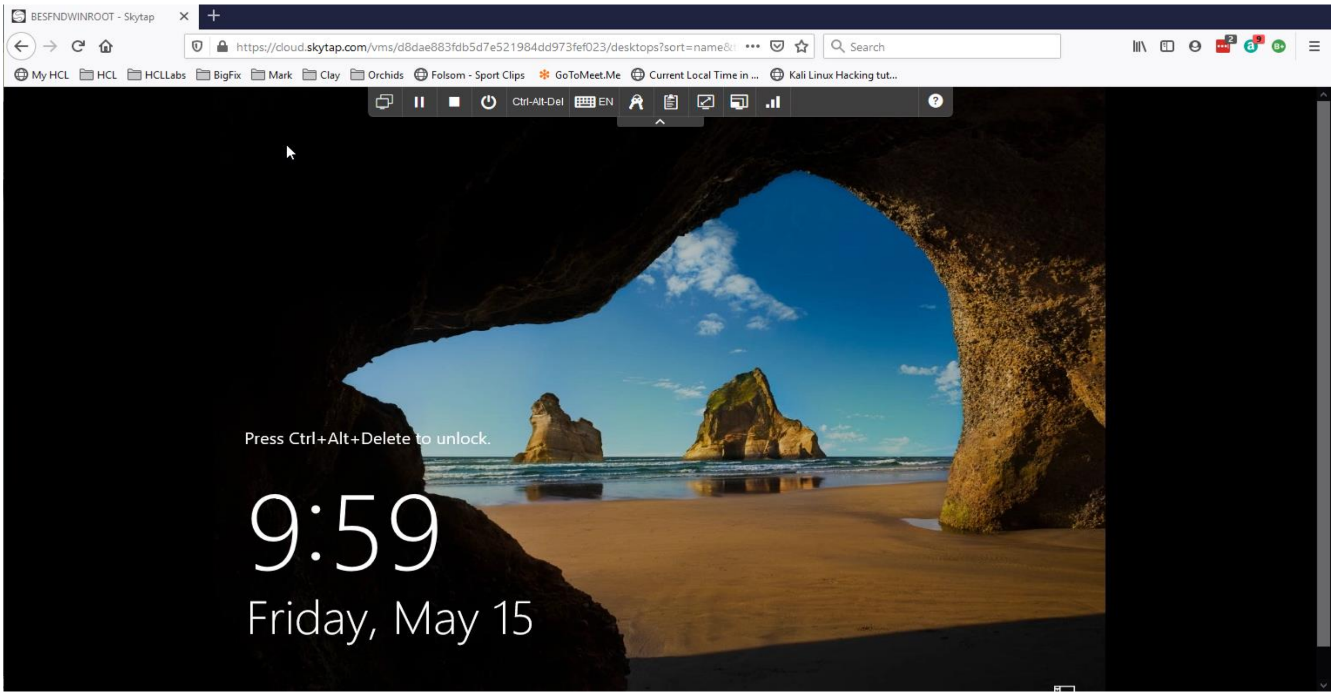
Instructors:

Instructor Email/ID	Instructor Name	Region
leaphartmark@gmail.com	Mark Leaphart	US-Central

Click on the url provided in your email and provide your credentials (if asked). You will be taken into Skytap and you will see your provisioned environment.



The vm's provided here are accessible via your browser (rdp is not required). Click on a vm and your browser will present your vm:

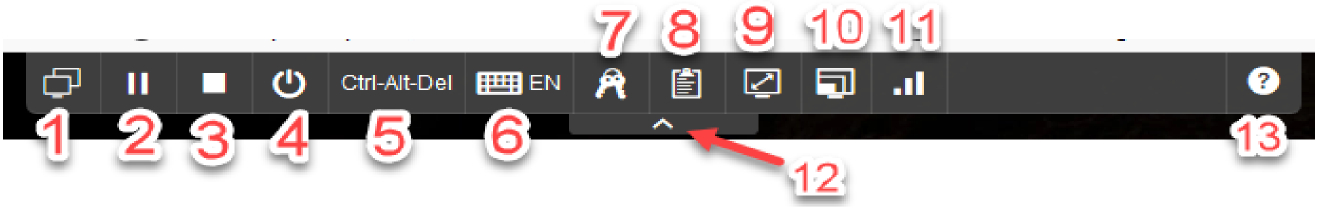

BESFNDWINROOT - Skytap
https://cloud.skytap.com/vms/d8dae883fdb5d7e521984dd973fef023/desktops?sort=name&
Search
My HCL
HCL
HCLLabs
BigFix
Mark
Clay
Orchids
Folsom - Sport Clips
GoToMeet.Me
Current Local Time in ...
Kali Linux Hacking tut...
Ctrl-Alt-Del
EN

Press Ctrl+Alt+Delete to unlock.

9:59

Friday, May 15

Now let's look at the controls in the browser for this vm.



1) Environment VM's: View all vm's in your environment or switch to another vm in your environment
2) Suspend this vm
3) Shutdown this vm
4) Power options for vm - a) shutdown, b) reset, c) power off
5) Ctrl-Alt-Del is passed to the vm
6) Keyboard layout and or inject key combinations
7) Credentials: operating system and applications in this vm
8) VM Clipboard
9) Fit to window
10) Change video resolution
11) Network Quality Indicator
12) Hide this tool bar
13) Help

When you open any of the Windows vm's, always answer YES to the network connection question.

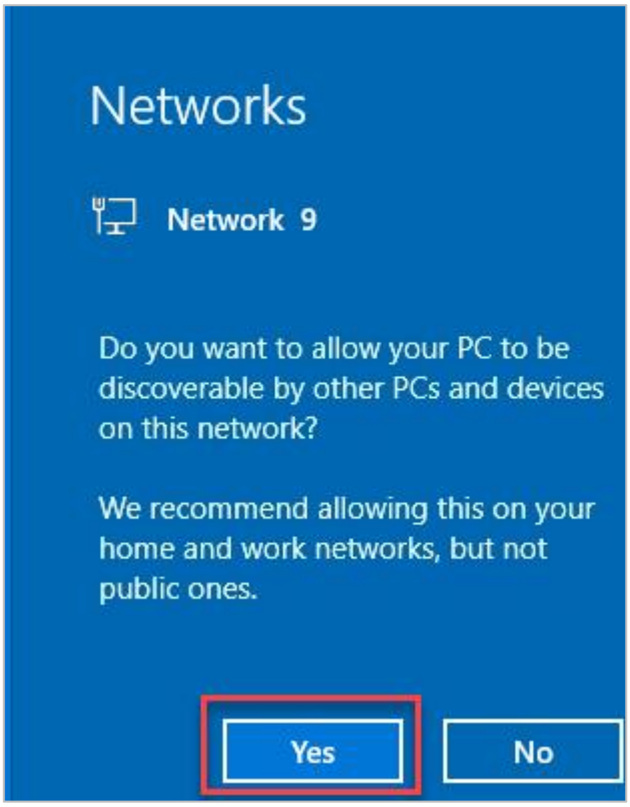
BigFix Compliance Labs

BigFix Compliance enforces continuous compliance with security policies throughout your organization for every endpoint both on and off the corporate network. It includes out-of-the-box support for the most popular security best practices published by CIS, DISA STIG, USGCB and PCI-DSS and others. An intelligent agent on every endpoint, monitors, enforces, and reports on the security configuration status of the endpoints in real-time regardless of OS type or location. Any compliance drift is reported instantly and can be remediated quickly, to reduce the overall security risks.

Exercise 1 - Starting the environment

In this exercise, you will install BigFix and start the configuration process.

1. Verify that the following virtual machines are started:
   - BigFix Server: BESFNDWINROOT
   - BigFix Windows Client: BESFNDWIN10
   - BigFix Linux Client: BESFNDCENTOS
2. Switch to the BigFix Server virtual machine. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**
3. Click **YES** to **Networks** question for all vm's (the network number will change; the graphic below is an example):



Networks

Network 9

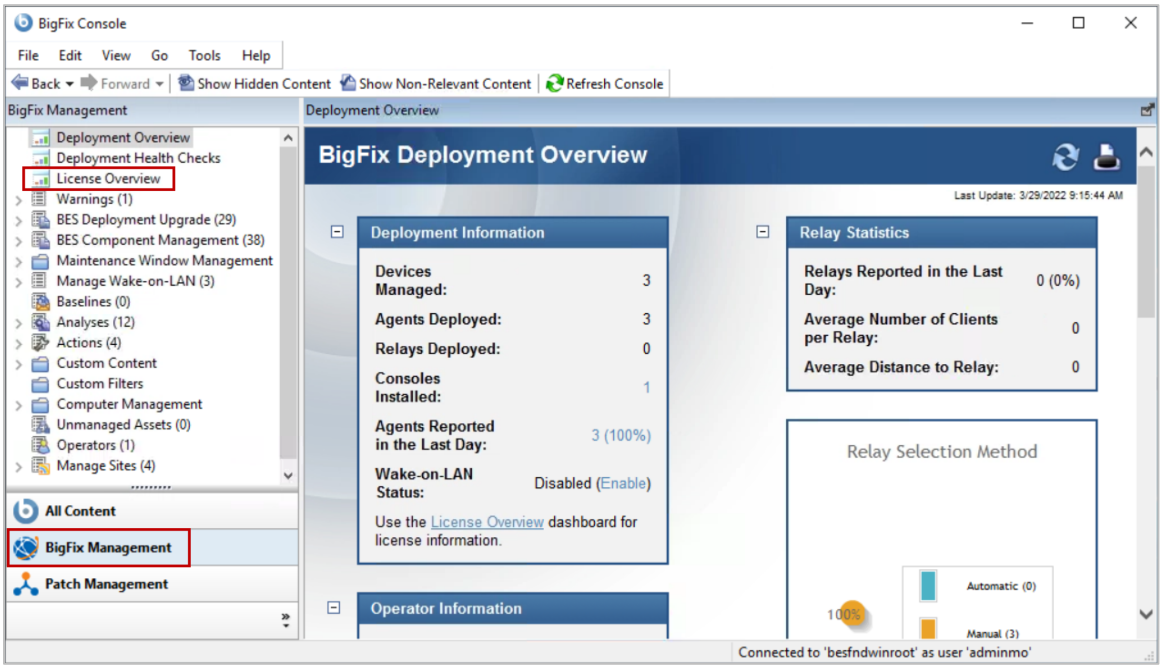
Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

Exercise 2 – Enabling Compliance Content

To take advantage of the Compliance content, it must first be enabled in the BigFix server. In this exercise, you enable the BigFix Compliance content.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens.
4. Click the **BigFix Management Domain** in the lower-left portion of the Console, then click **License Overview** in the navigation pane in the upper-left portion of the Console. The License Overview dashboard opens.



Last Update: 3/29/2022 9:15:44 AM

Deployment Information

Devices Managed:	3
Agents Deployed:	3
Relays Deployed:	0
Consoles Installed:	1
Agents Reported in the Last Day:	3 (100%)
Wake-on-LAN Status:	Disabled (Enable)

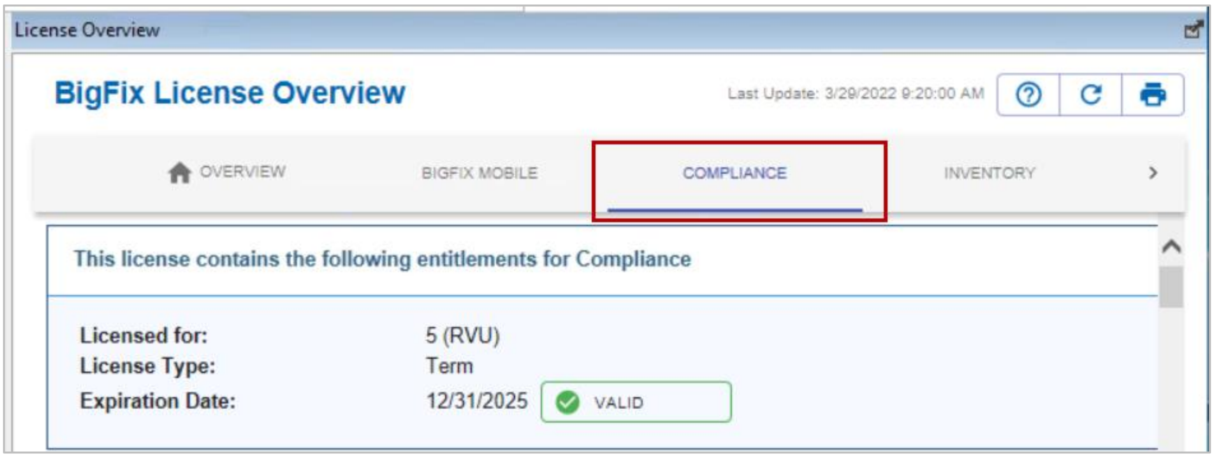
Use the License Overview dashboard for license information.

Relay Statistics

Relays Reported in the Last Day:	0 (0%)
Average Number of Clients per Relay:	0
Average Distance to Relay:	0

Connected to 'besfndwinroot' as user 'adminmo'

5. Select **COMPLIANCE** in the products section at the top of the **License Overview** dashboard.



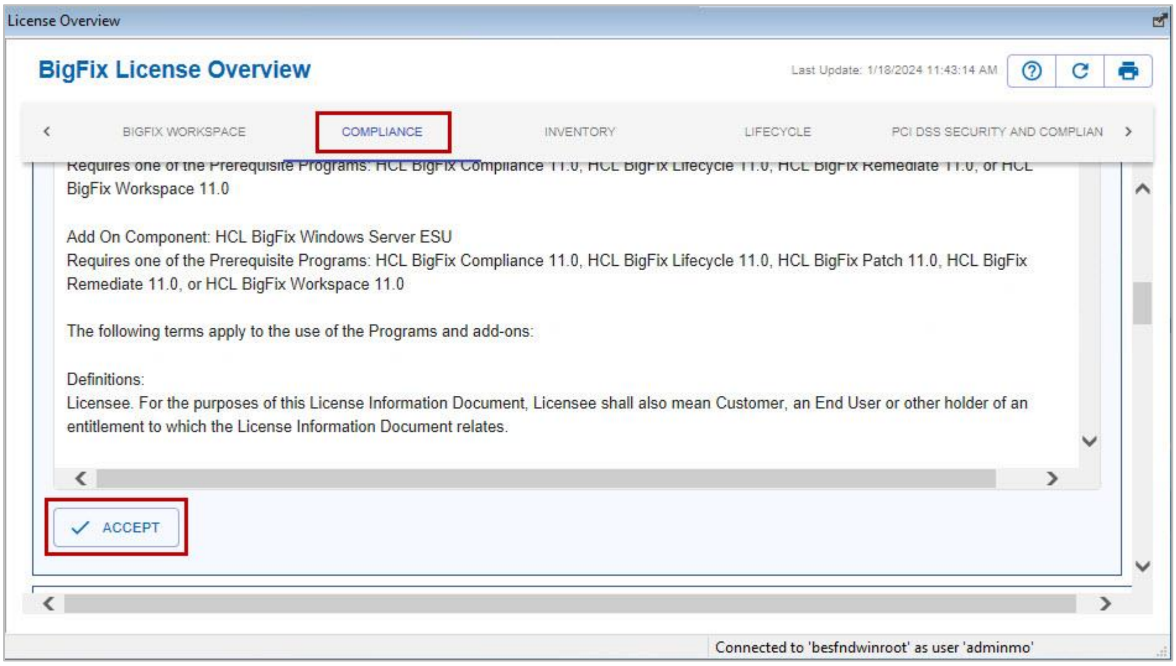
Last Update: 3/29/2022 9:20:00 AM

This license contains the following entitlements for Compliance

Licensed for:	5 (RVU)
License Type:	Term
Expiration Date:	12/31/2025 ✓ VALID

The License Overview dashboard updates to show the Product EULA Info page and the sites that are associated with the Compliance product.

6. Scroll down the **Product EULA Info** page and click **Accept** to accept the License Agreement for Compliance.



License Overview

BigFix License Overview

Last Update: 1/18/2024 11:43:14 AM

Requires one of the Prerequisite Programs: HCL BigFix Compliance 11.0, HCL BigFix Lifecycle 11.0, HCL BigFix Remediate 11.0, or HCL BigFix Workspace 11.0

Add On Component: HCL BigFix Windows Server ESU
Requires one of the Prerequisite Programs: HCL BigFix Compliance 11.0, HCL BigFix Lifecycle 11.0, HCL BigFix Patch 11.0, HCL BigFix Remediate 11.0, or HCL BigFix Workspace 11.0

The following terms apply to the use of the Programs and add-ons:

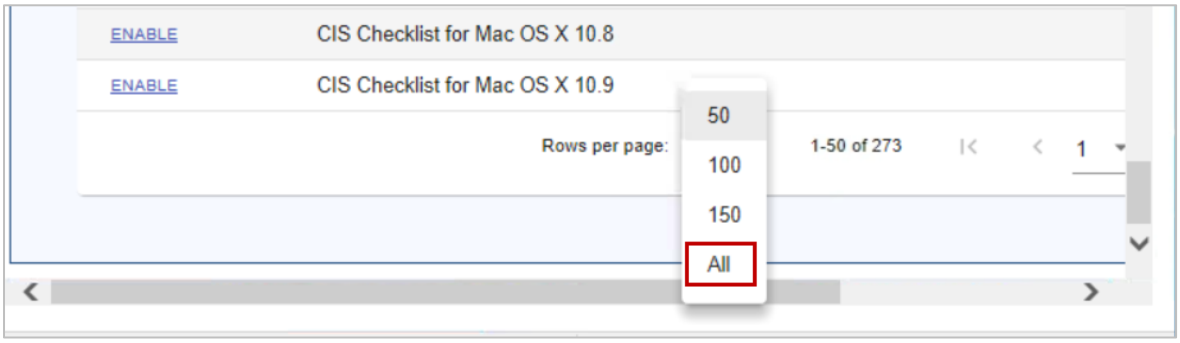
Definitions:
Licensee. For the purposes of this License Information Document, Licensee shall also mean Customer, an End User or other holder of an entitlement to which the License Information Document relates.

Connected to 'besfndwinroot' as user 'adminmo'

The Product EULA Info page closes and the dashboard updates to show a list of external sites that are included with Compliance.

7. Review the list of **Enabled Sites**. Enable the following additional sites by clicking the **Enable** link beside the site name in the **Available Sites** section.
   a. **BigFix Client Compliance (IPSec Framework)**
   b. **BigFix Client Compliance Configuration**
   c. **CIS Checklist for CentOS Linux 7**
   d. **CIS Checklist for Windows 10**
   e. **CIS Checklist for Windows 2019 MS**
   f. **Client Manager for Endpoint Protection**
   g. **SCM Reporting**
   h. **cyberfocus**

Tip: The external sites list in the BigFix License Overview dashboard are displayed in pages and show **50 rows** at a time by default. You can change the number of rows per page by scrolling to the bottom of the dashboard and selecting a different option from the **Rows per page drop-down**.

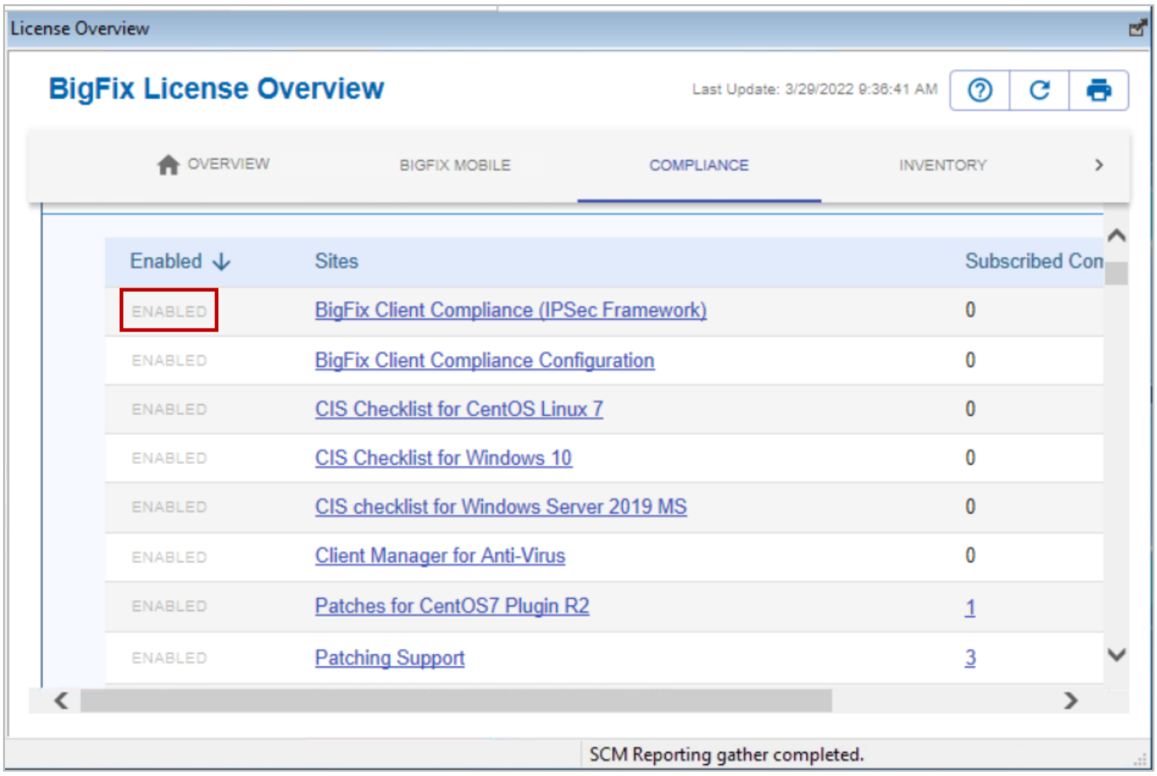


ENABLE	CIS Checklist for Mac OS X 10.8
ENABLE	CIS Checklist for Mac OS X 10.9

Rows per page: 1-50 of 273 1

Note: You can also enable one or two other checklist sites that you might be interested in reviewing (CIS, DISA STIG).

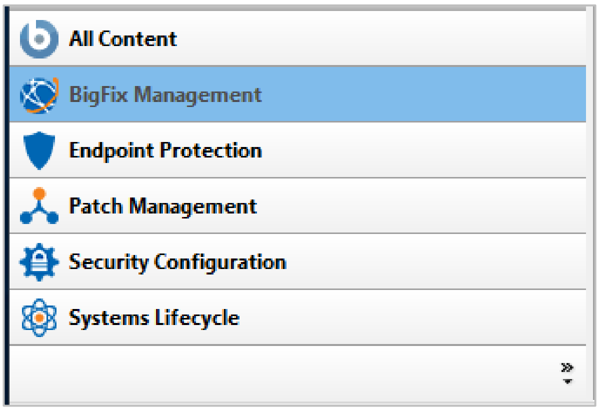
As each site is enabled, it is moved to the top of the list with an **Enabled** status.



Enabled	Sites	Subscribed Con
ENABLED	BigFix Client Compliance (IPSec Framework)	0
ENABLED	BigFix Client Compliance Configuration	0
ENABLED	CIS Checklist for CentOS Linux 7	0
ENABLED	CIS Checklist for Windows 10	0
ENABLED	CIS checklist for Windows Server 2019 MS	0
ENABLED	Client Manager for Anti-Virus	0
ENABLED	Patches for CentOS7 Plugin R2	1
ENABLED	Patching Support	3

SCM Reporting gather completed.

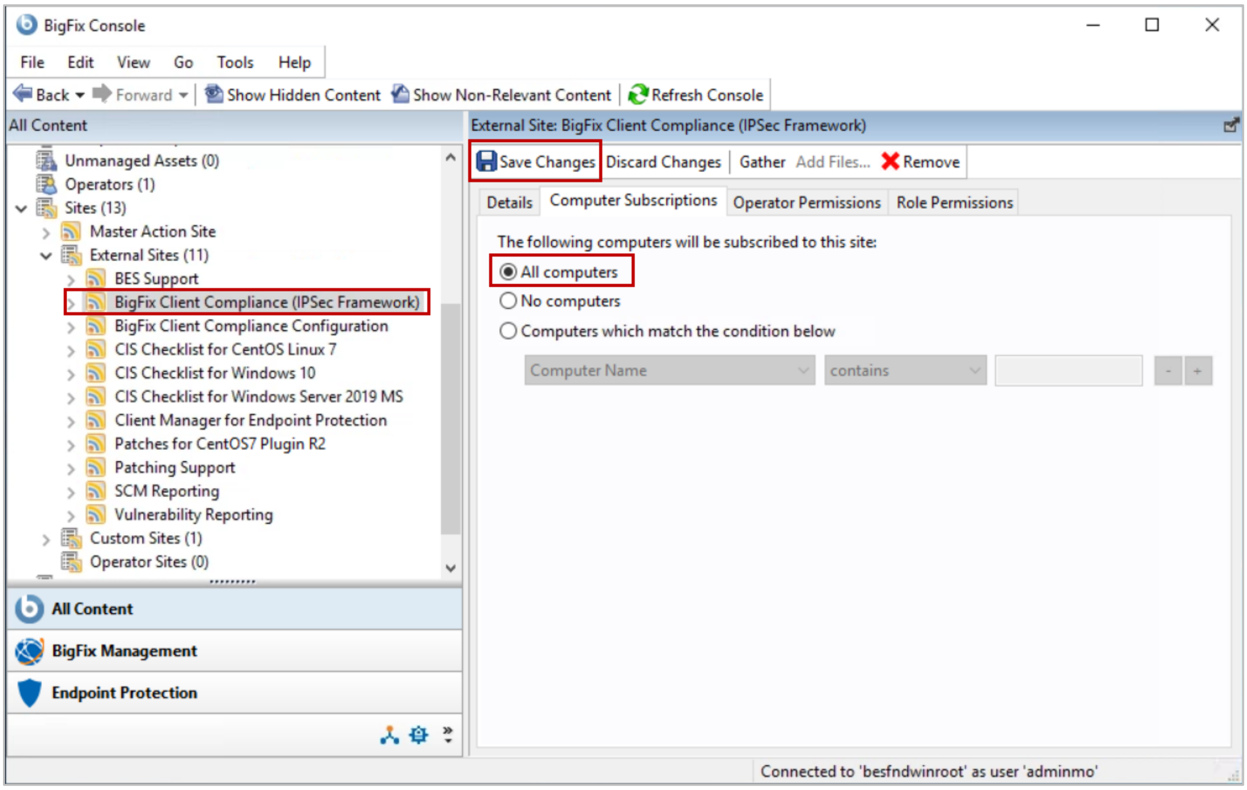
Once the sites are enabled the content for each of the enabled sites is gathered from the Content servers and imported into the BigFix database. Notice the additional domains that appear in the lower-left portion of the Console as the site content is gathered.



Note: This initial site gather might take up to 15 minutes to complete. You can monitor the progress of the gather process by opening the C:\Program Files (x86)\BigFix Enterprise\BES Server\GatherDBData\GatherDB.log file with baretail.

8. Click the **All Content** in the lower-left portion of the Console. The navigation pane displays the content that is associated with the All Content domain.
9. Expand the **Sites > External Sites** nodes in the navigation pane.

10. Perform the following steps for each of the **non-checklist** sites that you enabled in step 7 on page 10 to subscribe computers to those External **non-checklist** content sites.
    a. Click the **non-checklist** site name in the **Navigation** pane. The site details open in the upper-right portion of the Console.
    b. Click the **Computer Subscriptions** tab, then select the **All computers** radio button.
    c. Click **Save Changes** in the upper-left portion of the site details pane.



The following computers will be subscribed to this site:

● All computers
○ No computers
○ Computers which match the condition below

Note: Perform the Computer Subscription steps for **ONLY** the following external Compliance sites:

- BigFix Client Compliance (IPSec Framework)
- BigFix Client Compliance Configuration
- Client Manager for Endpoint Protection
- CyberFOCUS
- SCM Reporting

Important: Managed endpoints should never be subscribed directly to external checklist sites because external sites are read only and will not allow configuration settings to be modified from the default values. These sites are loaded as reference for creating Custom Checklists which is performed in a later lab exercise.

The Compliance content has now been enabled and you have successfully completed this exercise.

Exercise 3 – Installing the BigFix Compliance Analytics Server

BigFix Compliance provides a dedicated reporting server called BigFix Security Compliance Analytics (SCA). It has its own database separate from the BigFix Root Server database BFEnterprise. The hardware requirements are minimal because the Compliance server primarily functions as a web server. The BigFix Security Compliance Analytics server performs scheduled imports by running an

ETL process to pull information from the BFEnterprise database and update the SCA database. The Compliance reports are generated from the data in the SCA database (tem_analytics).

In this exercise, you install and configure the BigFix Security Compliance Analytics server.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens
4. Click **Security Configuration** in the lower-left portion of the Console. The navigation pane updates to display the Security Configuration content.
5. In the navigation pane, expand the **Configuration Management** node, then select **BigFix Compliance Install/Upgrade**. The installation and upgrade Fixlets for BigFix Compliance are displayed in the list area at the upper-right portion of the Console.

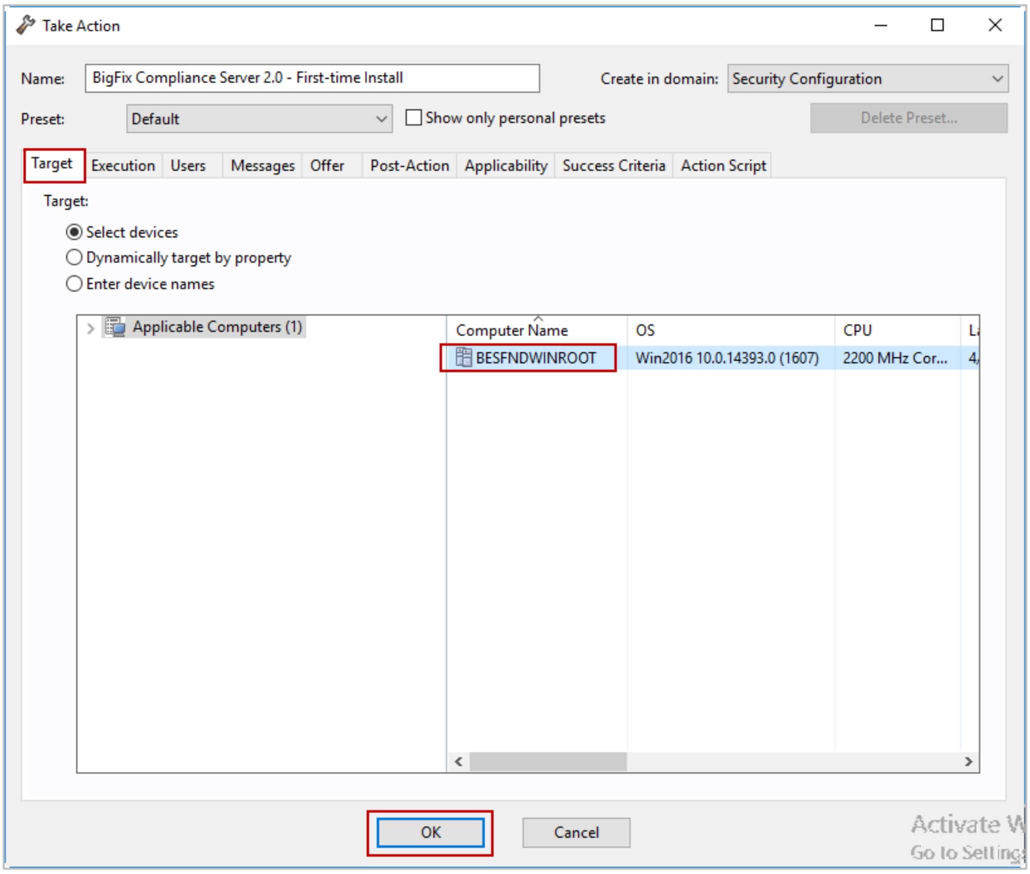
   Note: It might take several minutes for the content in the SCM Reporting site to be evaluated and the Compliance Server installation Fixlet to become relevant.

6. Select the **BigFix Compliance Server 2.0 – First-time Install** Fixlet from the list area. The details for the selected Fixlet are shown in the work area below
7. Select the **Description** tab if it is not already selected and review the installation steps.

   Note: This Fixlet deploys the installer to the target endpoint. Once the action completes, you log into the target machine to install and configure the BigFix Compliance Server.

8. Click **Take Action**. The Take Action window opens.

9. Select the **Target** tab if not already selected, then select **BESFNDWINROOT** from the list of available targets. Click **OK** to initiate the action.



Name: BigFix Compliance Server 2.0 - First-time Install

Create in domain: Security Configuration

Preset: Default

□ Show only personal presets

Target:

● Select devices
○ Dynamically target by property
○ Enter device names

Applicable Computers (1)

Computer Name	OS	CPU	L
BESFNDWINROOT	Win2016 10.0.14393.0 (1607)	2200 MHz Cor...	4

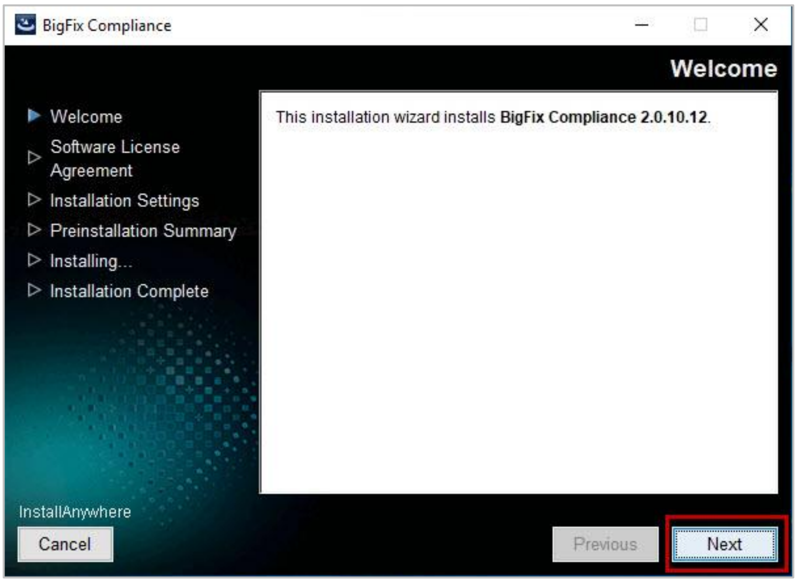
Monitor the status of the action and wait until the status changes to **Fixed** before continuing.

10. Open a **File Explorer** windows on the **BESFNDWINROOT** virtual machine and navigate to the following directory:

    C:\Program Files (x86)\BigFix Enterprise\BES Installers\Compliance\server

11. **Right-click** the self-extracting archive file beginning with the name **bfc-server-2.** and select **Run as Administrator**. The 7-Zip window opens. Leave the default directory and click **Extract** to expand the installer archive.
12. Right-click the **bfc_setup.exe** file that was extracted from the archive and select **Run as administrator**. The BigFix Compliance pane open
13. Click **OK** at the bottom of the BigFix Compliance pane to begin the installation. After several seconds, the Welcome pane opens.

14. Click **Next**.



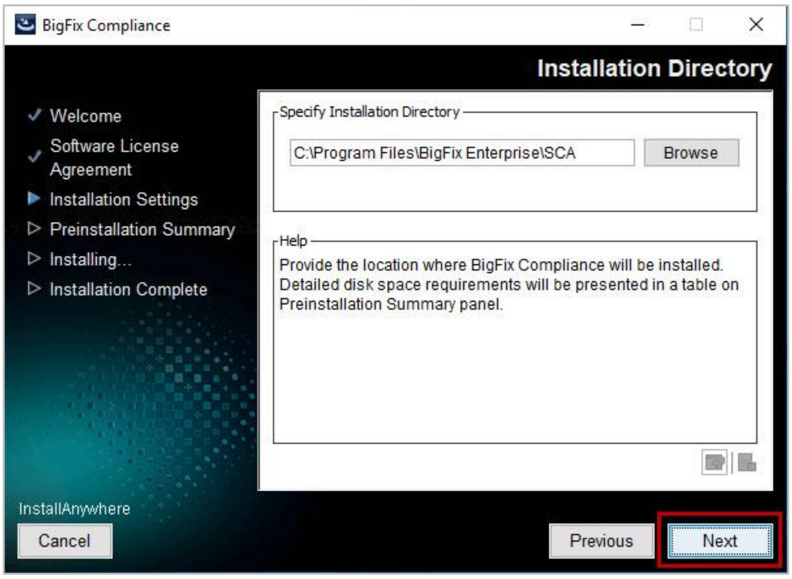
This installation wizard installs **BigFix Compliance 2.0.10.12**.

The License Agreement is displayed.

15. Select the **checkbox** to accept the license agreement. Click **Next**.

The Installation Directory window opens.

16. Click **Next** to accept the default installation directory.



Specify Installation Directory

C:\Program Files\BigFix Enterprise\SCA

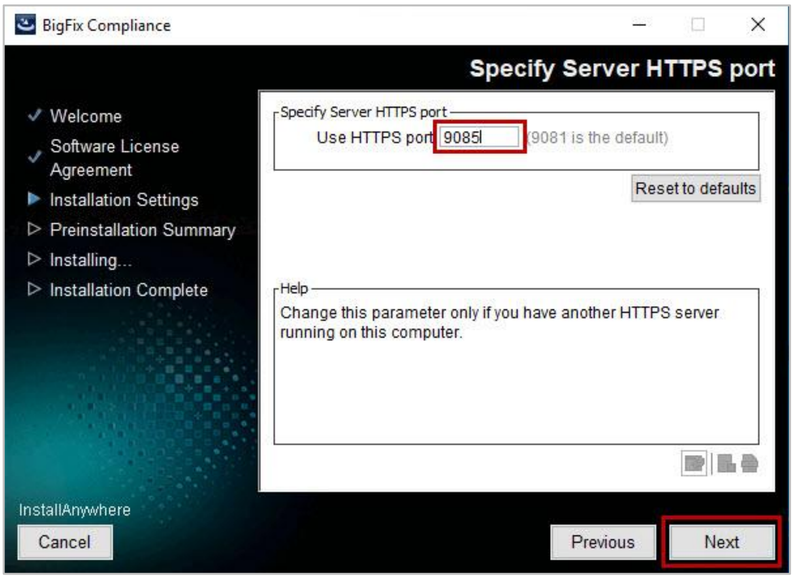
Help

Provide the location where BigFix Compliance will be installed. Detailed disk space requirements will be presented in a table on Preinstallation Summary panel.

The Specify Server HTTPS Port window is displayed.

17. Change the default port to **9085**.

    Note: The default ports for both BigFix Inventory and BigFix Security Compliance Analytics are 9081. To avoid a port conflict when both applications are installed on the same server, change the default port for this lab to **9085**.



BigFix Compliance

Specify Server HTTPS port

Specify Server HTTPS port

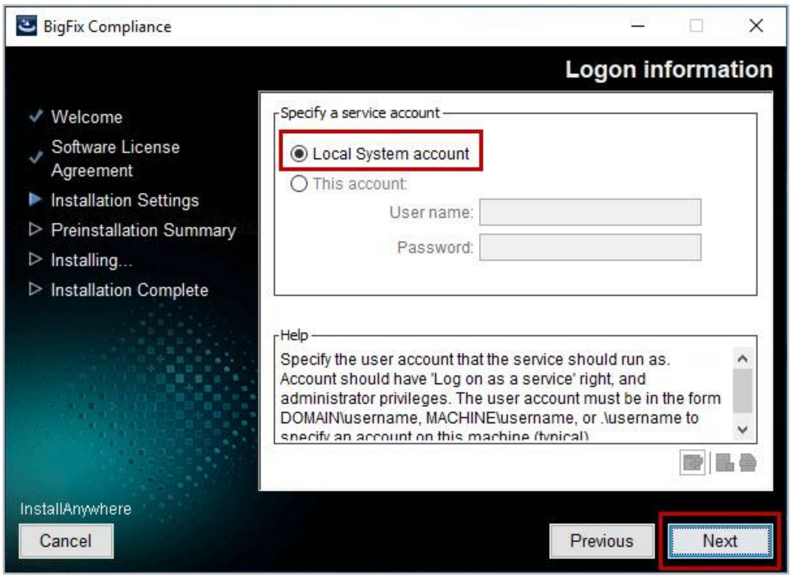
Use HTTPS port 9085 (9081 is the default)

Help

Change this parameter only if you have another HTTPS server running on this computer.

The Logon information window is displayed.

18. Accept the default setting **Local System account**. Click **Next**.



BigFix Compliance

Logon information

Specify a service account

● Local System account

○ This account:

User name:

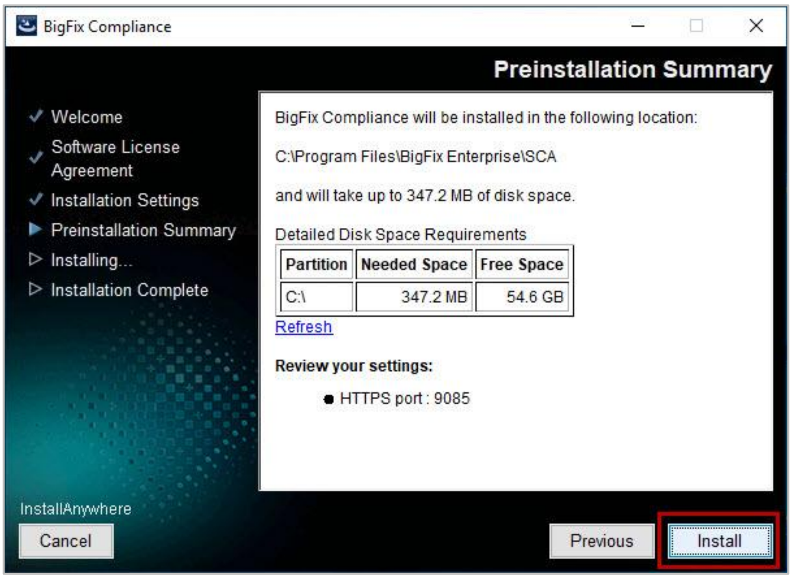
Password:

Help

Specify the user account that the service should run as. Account should have 'Log on as a service' right, and administrator privileges. The user account must be in the form DOMAIN\username, MACHINE\username, or .\username to specify an account on this machine (typical)

Note: The BigFix Security Compliance Analytics Server service can be configured to run as a service account. If you use this option in your production environment, the service account must have **Log on as a service** permissions as well as **administrator privileges** on the server.

19. Click **Next**. The Preinstallation Summary is displayed.



BigFix Compliance will be installed in the following location:

C:\Program Files\BigFix Enterprise\SCA

and will take up to 347.2 MB of disk space.

Detailed Disk Space Requirements

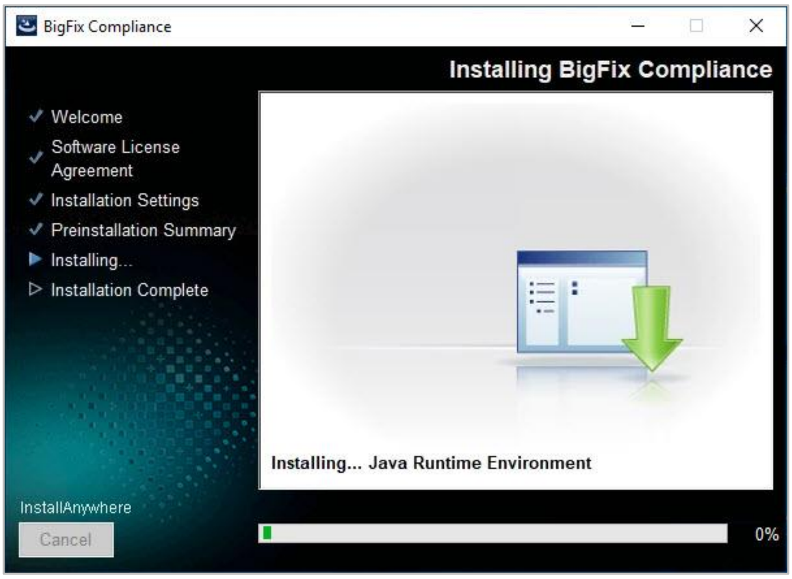
Partition	Needed Space	Free Space
C:\	347.2 MB	54.6 GB

Refresh

Review your settings:

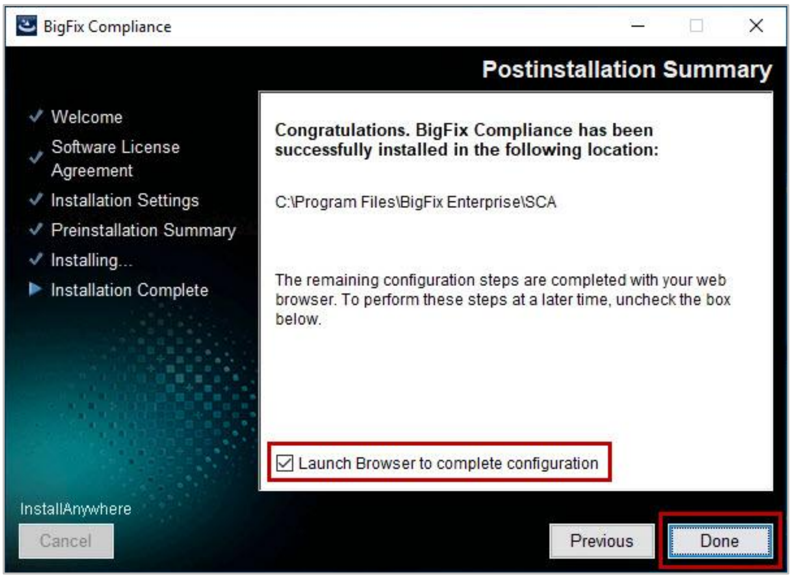
- HTTPS port : 9085

20. Click **Install**. The installation progress is shown as the software installation proceeds.



Installing... Java Runtime Environment

21. After the installation completes, the **Postinstallation Summary** window opens. Verify that the **Launch Browser to complete configuration** option is selected and click **Done**. A browser launches where the remaining setup and configuration steps are performed.



Congratulations. BigFix Compliance has been successfully installed in the following location:

C:\Program Files\BigFix Enterprise\SCA

The remaining configuration steps are completed with your web browser. To perform these steps at a later time, uncheck the box below.

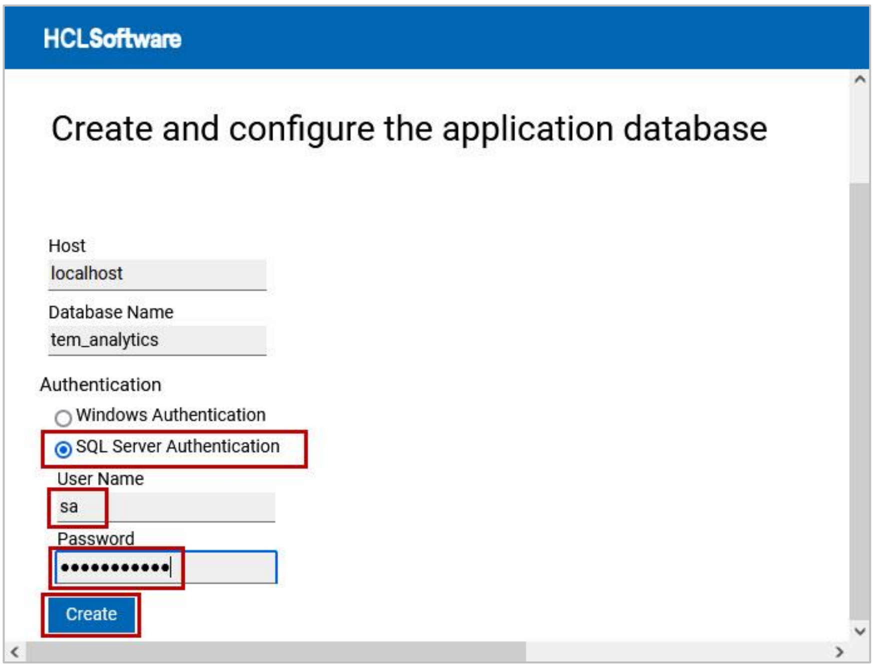
☑ Launch Browser to complete configuration

Note: Once the browser opens, you might see a Security Warning about a security risk connecting to the Compliance Server. If you see this warning, accept the risk as required by the browser in use and continue connecting to the Compliance Server.

Tip: If the browser does not automatically open, double-click the Firefox icon on the Windows Desktop and enter the following URL in the address bar:

https://localhost:9085

22. Enter the following values on the **Host and Database Name on the Create and configure the application database** window. Click **Create**.
    - Select the **SQL Server Authentication** option
    - Enter **sa** in the user Name field
    - Enter **bigfixrocks** in the Password field



HCLSoftware

Create and configure the application database

Host
localhost

Database Name
tem_analytics

Authentication

○ Windows Authentication

● SQL Server Authentication

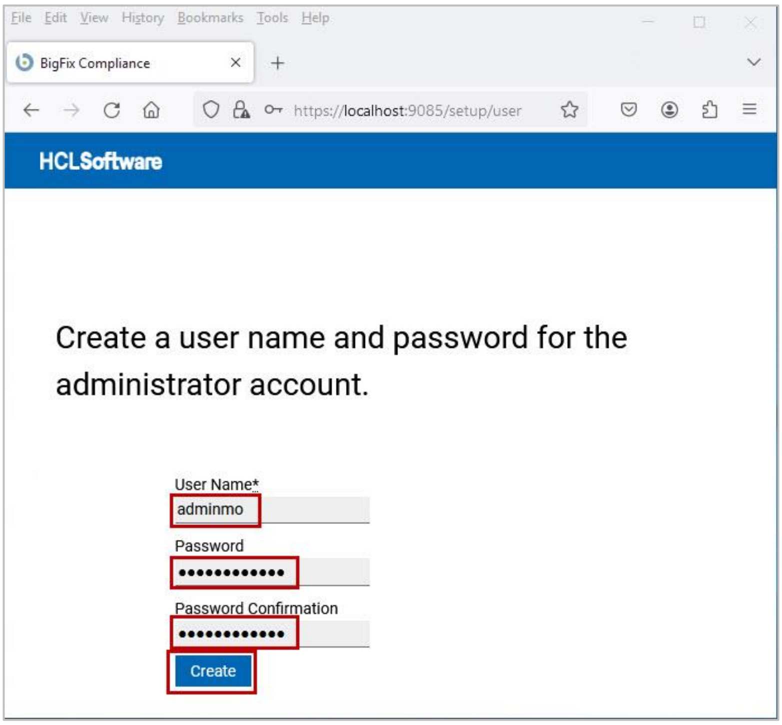
User Name
sa

Password
•••••••••••

Note: It might take several minutes for the database to be created.

23. Next you create the local administrator account for the Security Compliance Analytics server. Enter the administrator account information as follows. Click **Create**.
    - User Name: **adminmo**
    - Password: **B1gfixrocks!**
    - Password Confirmation: **B1gfixrocks!**

Important: Be sure and verify that you include the exclamation point at the end of the password so that the password complexity requirements of the Security Compliance Analytics server are satisfied.



File Edit View History Bookmarks Tools Help
BigFix Compliance
https://localhost:9085/setup/user

HCLSoftware

Create a user name and password for the administrator account.

User Name*
adminmo

Password
••••••••••••

Password Confirmation
••••••••••••

24. Next you create the Data Source which informs the Compliance Server of the BigFix database location and optionally the Web Reports Database. To complete this configuration, enter the following information on the connection parameters page and click **Create**.

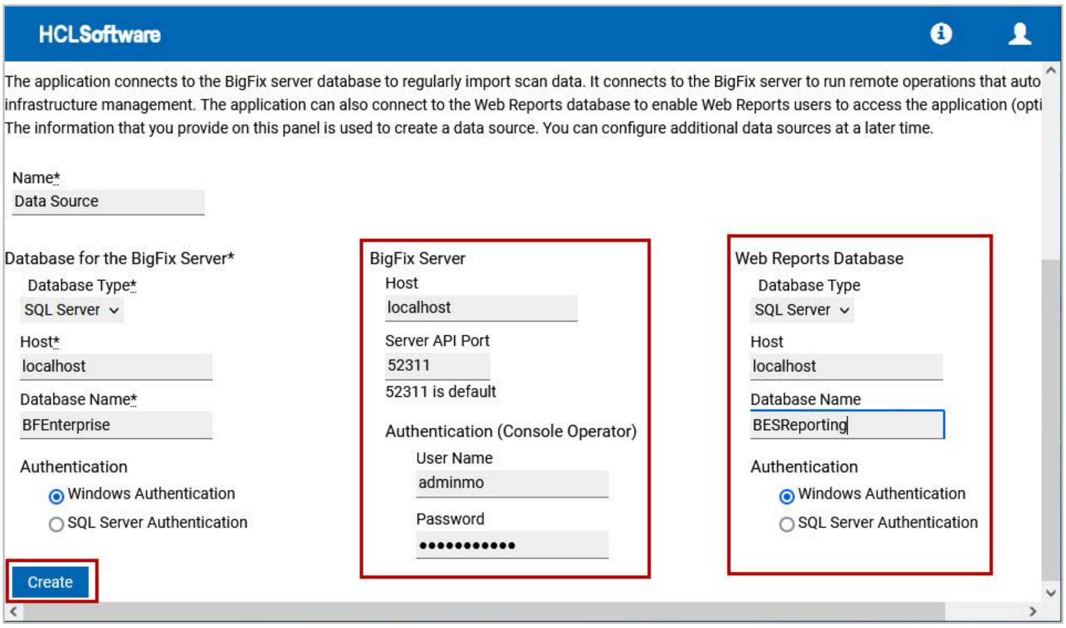
    Database for the BigFix Server section: Accept all the default values

    BigFix Server section:

    - Host: **localhost**
    - Server API Port: **52311**
    - Authentication User Name: **adminmo**
    - Authentication Password: **B1gfixrocks**

    Web Reports Database section:

    - Database Type: **SQL Server** (default)
    - Host: **localhost**
    - Database Name: **BESReporting**
    - Authentication: **Windows Authentication** (default)



The application connects to the BigFix server database to regularly import scan data. It connects to the BigFix server to run remote operations that auto
infrastructure management. The application can also connect to the Web Reports database to enable Web Reports users to access the application (opti
The information that you provide on this panel is used to create a data source. You can configure additional data sources at a later time.

Name*: Data Source

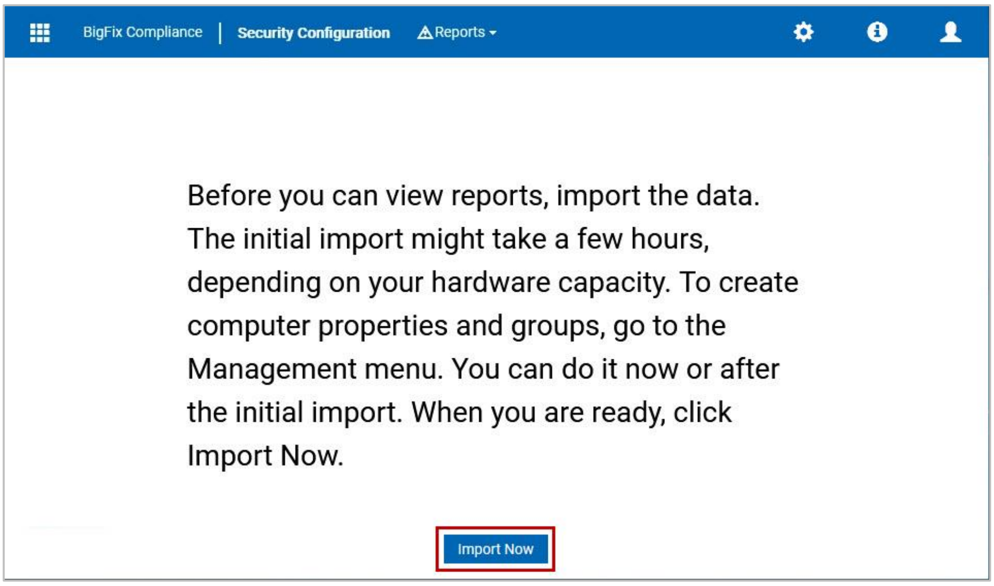
Database for the BigFix Server*
- Database Type*: SQL Server
- Host*: localhost
- Database Name*: BFEnterprise
- Authentication: ● Windows Authentication ○ SQL Server Authentication

BigFix Server
- Host: localhost
- Server API Port: 52311 (52311 is default)
- Authentication (Console Operator)
  - User Name: adminmo
  - Password: ●●●●●●●●●●●

Web Reports Database
- Database Type: SQL Server
- Host: localhost
- Database Name: BESReporting
- Authentication: ● Windows Authentication ○ SQL Server Authentication

Note: It will take several minutes for the Data Source to be created. Once the Data Source is created the **Import** page is displayed. Validation is performed before the Data Source is created and errors are highlighted on the page. If errors are displayed, correct the issues (mistyped passwords etc…) and click **Create** again.

25. Click **Import Now** to perform the initial ETL from the BigFix database to the Security Compliance Analytics database.



Before you can view reports, import the data. The initial import might take a few hours, depending on your hardware capacity. To create computer properties and groups, go to the Management menu. You can do it now or after the initial import. When you are ready, click Import Now.

Note: It will take several minutes for the import to complete. Once the Import has successfully completed, the BigFix Compliance Overview page is displayed.

You now configure the Java heap size for SCA.

26. Stop the **BigFix Compliance** service.
27. **Right-click** the Windows **File Explorer** and select **Run as Administrator**. Navigate to the following folder;

    C:\Program Files\BigFix Enterprise\SCA\wlp\usr\servers\server1\

28. Open the **jvm.options** file using **Notepad** and make the following changes to the file;

    Remove the comment (#) from the maximum and minimum heap size entries and update the settings as shown below:

    Original Settings-
    ```
    # Override maximum heap size
    #-Xmx4g

    # Override minimum heap size
    #-Xms4g
    ```

    Modified Settings –
    ```
    # Override maximum heap size
    -Xmx5g

    # Override minimum heap size
    -Xms4g
    ```

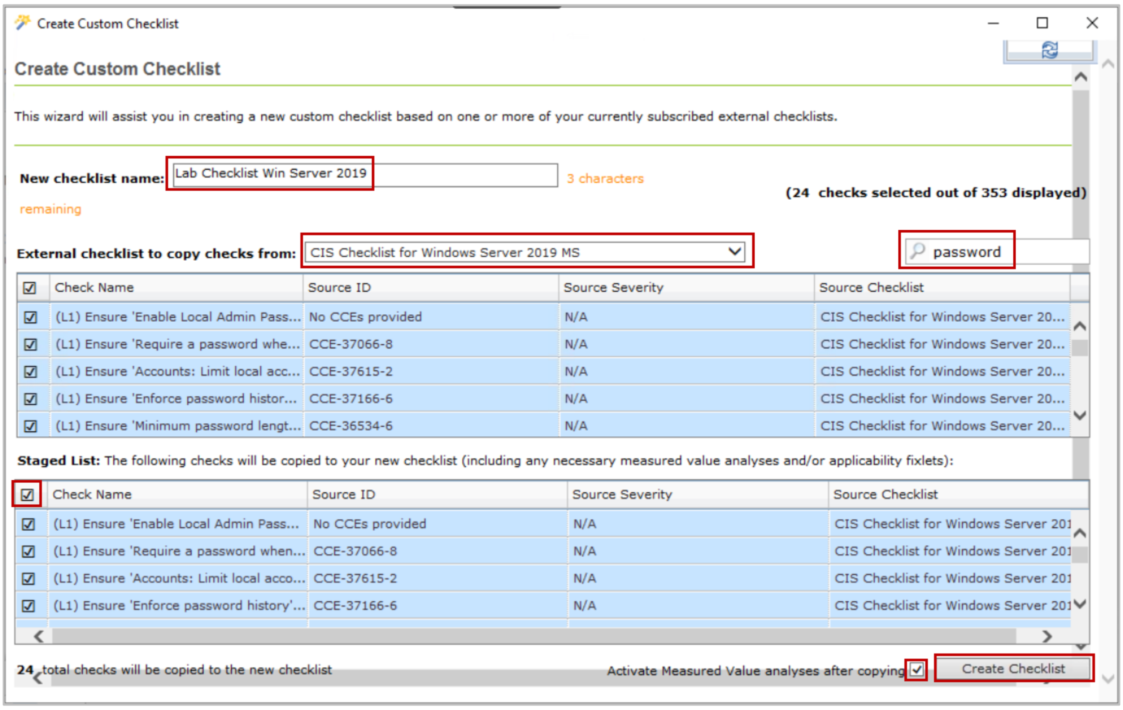
29. Save and close the **jvm.options** file.
30. Start the **BigFix Compliance** service.

You have now successfully completed Exercise 3.

Exercise 4 - Creating a Custom Checklist – BigFix Console

In this exercise, you create and configure a custom Security Configuration Management checklist that is used to enforce security policies.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens.
4. Click **Security Configuration** in the lower-left portion of the Console. The navigation pane updates to show the Security Configuration content.
5. In the navigation pane, expand **Configuration Management > Checklist Tools** nodes then select **Create Custom Checklist**. The Create Custom Checklist wizard opens in the list pane.
6. Perform the following steps to create the custom checklist:
   a. Enter **Lab Checklist Win Server 2019** in the New checklist name field
   b. Select **CIS Checklist for Windows 2019 MS** from the **External checklist to copy checks from** drop down box.
   c. Enter **password** in the **Search** box that is located to the right of the **External checklist to copy checks from** drop-down.
   d. Place a **check** beside the **Check Name** box. This selects all the checks and places them in the Staged List at the bottom of the wizard.
   e. Place a **check** beside the **Activate Measured Value analyses after copying** box in the lower-right portion of the wizard.
   f. Click **Create Checklist**.



Create Custom Checklist

Create Custom Checklist

This wizard will assist you in creating a new custom checklist based on one or more of your currently subscribed external checklists.

New checklist name: Lab Checklist Win Server 2019 3 characters remaining

(24 checks selected out of 353 displayed)

External checklist to copy checks from: CIS Checklist for Windows Server 2019 MS

password

☑	Check Name	Source ID	Source Severity	Source Checklist
☑	(L1) Ensure 'Enable Local Admin Pass...	No CCEs provided	N/A	CIS Checklist for Windows Server 20...
☑	(L1) Ensure 'Require a password whe...	CCE-37066-8	N/A	CIS Checklist for Windows Server 20...
☑	(L1) Ensure 'Accounts: Limit local acc...	CCE-37615-2	N/A	CIS Checklist for Windows Server 20...
☑	(L1) Ensure 'Enforce password histor...	CCE-37166-6	N/A	CIS Checklist for Windows Server 20...
☑	(L1) Ensure 'Minimum password lengt...	CCE-36534-6	N/A	CIS Checklist for Windows Server 20...

Staged List: The following checks will be copied to your new checklist (including any necessary measured value analyses and/or applicability fixlets):

☑	Check Name	Source ID	Source Severity	Source Checklist
☑	(L1) Ensure 'Enable Local Admin Pass...	No CCEs provided	N/A	CIS Checklist for Windows Server 201
☑	(L1) Ensure 'Require a password when...	CCE-37066-8	N/A	CIS Checklist for Windows Server 201
☑	(L1) Ensure 'Accounts: Limit local acco...	CCE-37615-2	N/A	CIS Checklist for Windows Server 201
☑	(L1) Ensure 'Enforce password history'...	CCE-37166-6	N/A	CIS Checklist for Windows Server 201

24 total checks will be copied to the new checklist

Activate Measured Value analyses after copying ☑ Create Checklist

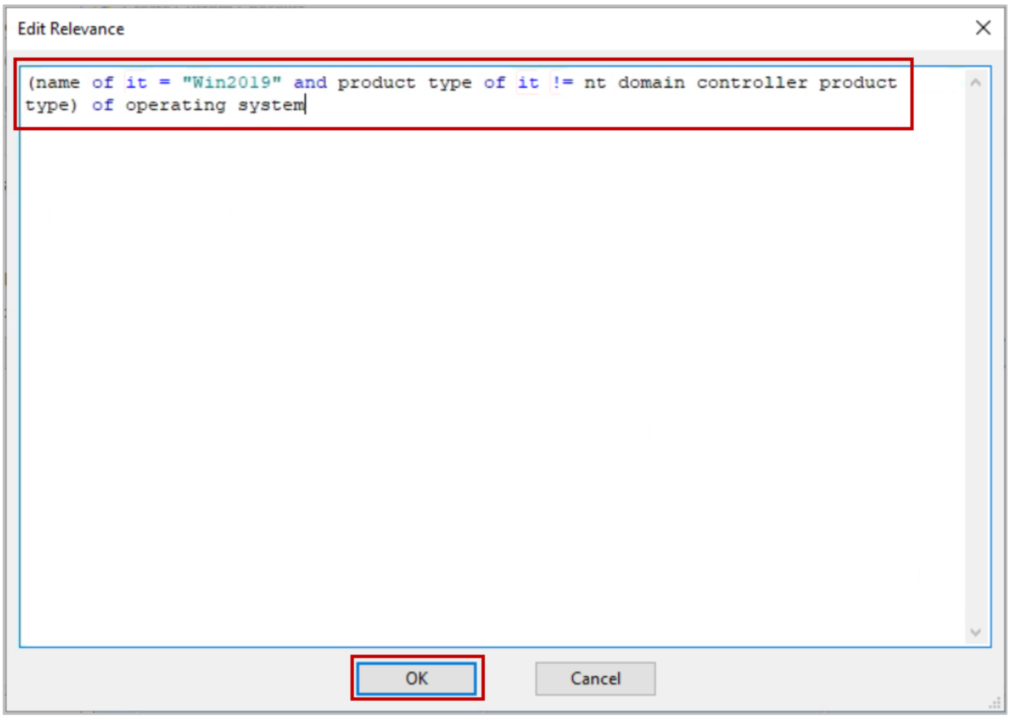
The custom checklist site is created and the site details page opens.

7. Click the **Details** tab. Enter **Password related audit checks for Windows Server 2019 Member Server machines** in the **Description** field,

8. Click the **Computer Subscriptions** tab. Define the computer subscriptions for the custom checklist by performing the following steps:
    a. Select the **Computers which match the condition below** option.
    b. Select **Relevance Expression** from the first drop-down box (it is located at the top of the list).
    c. Accept the default **is true** setting in the second drop-down box.
    d. Click **Edit Relevance** and enter the following Relevance Expression in the text field.

    Note: You must modify the "quotes" around the "Win2019" if you cut and paste the Relevance expression below from the Lab Guide.

    ```
    (name of it = "Win2019" and product type of it != nt
    domain controller product type) of operating system
    ```



```
(name of it = "Win2019" and product type of it != nt domain controller product
type) of operating system
```

    e. Click **OK**.
    f. Click **Save Changes** in the upper-left portion of the Custom Site pane.
9. In the **Navigation** pane expand the **Configuration Management > Custom Checklists > Lab Checklist Win Server 2019** nodes. Notice the standard site subcategories (Fixlets and Tasks, Baselines, Analyses etc…).
10. Click **Fixlets and Tasks** under the **Lab Checklist Win Server 2019** node. The Fixlets and Tasks are shown in the list area in the upper-right portion of the Console.

    Note: It might take several minutes for the computers that are subscribed to the custom checklist site to report their compliance status. The **Show Non-Relevant Content** button can be toggled to show non-relevant content. The list area will be blank until one or more Fixlets are reported as Relevant.

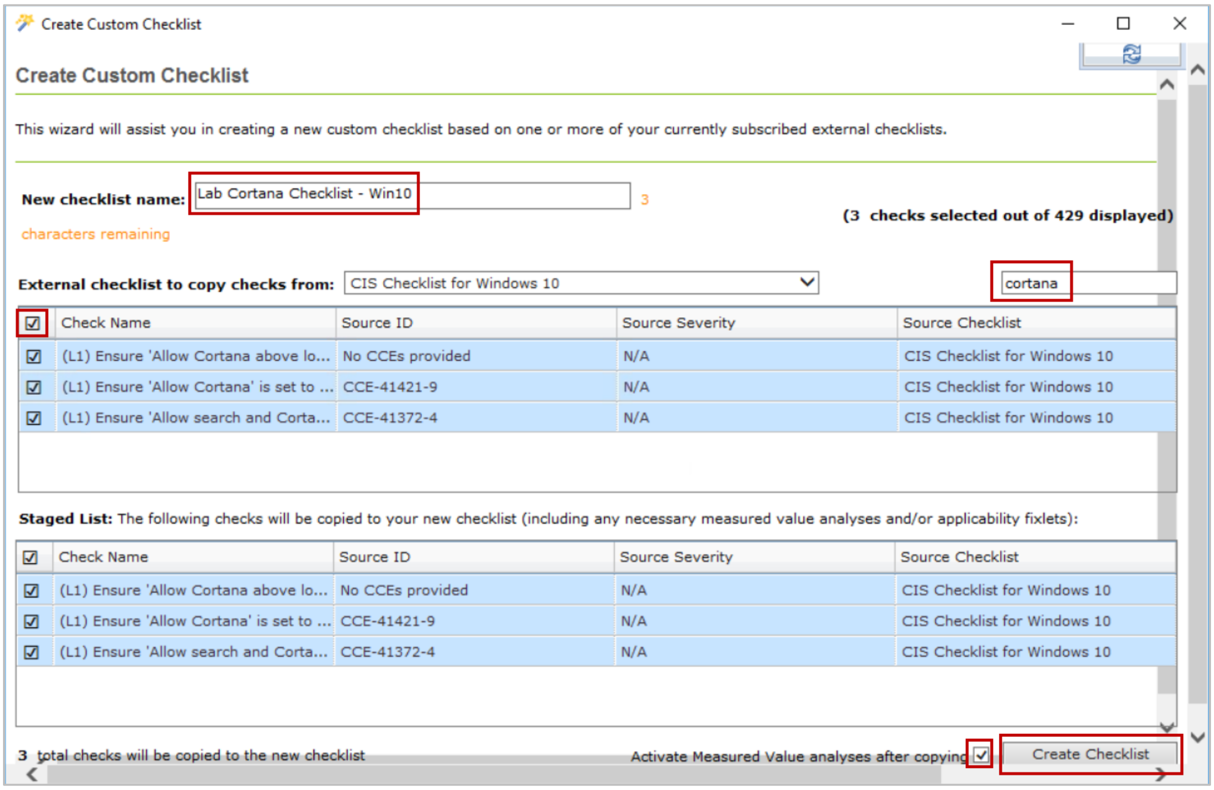
    With respect to Compliance, Relevant Fixlets represent non-compliant configurations while non-Relevant Fixlets indicate that all subscribed computers are compliant with the configuration setting.

You have now successfully completed Exercise 4.

Exercise 5 – Create a Windows 10 Custom Checklist - Console

In this exercise, you create a custom checklist based on Compliance checks from the CIS Checklist for Windows 10 External Checklist site that you previously enabled.

1. Create a custom checklist named **Lab Cortana Checklist – Win10** by using the steps in Exercise 4 - Creating a Custom Checklist on page 22 as a guide. Use the information below as a reference for your custom checklist:
    - New checklist name: **Lab Cortana Checklist – Win10**
    - Select the following external source checklist: **CIS Checklist for Windows 10**
    - Search box criteria: **Cortana**
    - Select all available Cortana checks
    - Select **Activate Measured Value analyses after copying** option, then click **Create Checklist**.



Create Custom Checklist

This wizard will assist you in creating a new custom checklist based on one or more of your currently subscribed external checklists.

New checklist name: Lab Cortana Checklist - Win10 3 characters remaining

(3 checks selected out of 429 displayed)

External checklist to copy checks from: CIS Checklist for Windows 10

cortana

☑	Check Name	Source ID	Source Severity	Source Checklist
☑	(L1) Ensure 'Allow Cortana above lo...	No CCEs provided	N/A	CIS Checklist for Windows 10
☑	(L1) Ensure 'Allow Cortana' is set to ...	CCE-41421-9	N/A	CIS Checklist for Windows 10
☑	(L1) Ensure 'Allow search and Corta...	CCE-41372-4	N/A	CIS Checklist for Windows 10

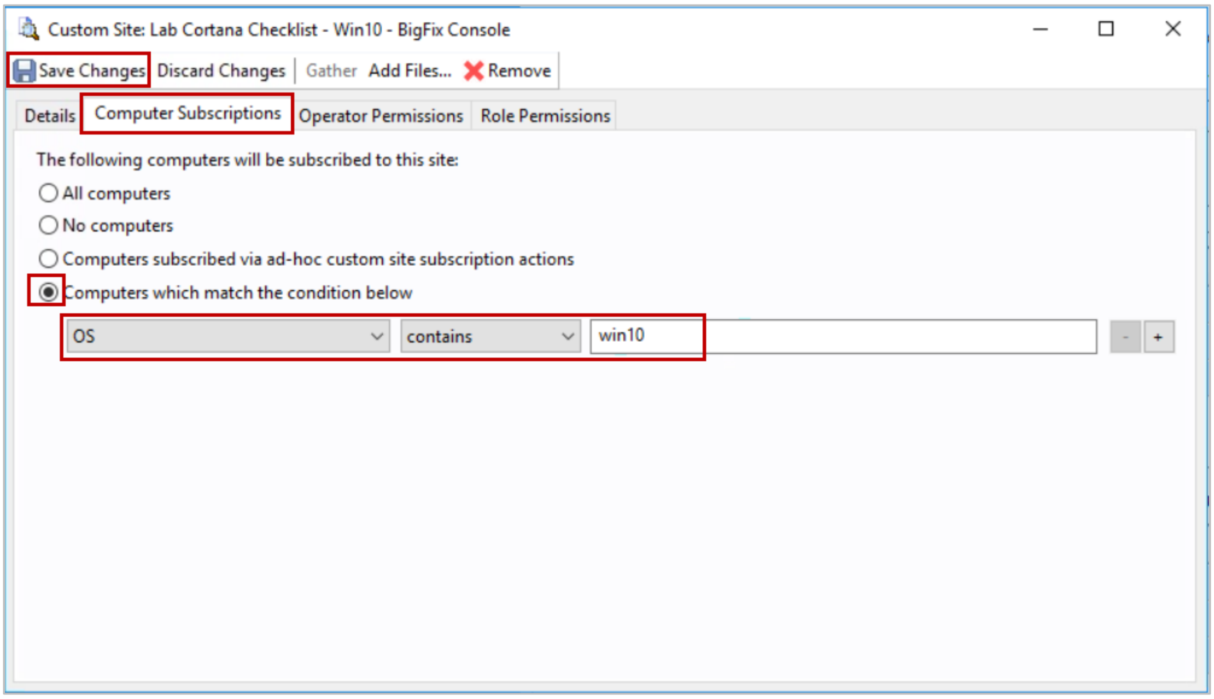
Staged List: The following checks will be copied to your new checklist (including any necessary measured value analyses and/or applicability fixlets):

☑	Check Name	Source ID	Source Severity	Source Checklist
☑	(L1) Ensure 'Allow Cortana above lo...	No CCEs provided	N/A	CIS Checklist for Windows 10
☑	(L1) Ensure 'Allow Cortana' is set to ...	CCE-41421-9	N/A	CIS Checklist for Windows 10
☑	(L1) Ensure 'Allow search and Corta...	CCE-41372-4	N/A	CIS Checklist for Windows 10

3 total checks will be copied to the new checklist

Activate Measured Value analyses after copying ☑

- Subscribe **Win10** endpoints to the custom checklist site. Select the **Computers which match the condition below option**. Then chose **OS** from the first drop down, **contains** from the second drop-down box, and enter **win10** in the text field. Click **Save Changes**.



Custom Site: Lab Cortana Checklist - Win10 - BigFix Console

The following computers will be subscribed to this site:

○ All computers
○ No computers
○ Computers subscribed via ad-hoc custom site subscription actions
● Computers which match the condition below

OS | contains | win10

You have now successfully completed Exercise 5.

Exercise 6 – Create a CentOS7 Custom Checklist - WebUI

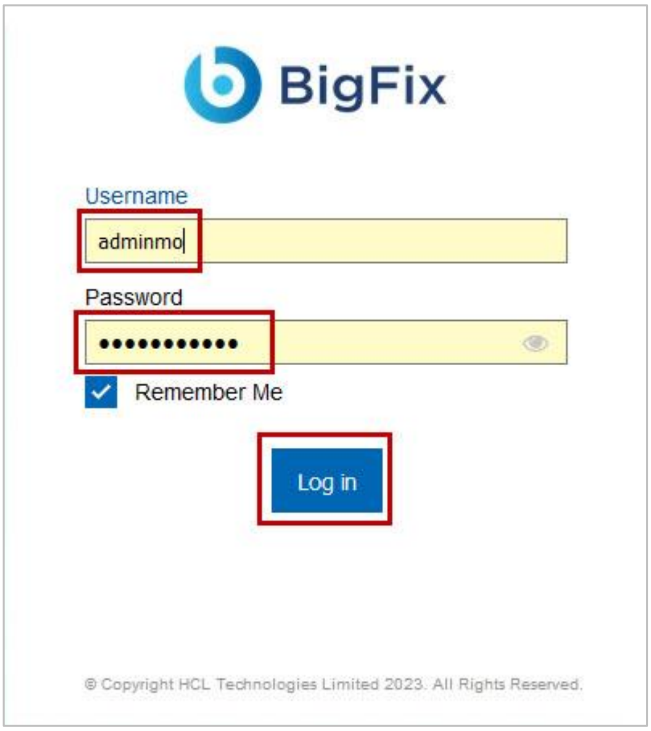
In this exercise, you use the WebUI to create a custom checklist based on Compliance checks from the CIS Checklist for CentOS Linux 7 external Checklist site that you previously enabled.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double-click the **Firefox** icon on the Windows desktop. The Firefox web browser opens.
3. Access the **WebUI** by entering the following URL in the address bar of the **Firefox** browser:

   ```
   https://besfndwinroot
   ```

   Note: If you receive the security warning, click **Advanced**, then click **Accept the Risk and Continue**. The WebUI Login page is shown.

4. Enter the **Username** as **adminmo** and the **Password** as **B1gfixrocks**. Click **Login**.



BigFix

Username

adminmo

Password

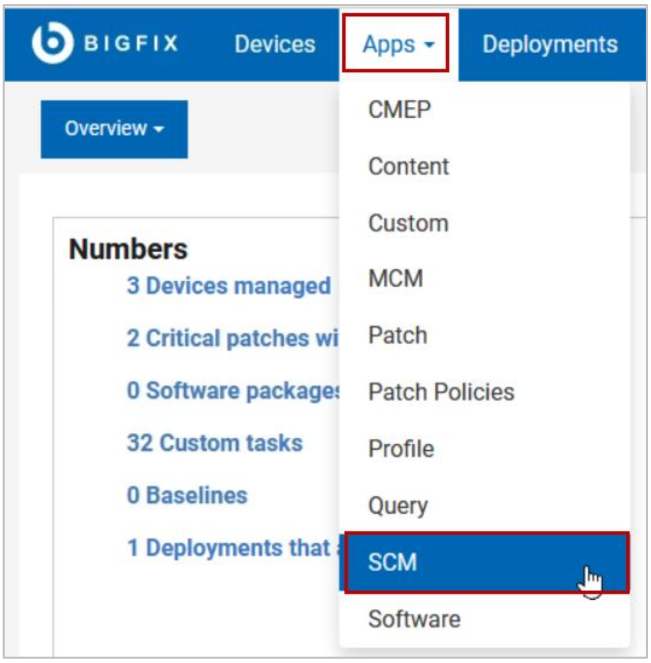
●●●●●●●●●●●

☑ Remember Me

© Copyright HCL Technologies Limited 2023. All Rights Reserved.

The WebUI Overview page opens.

5. Select **SCM** from the **Apps** tab at the top of the WebUI Overview page.



Numbers

3 Devices managed

2 Critical patches wi

0 Software package:

32 Custom tasks

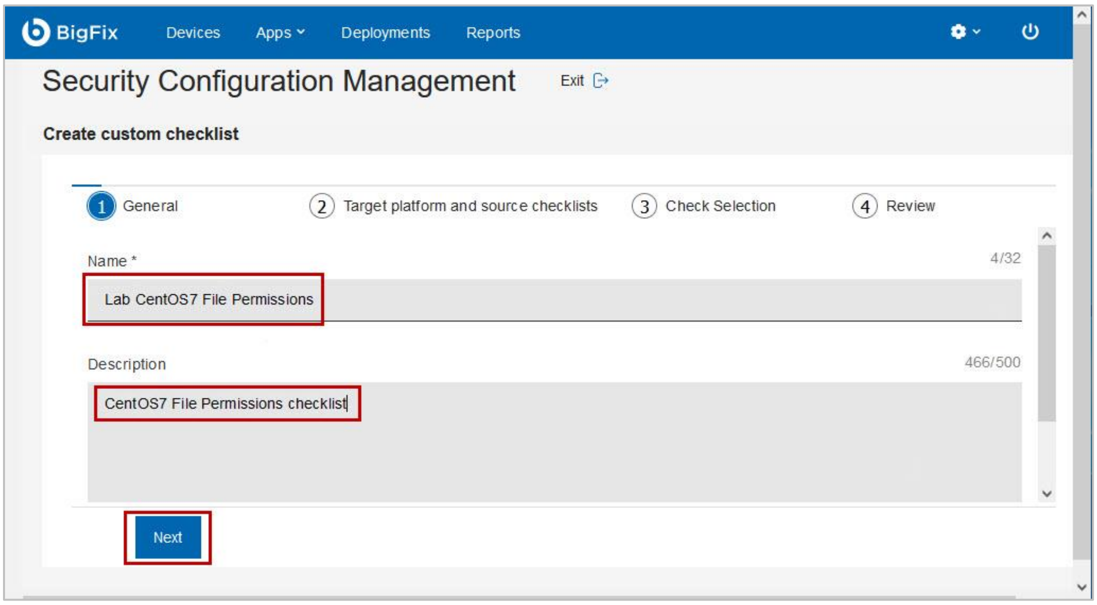
0 Baselines

1 Deployments that

The Security Configuration Management page opens and displays the 2 custom checklists that you previously created.

6. Click **Create** in the upper portion of the **Security Configuration Management** page then click **Create custom checklist** from the drop-down menu. The General step of the Create custom checklist page opens.

7. Enter the custom checklist Name and Description as follows:
    - Name: **Lab CentOS7 File Permissions**
    - Description: **CentOS7 File Permissions checklist**



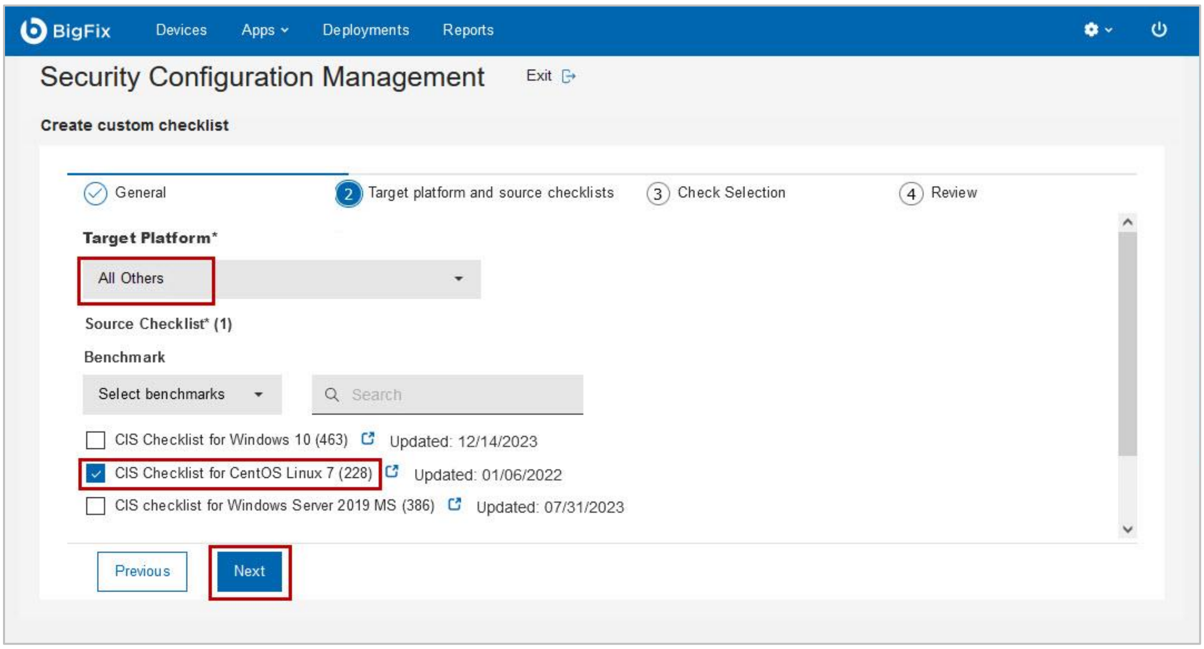
Security Configuration Management

Create custom checklist

Name *: Lab CentOS7 File Permissions

Description: CentOS7 File Permissions checklist

8. Click **Next**. The Target platform and source checklists step is displayed.
9. Select **All Others** from the **Target Platform** drop-down box.
10. Place a **check** beside the **CIS Checklist for CentOS Linux 7** checklist.



Security Configuration Management

Create custom checklist

Target Platform*: All Others

Source Checklist* (1)

Benchmark

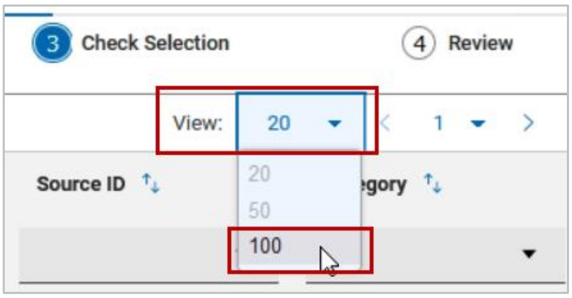
□ CIS Checklist for Windows 10 (463) Updated: 12/14/2023

☑ CIS Checklist for CentOS Linux 7 (228) Updated: 01/06/2022

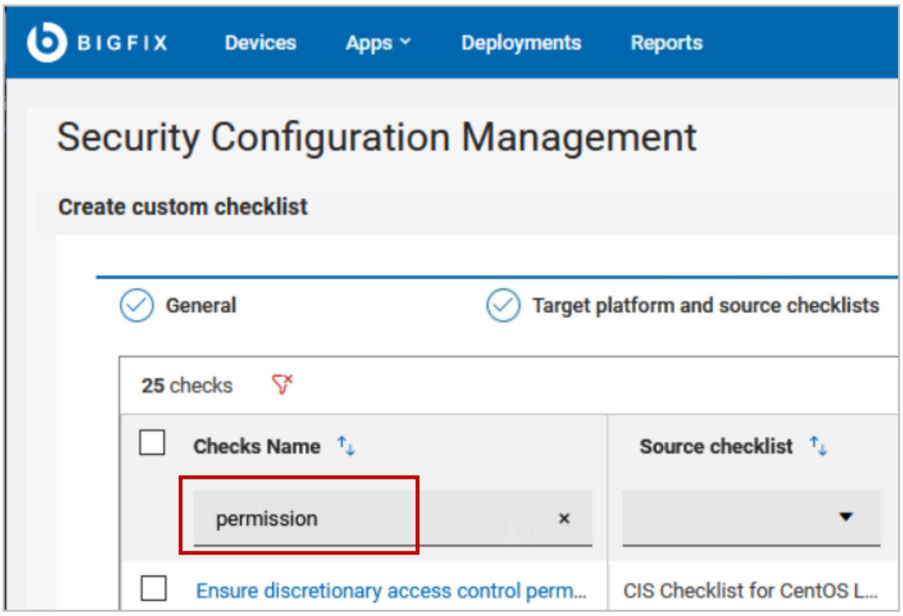
□ CIS checklist for Windows Server 2019 MS (386) Updated: 07/31/2023

11. Click **Next**. The Check Selection step is displayed.

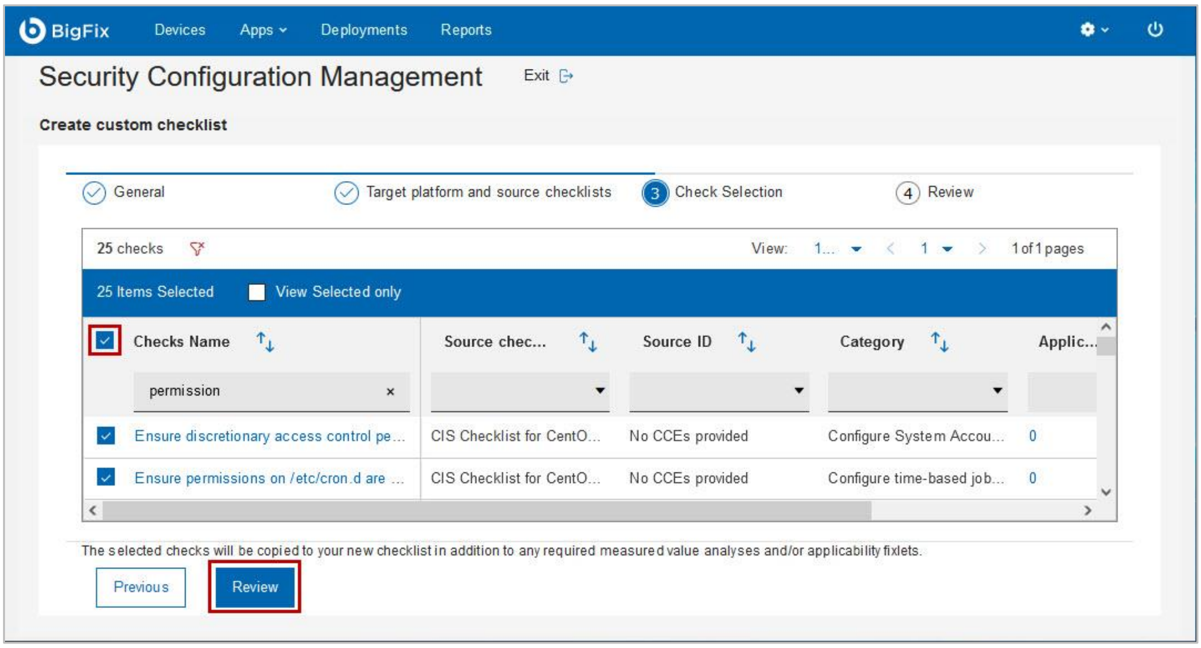
12. Select **100** from the **View** drop-down box to display up to 100 checks per page.



13. Enter **permission** in the **Checks Name** search box. The list of available checks is filtered to show only those with the string permission in the name.


BIGFIX
Devices
Apps
Deployments
Reports
Security Configuration Management
Create custom checklist
General
Target platform and source checklists
25 checks
Checks Name
Source checklist
permission
Ensure discretionary access control perm...
CIS Checklist for CentOS L...

14. Place a **check** in the box beside the **Checks Name** column header to select all the checks from the filtered list. Click **Review**.

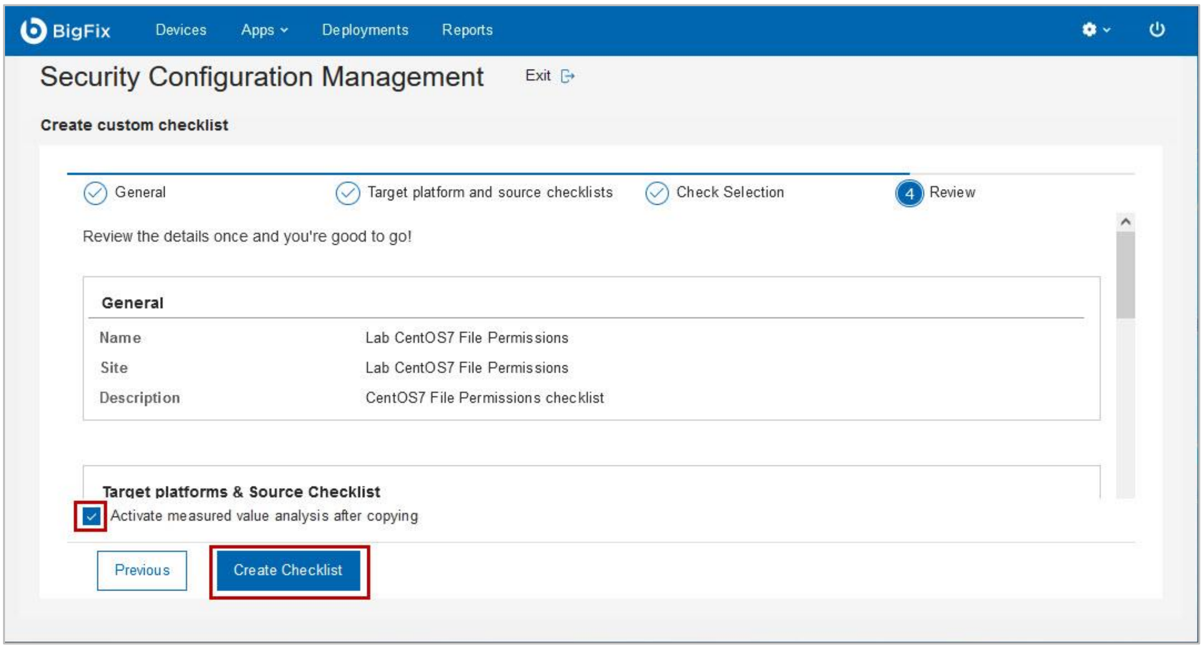


☑ Checks Name	Source chec...	Source ID	Category	Applic...
☑ Ensure discretionary access control pe...	CIS Checklist for CentO...	No CCEs provided	Configure System Accou...	0
☑ Ensure permissions on /etc/cron.d are ...	CIS Checklist for CentO...	No CCEs provided	Configure time-based job...	0

The selected checks will be copied to your new checklist in addition to any required measured value analyses and/or applicability fixlets.

The Review step page is displayed.

15. Place a **check** beside the **Activate measured value analysis after copying**. Click **Create Checklist**.



Security Configuration Management

Create custom checklist

Review the details once and you're good to go!

General

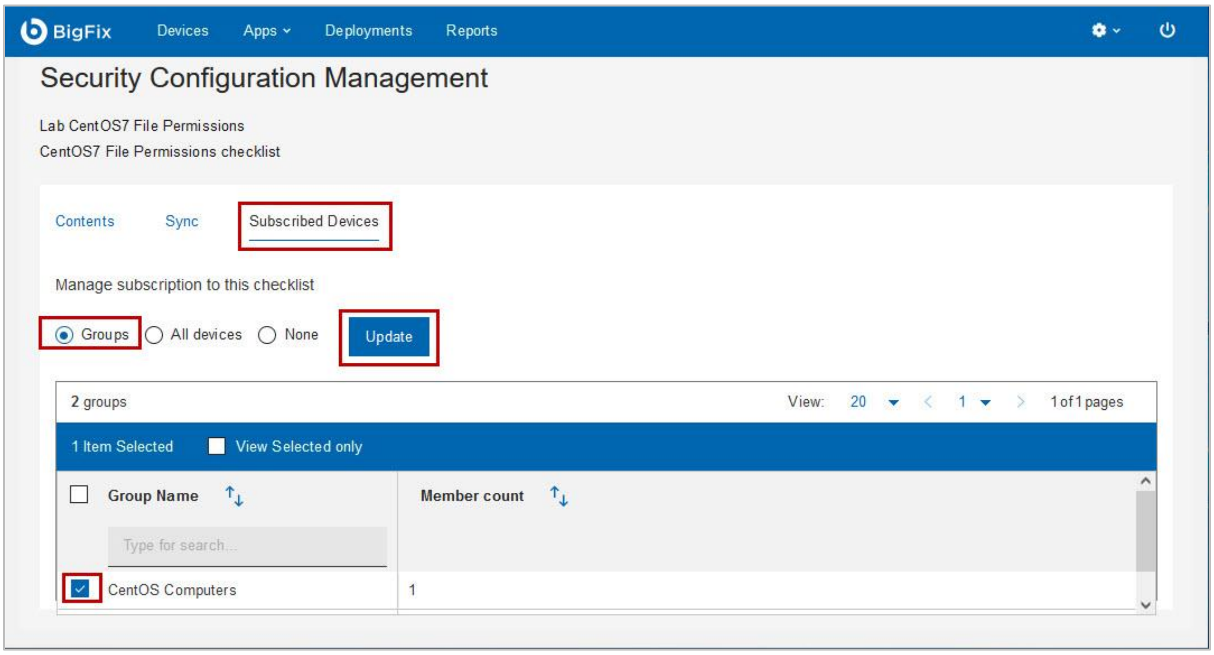
Name	Lab CentOS7 File Permissions
Site	Lab CentOS7 File Permissions
Description	CentOS7 File Permissions checklist

Target platforms & Source Checklist

☑ Activate measured value analysis after copying

A message is displayed showing that the checklist is being created. After the custom checklist is created, the CentOS7 File Permissions checklist page opens.

16. Click the **Subscribed Devices** tab. The Manage subscriptions options for the custom checklist are shown.
17. Select the **Groups** option, then place a check beside the **CentOS Computers** group. Click **Update**.



Security Configuration Management

Lab CentOS7 File Permissions
CentOS7 File Permissions checklist

Manage subscription to this checklist

● Groups ○ All devices ○ None

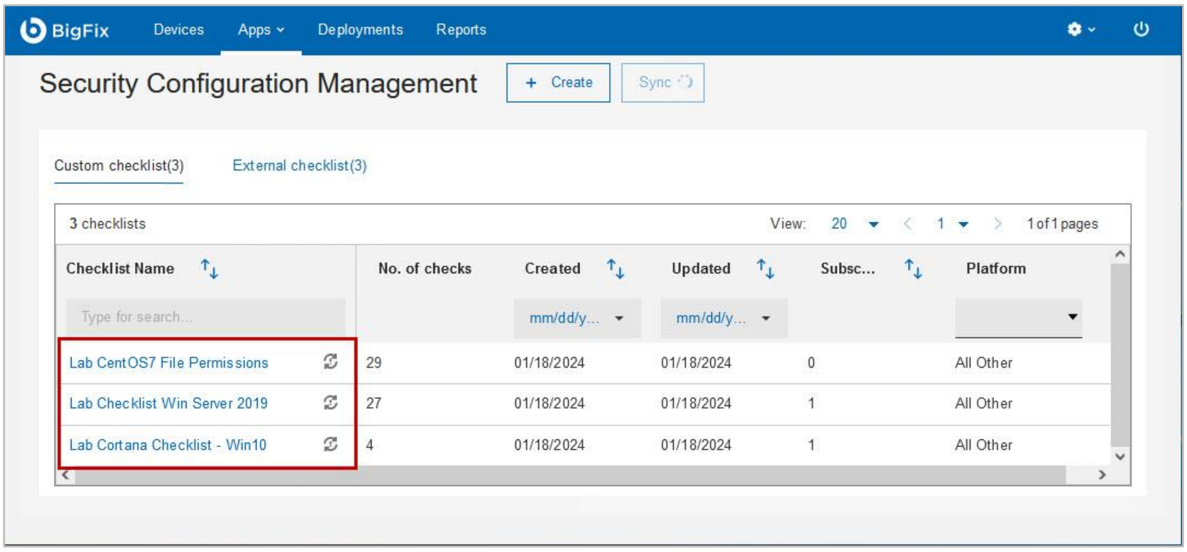
2 groups

1 Item Selected □ View Selected only

□ Group Name	Member count
☑ CentOS Computers	1

A message is displayed indicating that the subscriptions have been updated.

18. Select **SCM** from the **Apps** tab at the top of the WebUI page. The Security Configuration Management page displays the 3 custom checklists.



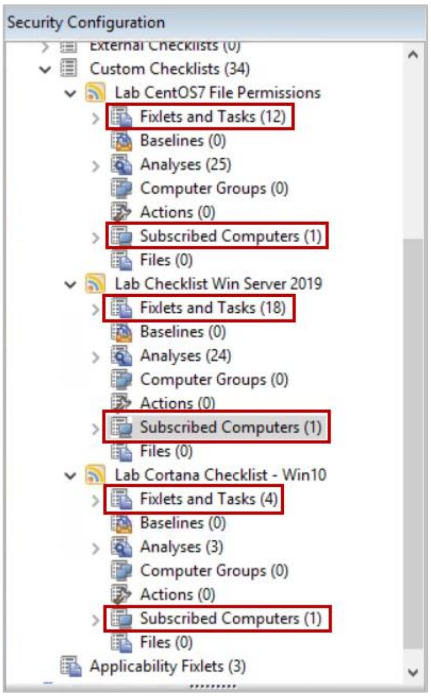
Security Configuration Management

Custom checklist(3) External checklist(3)

3 checklists View: 20 1 1 of 1 pages

Checklist Name	No. of checks	Created	Updated	Subsc...	Platform
Lab CentOS7 File Permissions	29	01/18/2024	01/18/2024	0	All Other
Lab Checklist Win Server 2019	27	01/18/2024	01/18/2024	1	All Other
Lab Cortana Checklist - Win10	4	01/18/2024	01/18/2024	1	All Other

19. Minimize the **Firefox** browser and return to the **BigFix Console**.
20. Click **Security Configuration** in the lower-left portion of the. The navigation pane updates to show the Security Configuration content.
21. In the navigation pane expand **Configuration Management > Custom Checklists.** The 3 Custom Checklists that you created are shown.
22. Expand the node beside each of the custom checklists, and verify that each of the Custom Checklist sites are reporting **Subscribed Computers** and Relevant **Fixlets and Tasks** before continuing to the next exercise.



Security Configuration

- External Checklists (0)
- Custom Checklists (34)
  - Lab CentOS7 File Permissions
    - Fixlets and Tasks (12)
    - Baselines (0)
    - Analyses (25)
    - Computer Groups (0)
    - Actions (0)
    - Subscribed Computers (1)
    - Files (0)
  - Lab Checklist Win Server 2019
    - Fixlets and Tasks (18)
    - Baselines (0)
    - Analyses (24)
    - Computer Groups (0)
    - Actions (0)
    - Subscribed Computers (1)
    - Files (0)
  - Lab Cortana Checklist - Win10
    - Fixlets and Tasks (4)
    - Baselines (0)
    - Analyses (3)
    - Computer Groups (0)
    - Actions (0)
    - Subscribed Computers (1)
    - Files (0)
- Applicability Fixlets (3)

You have now successfully completed Exercise 6.

Exercise 7 – Import the Checklists into the Analytics Server

Now that there are active checklists, the compliance data is available for reporting. In this exercise, you access the BigFix Compliance Analytics web interface using a browser and perform a data import.

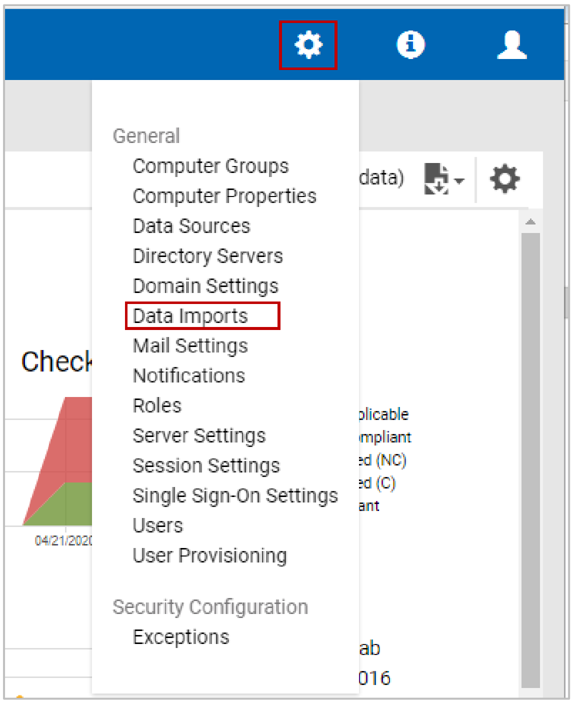
1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double click the **Firefox** icon on the desktop. The browser opens.
3. Enter the following URL in the address section of the browser:

   https://BESFNDWINROOT:9085

   Note: You might receive a security warning indicating that it is unsafe to continue to the page. Click the **Advanced** option, accept the risk and continue to the site.

   The BigFix Compliance login page opens.

4. Enter **adminmo** as the username with a password of **B1gfixrocks!**. Click **Login**. The Overview page opens.
5. Click the **gear** icon in the upper-right portion of the **Overview** page and select **Data Imports**.

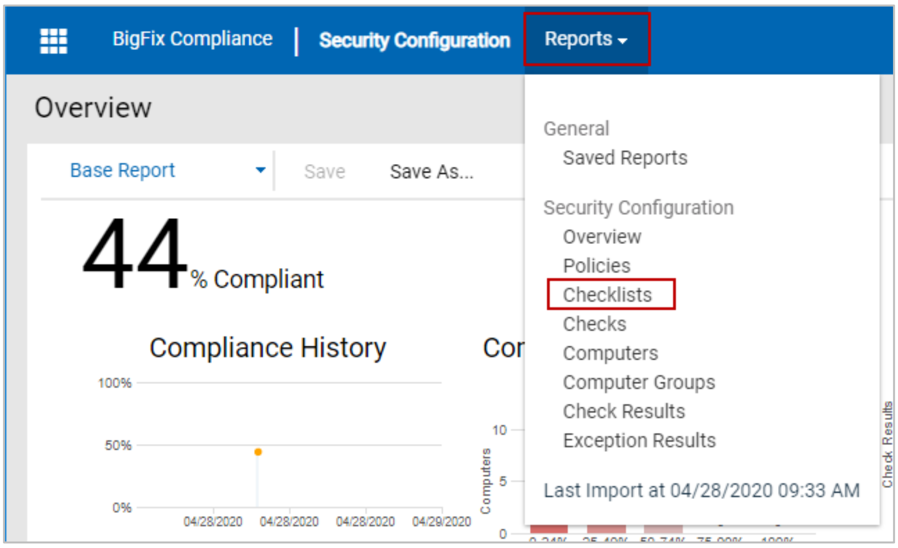


   The Management: Data Imports page opens.

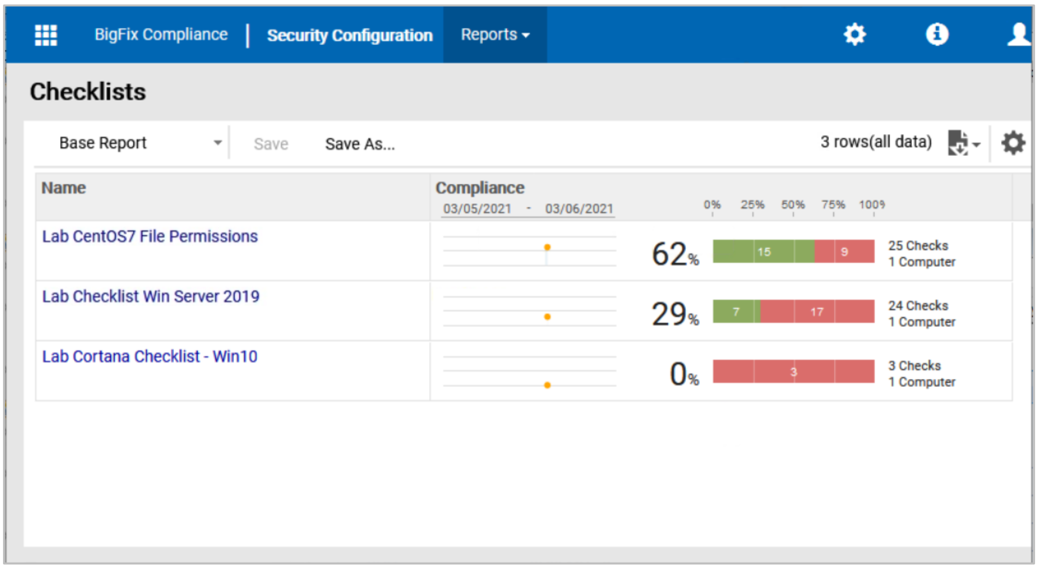
6. In this step, you turn off the default Import Schedule for the purpose of the lab exercises only. Select the **Import Settings** tab and remove the check beside the **Enabled** option, then click **Save**. This prevents a long import from automatically starting during the course and impacting the exercises.
7. Click **Import Now**. A message is shown that indicates that the import is running. The import takes several minutes to run. You can periodically refresh the browser page to view the number of steps that have completed. Wait until the import successfully completes before continuing.

Note: It might take up to 10 minutes for the Import to complete. You can monitor the progress by clicking the **Reports** tab at the top of the Compliance page and viewing the progress message at the bottom of the **Reports** menu.

8. Click the **Reports** menu at the top of the page, then select **Checklists**.



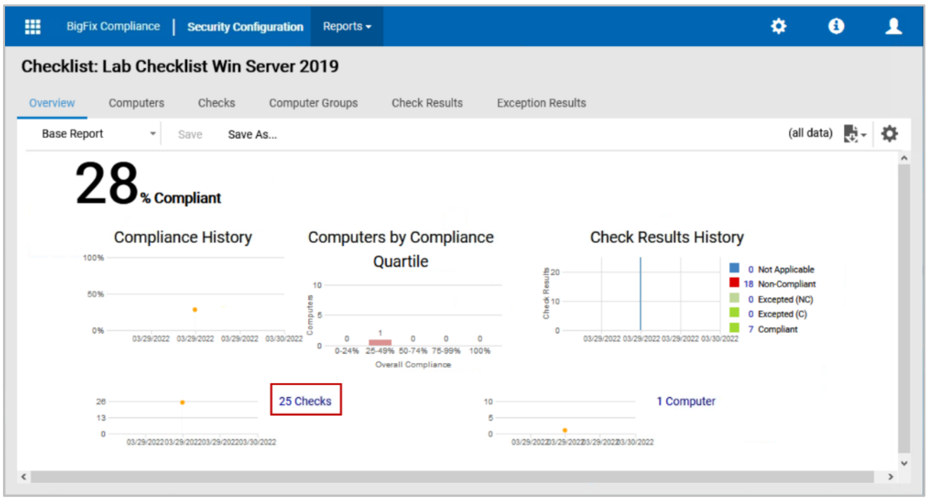
The Checklists page opens and shows the compliance percentage for each of the custom checklists that are created.



Name	Compliance 03/05/2021 - 03/06/2021		
Lab CentOS7 File Permissions	62%	15 / 9	25 Checks 1 Computer
Lab Checklist Win Server 2019	29%	7 / 17	24 Checks 1 Computer
Lab Cortana Checklist - Win10	0%	3	3 Checks 1 Computer

9. Locate the **Lab Checklist Win Server 2019** checklist and note the current compliance level.
10. Click the link for the **Lab Checklist Win Server 2019** in the **Name** column. The Overview report for the selected checklist opens.

11. Select the **Checks** link in the second row of graphs on the **Overview** report.



The **Checks** report opens for the selected checklist and shows the percentage compliance for each of the checks that are associated with that checklist.

Note: You can also navigate to the Checks page by clicking the Checks tab at the top of the Overview report.

12. Review the Compliance level for each of the checks in the **Lab Checklist Win Server 2019** Checks report.

Note: The Compliance graph in the Checks report indicates how compliance with the various checks changes over time and is updated each time a **Data Import** is performed.

You have now completed Exercise 7.

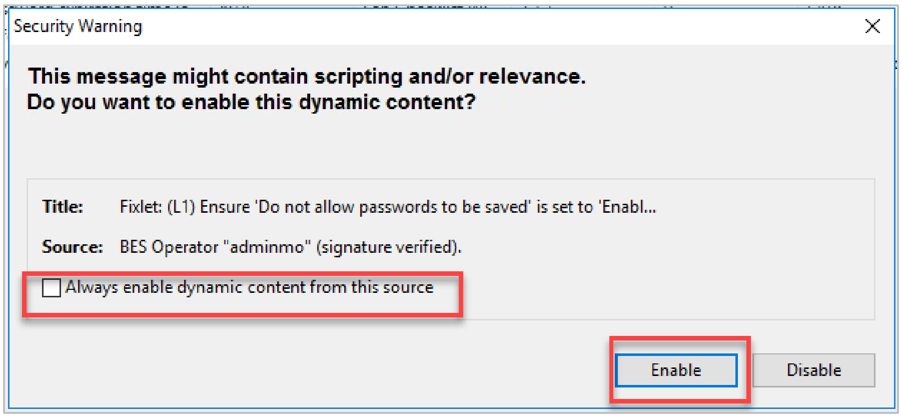
Exercise 8 - Customizing a Checklist Check - Console

The default values for the various Checks in the security checklists are based on the specification that is published by the respective standards organization that the checklist is based on. The required configuration standards in your enterprise might be different than the default values that are delivered with the out of the box checks.

In this Exercise, you modify the default value for an existing check in the **Lab Checklist Win Server 2019** custom checklist.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. If the Console is not already open, double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens.
4. Click **Security Configuration** in the lower-left portion of the Console if it is not already selected. The navigation pane updates to show the BigFix content that is related to Security Configuration.
5. Expand the **Configuration Management > Custom Checklists > Lab Checklist Win Server 2019** nodes, then select **Fixlets and Tasks**. The Fixlets that correspond to each of the checks in the custom checklist are shown in the list pane in the upper-right portion of the Console.

6. Enter **enforce** in the live search box in the upper-right portion of the list pane. The list of Fixlets is filtered to show only those that contain the string **enforce** in the title or description.
7. Select the Fixlet named **(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'**. The details for the selected Fixlet are shown in the work area below.
   a. If the Security Warning message is displayed, always click on the check box for: "Always enable dynamic content from this source" then click on the Enable button.



Security Warning

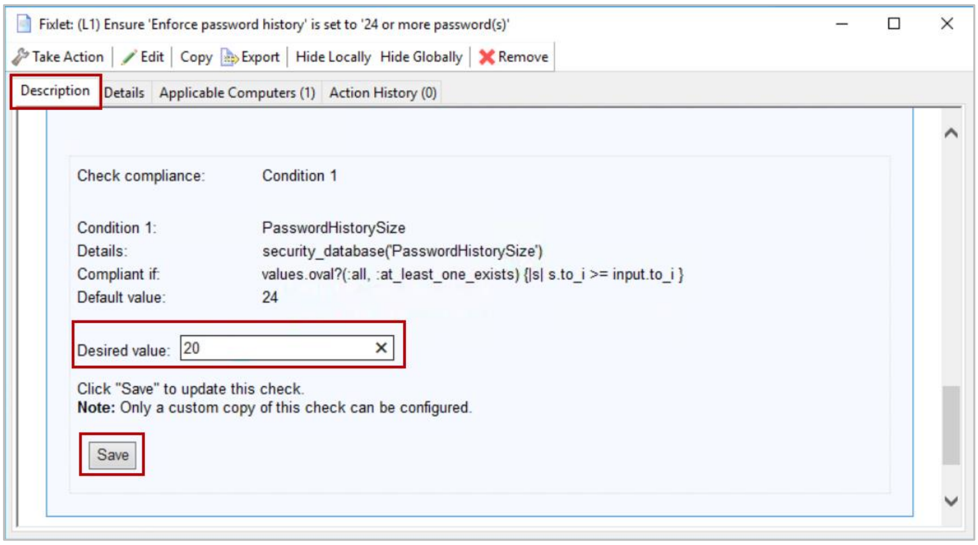
This message might contain scripting and/or relevance.
Do you want to enable this dynamic content?

Title: Fixlet: (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabl...

Source: BES Operator "adminmo" (signature verified).

□ Always enable dynamic content from this source

8. Click the **Description** tab if it is not already selected and review the information about the selected check.
9. Scroll down to the bottom of the **Description** tab and located the **Desired value** field. Enter **20** in the **Desired value** field, then click **Save**.



Fixlet: (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'

Check compliance: Condition 1

Condition 1: PasswordHistorySize
Details: security_database('PasswordHistorySize')
Compliant if: values.oval?(:all, :at_least_one_exists) {|s| s.to_i >= input.to_i }
Default value: 24

Desired value: 20

Click "Save" to update this check.
Note: Only a custom copy of this check can be configured.

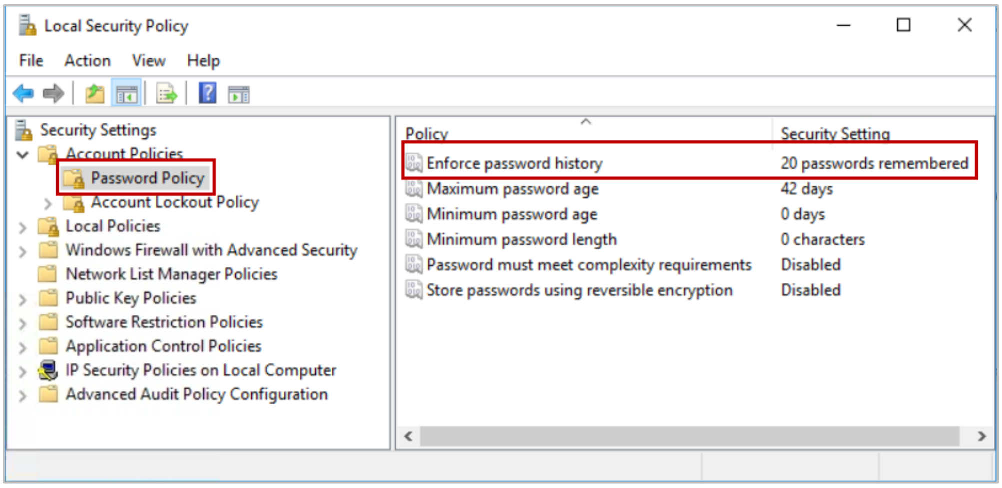
The Desired value parameter is updated to 20.

Note: You can also verify this by selecting the **Details** tab and reviewing the value for the **PasswodHistorySize** parameter in the Action script for **Action1**.

10. Click **Take Action**. The Take Action window opens.
11. Select **BESFNDWINROOT** from the list of available targets. Click **OK**.

Monitor the status of the action and wait until the status changes to **Fixed** before continuing. You can periodically click **Refresh Console** at the top of the Console to update the display.

12. Click the **Start** button on the **BESFNDWINROOT** virtual machine and enter **secpol.msc** in the search field. Press **Enter**. The **Local Security Policy** editor opens.
13. Expand **Account Policies** and select **Password Policy**. The various password policies and security settings are shown.
14. Locate the **Enforce password history** policy and verify that the **Security Setting** is now set to **20 passwords remembered**.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	20 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

15. Close the **Local Security Policy** window.

You have now completed Exercise 8.

Exercise 9 - Customizing a Checklist Check - WebUI

In this Exercise, you use the WebUI to modify the default value for an existing check in the **Lab Checklist Win Server 2019** custom checklist.

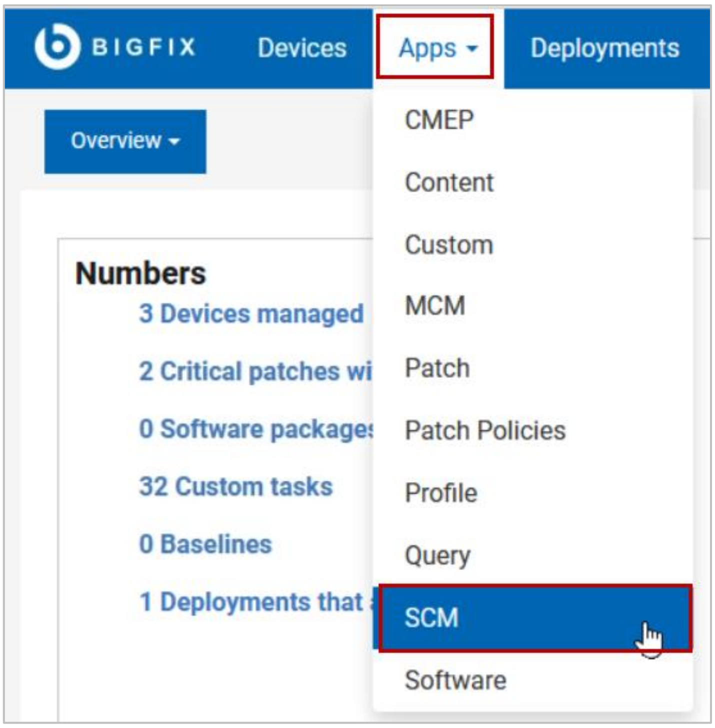
1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Minimize the Console and double-click the **Firefox** icon on the **Windows Desktop** to open the **Firefox** browser if it is not already open.
3. Enter the **URL** for the **WebUI** in the address bar of the **Firefox** browser as follows and press Enter.

   https://BESFNDWINROOT

   The WebUI login page opens.

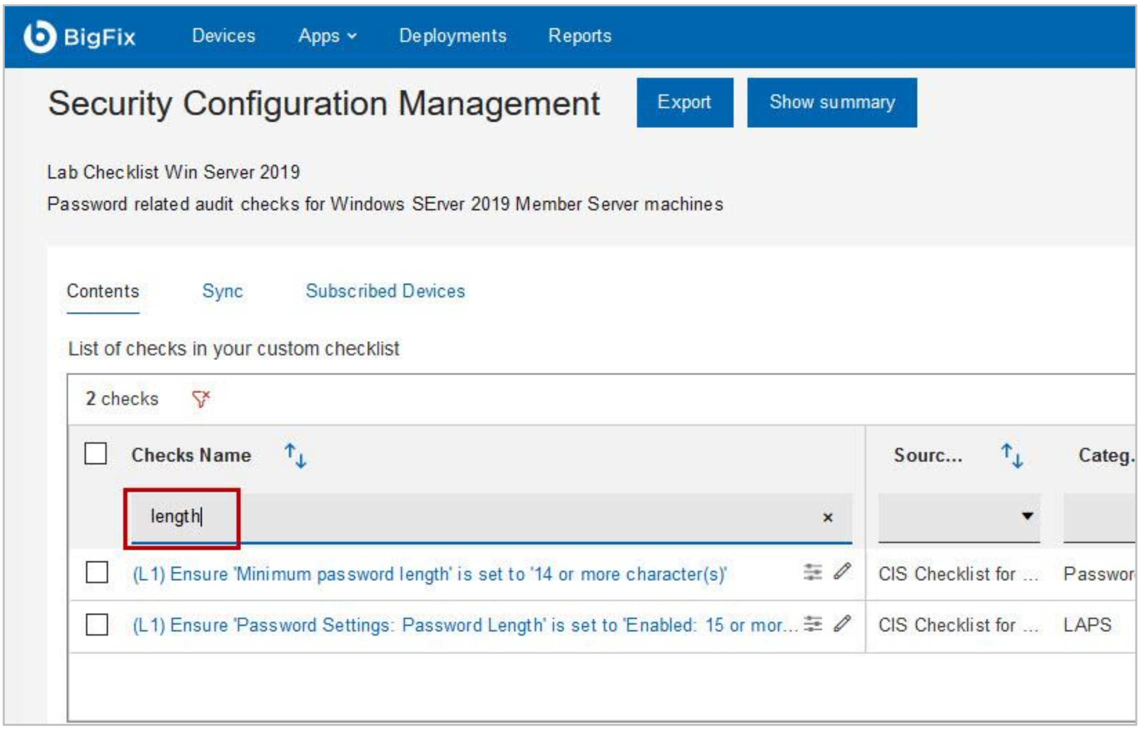
4. Log in to the **WebUI** as **adminmo** with a password of **B1gfixrocks**. The WebUI Overview page opens.

5. Select **SCM** from the **Apps** tab at the top of the WebUI **Overview** page.



The Security Configuration Management page opens.

6. Click the **Lab Checklist Win Server 2019** custom checklist. The custom checklist opens and displays a list of all the custom checks in the checklist.
7. Enter the string **length** in the **Checks Name** filter. The list of custom checks is filtered to display only those that contain the string "length" in their name.



Security Configuration Management

Lab Checklist Win Server 2019

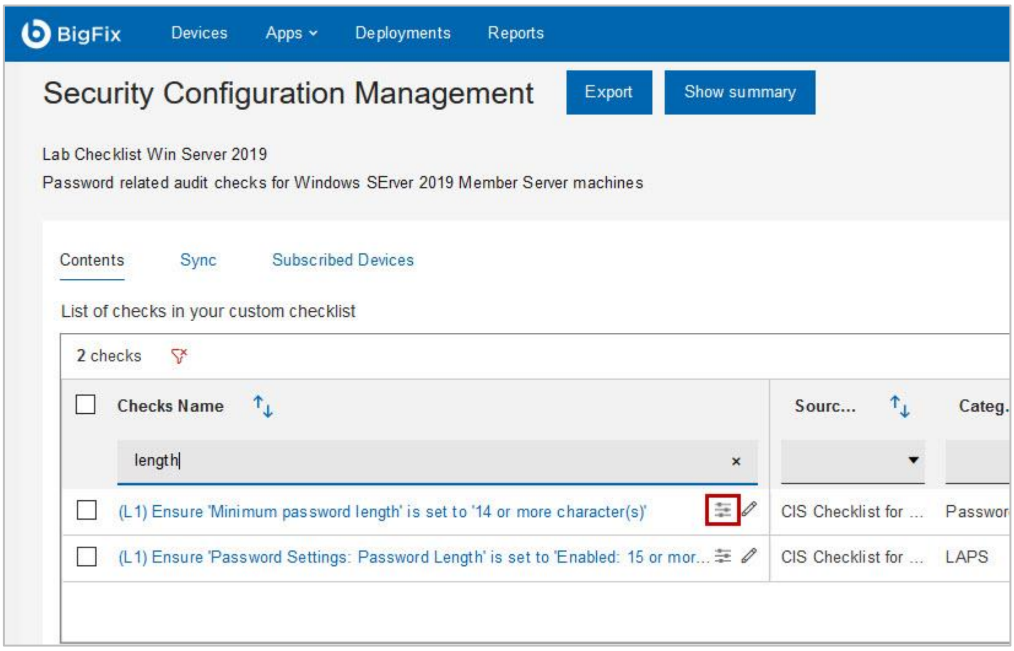
Password related audit checks for Windows SErver 2019 Member Server machines

List of checks in your custom checklist

2 checks

□	Checks Name	Sourc...	Categ.
	length		
□	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	CIS Checklist for ...	Passwor
□	(L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or mor...	CIS Checklist for ...	LAPS

8. Locate the check **named (L1) Ensure Minimum password length is set to 14 or more character(s)** and click the **Edit Parameter** icon located to the right of the check name.



Security Configuration Management

Lab Checklist Win Server 2019

Password related audit checks for Windows SErver 2019 Member Server machines

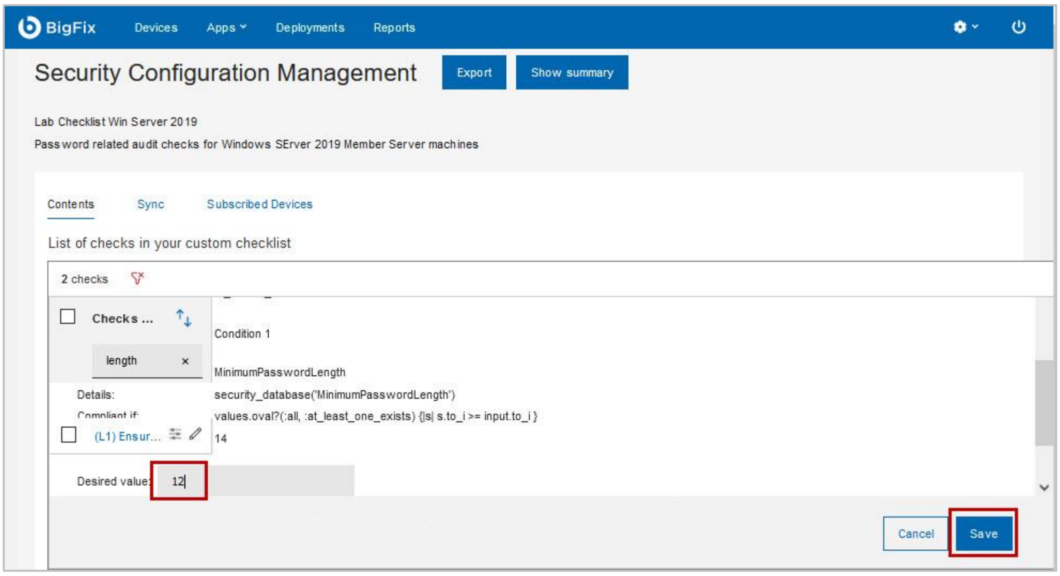
List of checks in your custom checklist

2 checks

□	Checks Name	Sourc...	Categ.
	length		
□	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	CIS Checklist for ...	Passwor
□	(L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or mor...	CIS Checklist for ...	LAPS

The Edit Parameters page opens for the selected check.

9. **Scroll down** to the bottom of the **Edit Parameters** page and locate the **Desired value** field. Change the **Desired value** from 14 to **12**. Click **Save**.



Security Configuration Management

Lab Checklist Win Server 2019

Password related audit checks for Windows SErver 2019 Member Server machines

List of checks in your custom checklist

2 checks

□ Checks ...

length

□ (L1) Ensur...

Condition 1

MinimumPasswordLength

Details: security_database('MinimumPasswordLength')

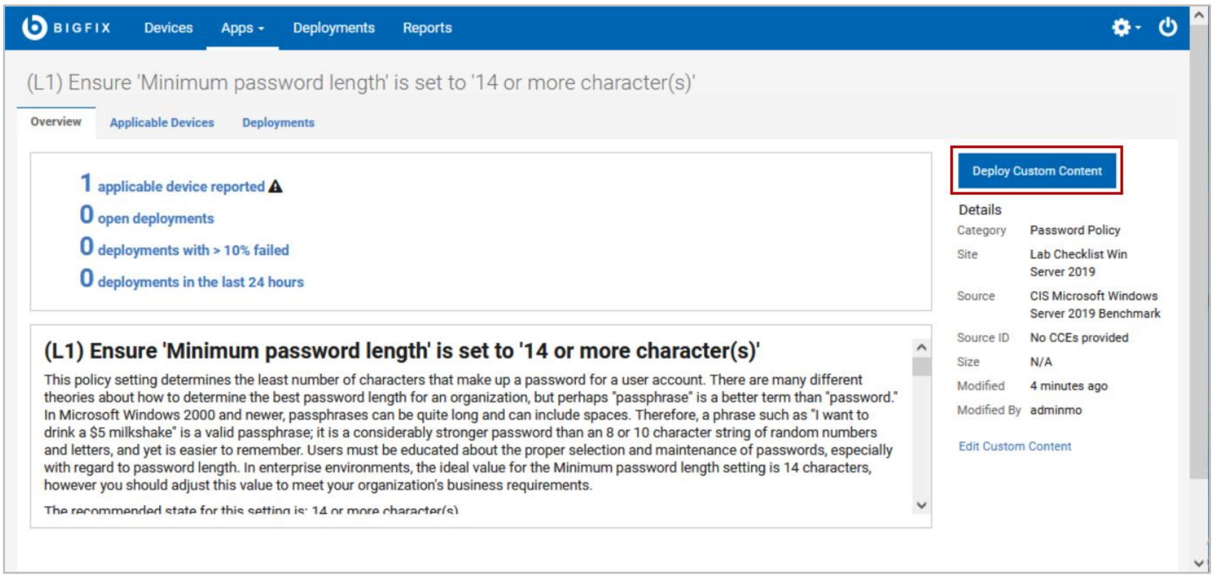
Compliant if: values.oval?(:all, :at_least_one_exists) {|s| s.to_i >= input.to_i }

14

Desired value: 12

10. Click the link represented by **the (L1) Ensure Minimum password length is set to 14 or more character(s)** check name. A page showing the details for the selected check opens.

11. Click **Deploy Custom Content** in the upper-right portion of the check details page.



(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

1 applicable device reported ⚠

0 open deployments

0 deployments with > 10% failed

0 deployments in the last 24 hours

(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password." In Microsoft Windows 2000 and newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements.

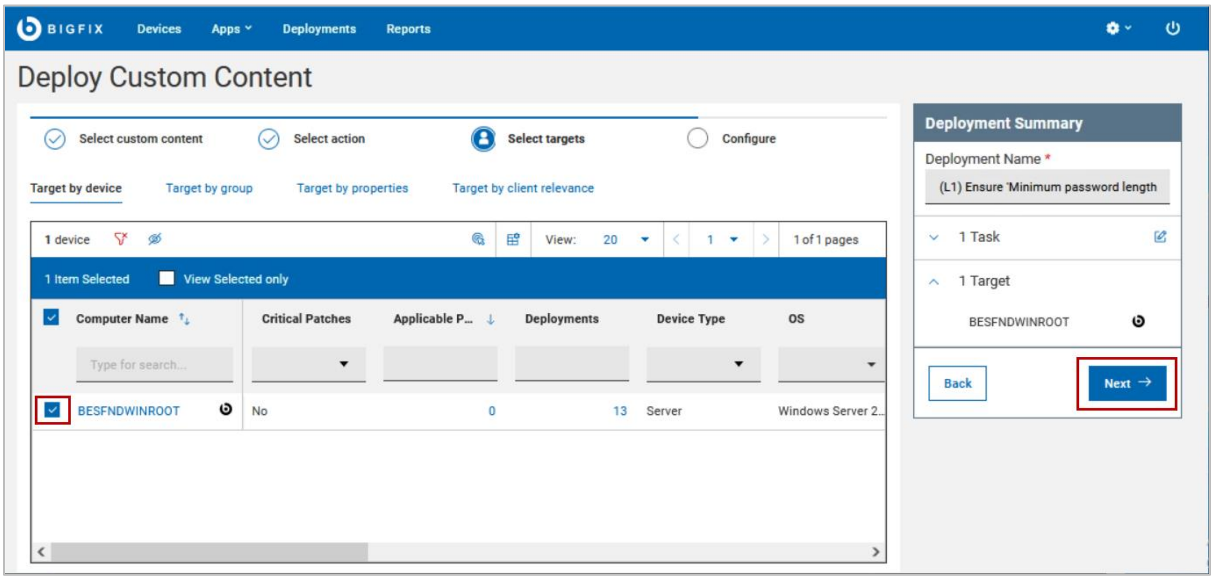
The recommended state for this setting is: 14 or more character(s)

Details

Category	Password Policy
Site	Lab Checklist Win Server 2019
Source	CIS Microsoft Windows Server 2019 Benchmark
Source ID	No CCEs provided
Size	N/A
Modified	4 minutes ago
Modified By	adminmo

The Deploy Custom Content page opens.

12. Click **Next**. The Select targets step is displayed.
13. Place a check beside **BESFNDWINROOT**. Click **Next**.



Deploy Custom Content

1 device | View: 20 | 1 | 1 of 1 pages

1 Item Selected

☑ Computer Name	Critical Patches	Applicable P...	Deployments	Device Type	OS
☑ BESFNDWINROOT	No	0	13	Server	Windows Server 2...

Deployment Summary

Deployment Name *

(L1) Ensure 'Minimum password length

1 Task

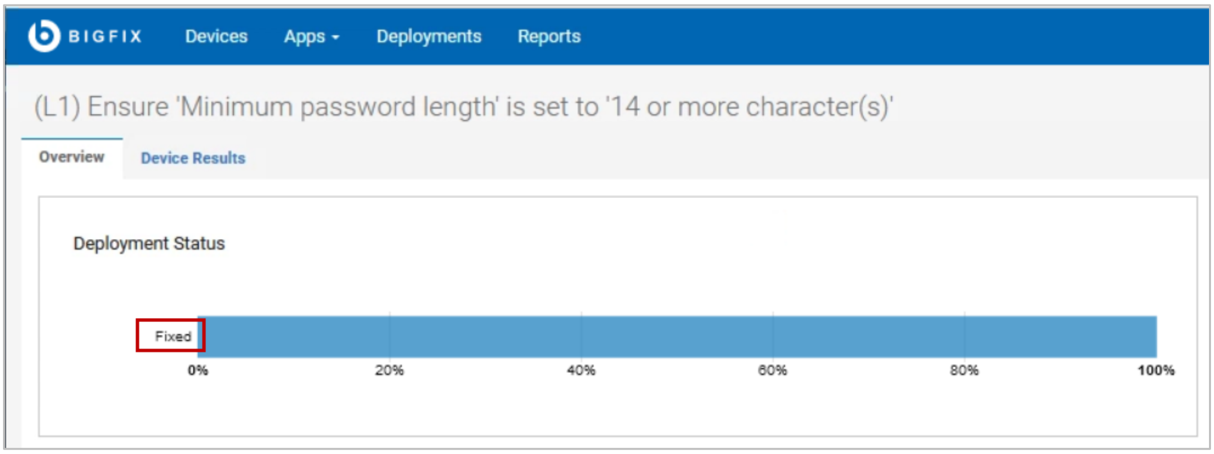
1 Target

BESFNDWINROOT

The Configure step is displayed.

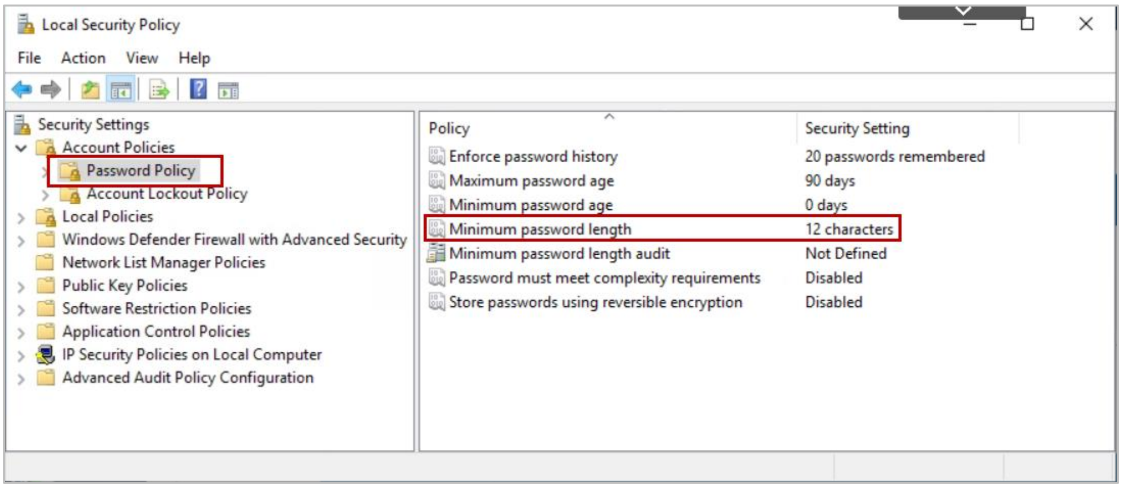
14. Accept the **default** values for the **Configure** step, then scroll down and click **Deploy** on the right side of the **Deploy Custom Content** page. The deployment page opens.

15. Monitor the status of the deployment and wait for it to complete before continuing. You can periodically refresh the browser page to view the updated status.



(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'

16. Click the **Start** button on the **BESFNDWINROOT** virtual machine and enter **secpol.msc** in the search field. Press **Enter**. The **Local Security Policy** editor opens.
17. Expand **Account Policies** and select **Password Policy**. The various password policies and security settings are shown.
18. Locate the **Minimum password length** policy and verify that the **Security Setting** is now set to **12 characters**.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	20 passwords remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

19. Close the **Local Security Policy** window.

You have now completed Exercise 9.

Exercise 10 – Enforcing Continuous Compliance

There might be certain configuration settings that must be enforced automatically either across the enterprise or groups of systems. It is possible for BigFix to automatically remediate out of compliance systems without operator intervention.

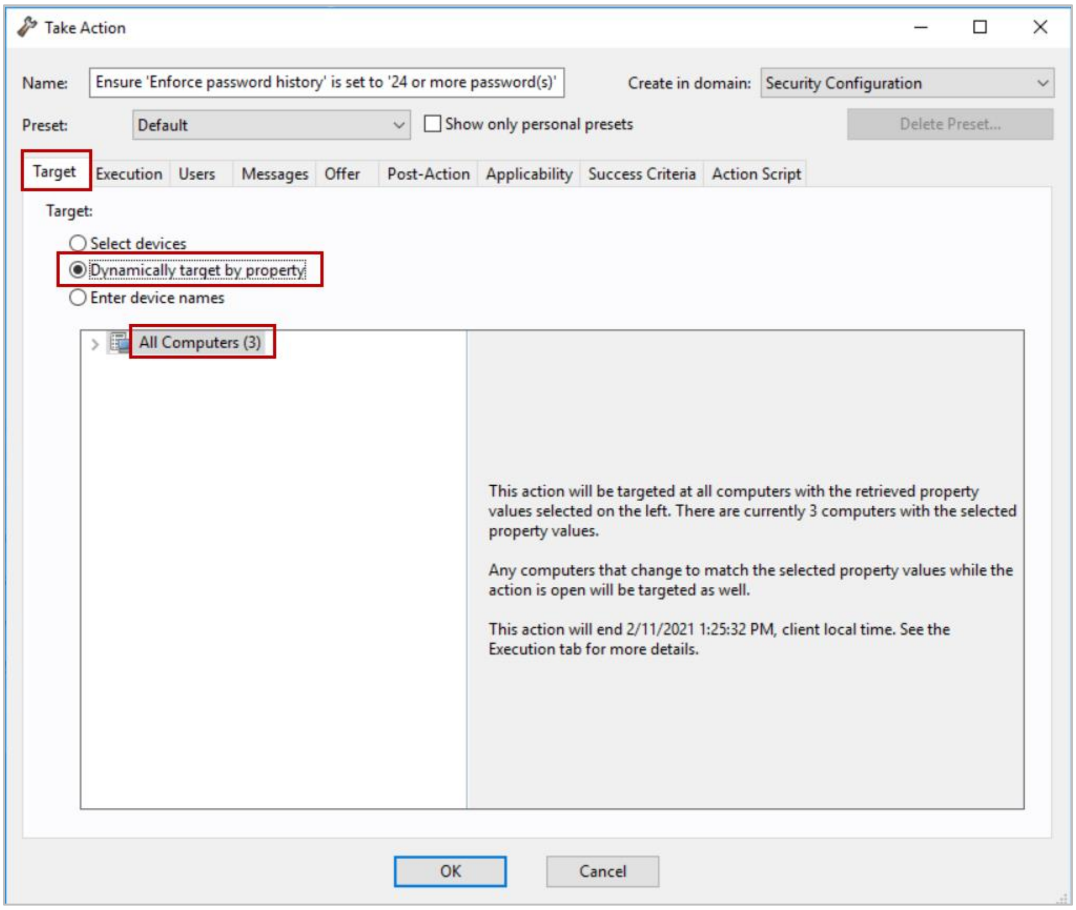
In this exercise, you deploy a policy action to automatically enforce the compliance check that was modified in the previous exercise.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.

2. If the Console is not already open, double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens
4. Click **Security Configuration** in the lower-left portion of the Console if it is not already selected. The navigation pane updates to show the BigFix content that is related to Security Configuration.
5. Expand the **Configuration Management > Custom Checklists > Lab Checklist Win Server 2019** nodes, then select **Fixlets and Tasks**. The Fixlets that correspond to each of the checks in the custom checklist are shown in the list pane in the upper-right portion of the Console.
6. Enter **enforce** in the live search box in the upper-right portion of the list pane. The list of Fixlets is filtered to show only those that contain the string **enforce** in the title or description.

   Hint: This Fixlet might no longer be Relevant. If it is not shown in the List Area click the Show Non-Relevant Content button at the top of the Console.

7. Select the Fixlet named **(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'**. The details for the selected Fixlet are shown in the work area below.
8. Click the **Description** tab if it is not already selected and review the information about the selected check.
9. Click **Take Action**. The Take Action window opens.
10. Select the **Target** tab.
11. Select the **Dynamically Target by Property** option.
12. Select **All Computers (3)**



Name: Ensure 'Enforce password history' is set to '24 or more password(s)'

Create in domain: Security Configuration

Preset: Default

☐ Show only personal presets

Target:

○ Select devices

● Dynamically target by property

○ Enter device names

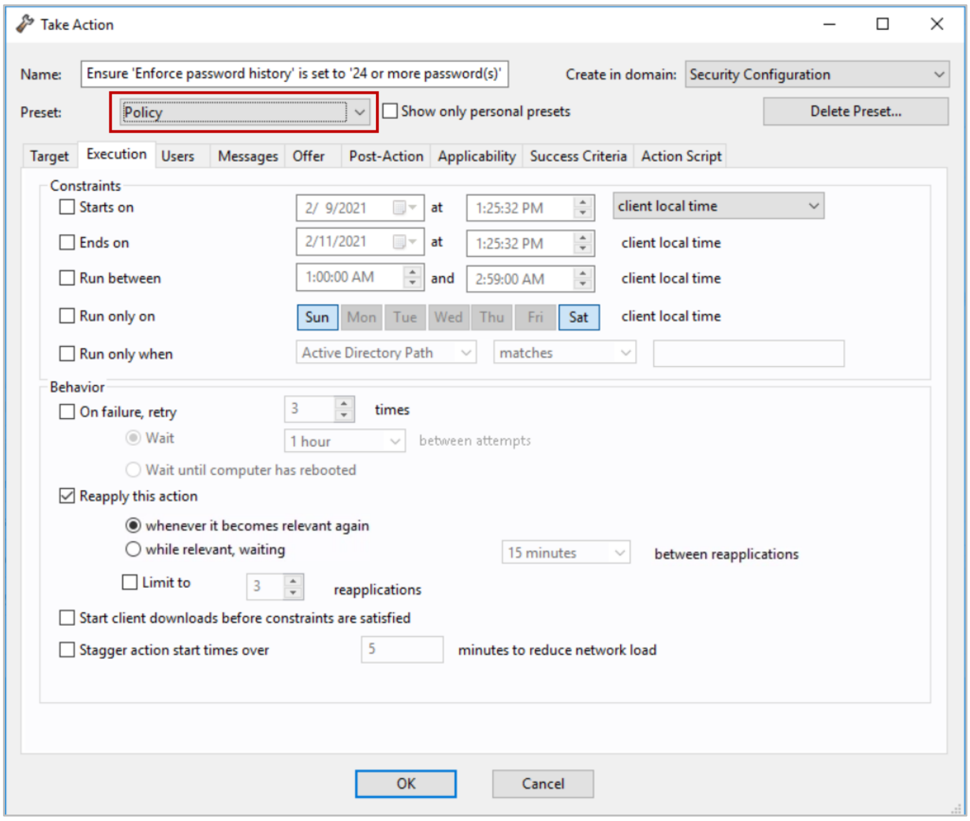
All Computers (3)

This action will be targeted at all computers with the retrieved property values selected on the left. There are currently 3 computers with the selected property values.

Any computers that change to match the selected property values while the action is open will be targeted as well.

This action will end 2/11/2021 1:25:32 PM, client local time. See the Execution tab for more details.

13. Click the **Execution** tab.
14. Select **Policy** from the **Preset** drop-down box. Observe the various changes to the settings on the Execution tab as a result of selecting the Policy preset.



Take Action

Name: Ensure 'Enforce password history' is set to '24 or more password(s)'

Create in domain: Security Configuration

Preset: Policy

□ Show only personal presets

Constraints

□ Starts on 2/ 9/2021 at 1:25:32 PM client local time

□ Ends on 2/11/2021 at 1:25:32 PM client local time

□ Run between 1:00:00 AM and 2:59:00 AM client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time

□ Run only when Active Directory Path matches

Behavior

□ On failure, retry 3 times

○ Wait 1 hour between attempts

○ Wait until computer has rebooted

☑ Reapply this action

● whenever it becomes relevant again

○ while relevant, waiting 15 minutes between reapplications

□ Limit to 3 reapplications

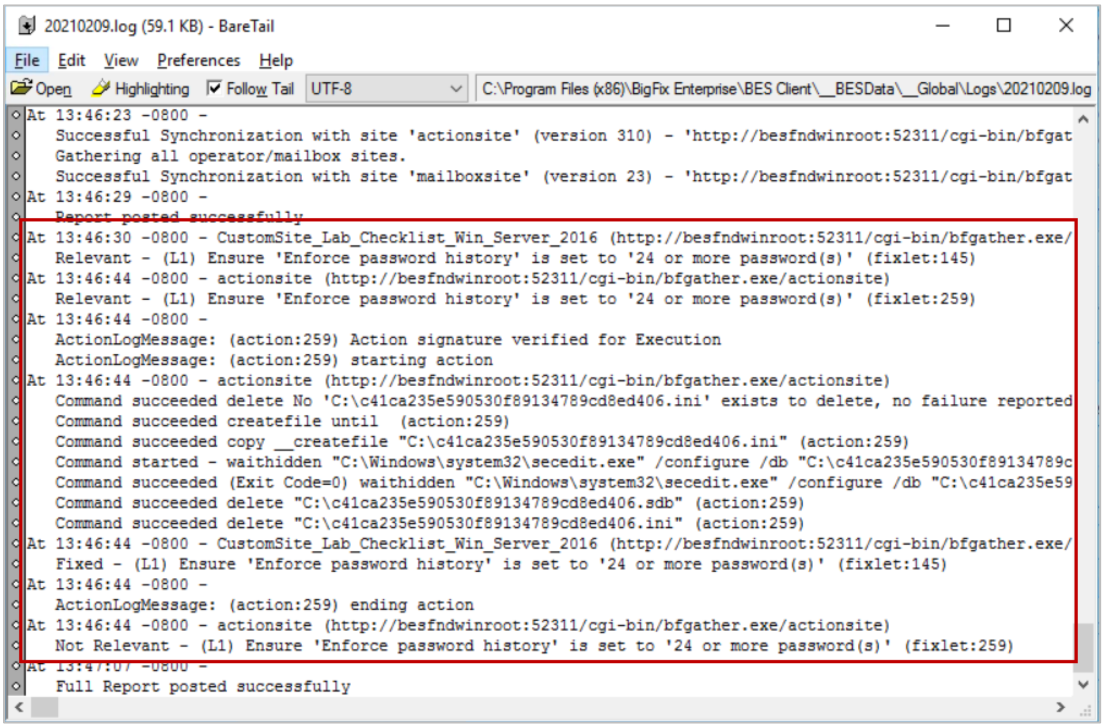
□ Start client downloads before constraints are satisfied

□ Stagger action start times over 5 minutes to reduce network load

15. Click **OK**. The action is deployed to the targeted endpoints as they become Relevant and remains open until it is stopped by an operator.
16. Click the **Start** button on the **BESFNDWINROOT** virtual machine and enter **secpol.msc** in the search field. Press **Enter**. The **Local Security Policy** editor opens.
17. Expand **Account Policies** and select **Password Policy**. The various password policies and security settings are shown.
18. Locate the **Enforce password history** policy and modify the value to **15**. Click **Apply**.
19. Click **OK**.
20. Close the **Local Security Policy** editor.
21. Double-click the **baretail** icon on the Windows desktop of the **BESFNDWINROOT** virtual machine. The baretail application opens.
22. Open the current BESClient log in the **baretail** application.

Note: The BESClient log files are located in the **C:\Program Files (x86)\BigFix Enterprise\BES Client__BESData__Global\Logs** directory.

23. Monitor the client log in **baretail**. The **Enforce password history** compliance check becomes Relevant and the action script executes. It might take several minutes for the check to become **Relevant** and appear in the log file. Observe that the **Enforce password history** Fixlet is shown a **Not Relevant** after the action script completes.


20210209.log (59.1 KB) - BareTail
File
Edit
View
Preferences
Help
Open
Highlighting
☑ Follow Tail
UTF-8
C:\Program Files (x86)\BigFix Enterprise\BES Client__BESData__Global\Logs\20210209.log

```
At 13:46:23 -0800 -
   Successful Synchronization with site 'actionsite' (version 310) - 'http://besfndwinroot:52311/cgi-bin/bfgat
   Gathering all operator/mailbox sites.
   Successful Synchronization with site 'mailboxsite' (version 23) - 'http://besfndwinroot:52311/cgi-bin/bfgat
At 13:46:29 -0800 -
   Report posted successfully
At 13:46:30 -0800 - CustomSite_Lab_Checklist_Win_Server_2016 (http://besfndwinroot:52311/cgi-bin/bfgather.exe/
   Relevant - (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (fixlet:145)
At 13:46:44 -0800 - actionsite (http://besfndwinroot:52311/cgi-bin/bfgather.exe/actionsite)
   Relevant - (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (fixlet:259)
At 13:46:44 -0800 -
   ActionLogMessage: (action:259) Action signature verified for Execution
   ActionLogMessage: (action:259) starting action
At 13:46:44 -0800 - actionsite (http://besfndwinroot:52311/cgi-bin/bfgather.exe/actionsite)
   Command succeeded delete No 'C:\c41ca235e590530f89134789cd8ed406.ini' exists to delete, no failure reported
   Command succeeded createfile until  (action:259)
   Command succeeded copy __createfile "C:\c41ca235e590530f89134789cd8ed406.ini" (action:259)
   Command started - waithidden "C:\Windows\system32\secedit.exe" /configure /db "C:\c41ca235e590530f89134789c
   Command succeeded (Exit Code=0) waithidden "C:\Windows\system32\secedit.exe" /configure /db "C:\c41ca235e59
   Command succeeded delete "C:\c41ca235e590530f89134789cd8ed406.sdb" (action:259)
   Command succeeded delete "C:\c41ca235e590530f89134789cd8ed406.ini" (action:259)
At 13:46:44 -0800 - CustomSite_Lab_Checklist_Win_Server_2016 (http://besfndwinroot:52311/cgi-bin/bfgather.exe/
   Fixed - (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (fixlet:145)
At 13:46:44 -0800 -
   ActionLogMessage: (action:259) ending action
At 13:46:44 -0800 - actionsite (http://besfndwinroot:52311/cgi-bin/bfgather.exe/actionsite)
   Not Relevant - (L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (fixlet:259)
At 13:47:07 -0800 -
   Full Report posted successfully
```

24. Open the **Local Policy Editor** and verify that the value of the **Enforce password history** Security Setting is now reset to **20 remembered passwords**.

You have now completed Exercise 10.

Exercise 11 – Using the CVE Search Dashboard

The CVE Search dashboard allows you to analyze vulnerabilities in your environment based on their CVE ID. The CVE's can be searched by entering a comma separated list of CVE ID's, or you can choose to analyze vulnerabilities using one of the pre-defined vulnerability lists such as the CISA KEV list of Binding Operational Directives (BOD).

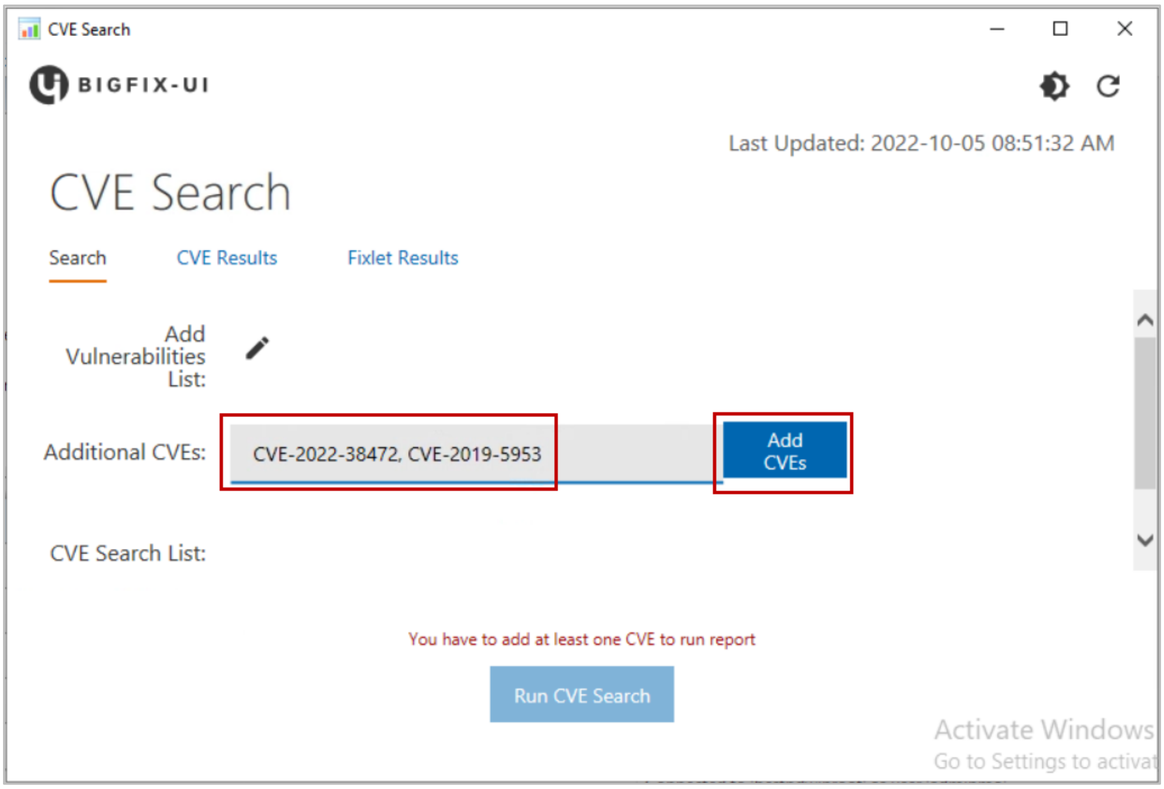
In this exercise, you use the CVE Search dashboard to search for known vulnerabilities in the environment. You then build a baseline to remediate those vulnerabilities.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. If the Console is not already open, double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Click **All Content** in the lower-left portion of the Console if it is not already selected. The navigation pane updates to show all the BigFix content.
4. Expand the **Dashboards > All Dashboards** nodes, then select **CVE Search**. The CVE Search dashboard is opens.

5. Enter the following comma separated list of CVE’s in the **Additional CVEs** field:

   CVE-2022-38472, CVE-2019-5953

6. Click **Add CVEs**.

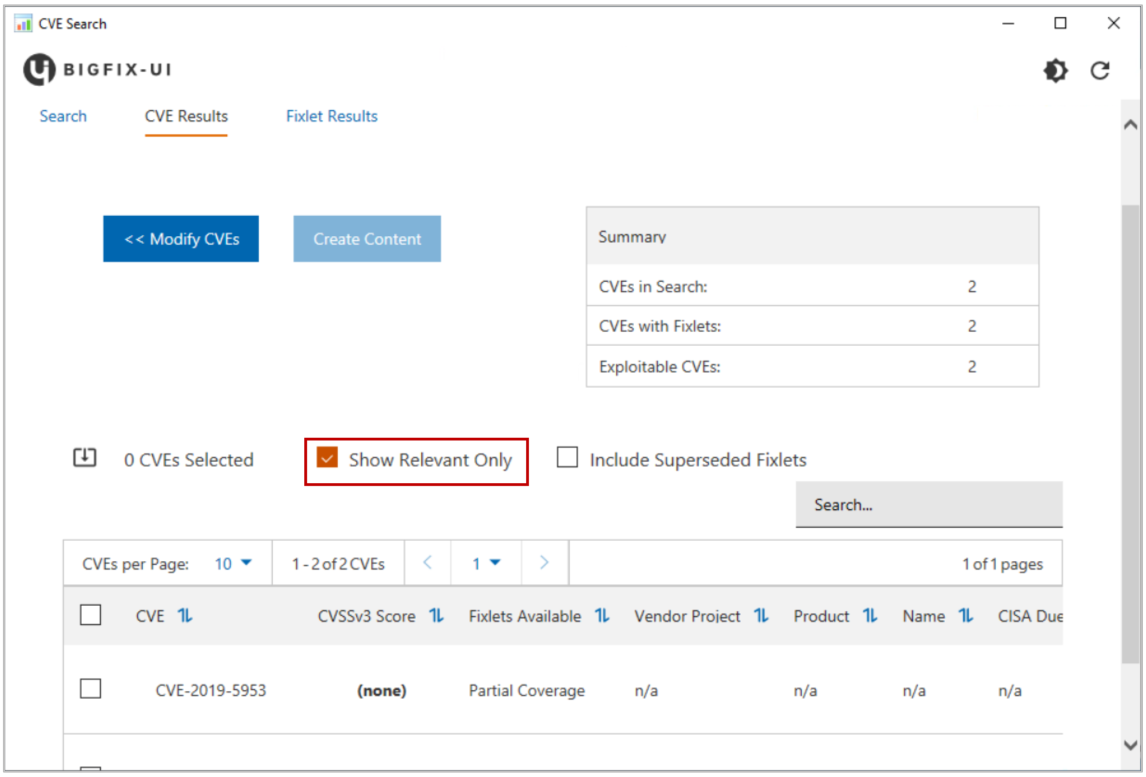


CVE Search
BIGFIX-UI
Last Updated: 2022-10-05 08:51:32 AM
CVE Search
Search
CVE Results
Fixlet Results
Add Vulnerabilities List:
Additional CVEs:
CVE-2022-38472, CVE-2019-5953
Add CVEs
CVE Search List:
You have to add at least one CVE to run report
Run CVE Search
Activate Windows
Go to Settings to activat

The CVEs are added to the CVE Search List and the Run CVE Search button becomes live.

7. Click **Run CVE Search**. The results of the search are displayed on the CVE Results tab of the dashboard.

8. Click the **Show Relevant Only** option.



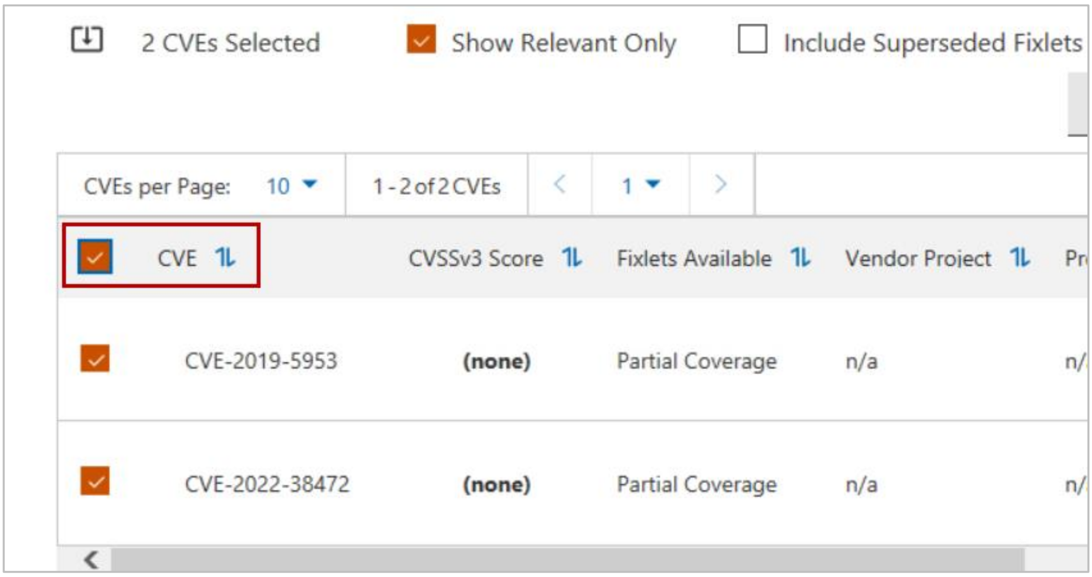
Summary	
CVEs in Search:	2
CVEs with Fixlets:	2
Exploitable CVEs:	2

0 CVEs Selected ☑ Show Relevant Only □ Include Superseded Fixlets

□	CVE	CVSSv3 Score	Fixlets Available	Vendor Project	Product	Name	CISA Due
□	CVE-2019-5953	**(none)**	Partial Coverage	n/a	n/a	n/a	n/a

The dashboard is updated to show only the content that is Relevant to at least 1 managed endpoint in the environment.

9. Place a **check** in the box to the left of the **CVE** column header. All the Relevant content is selected.

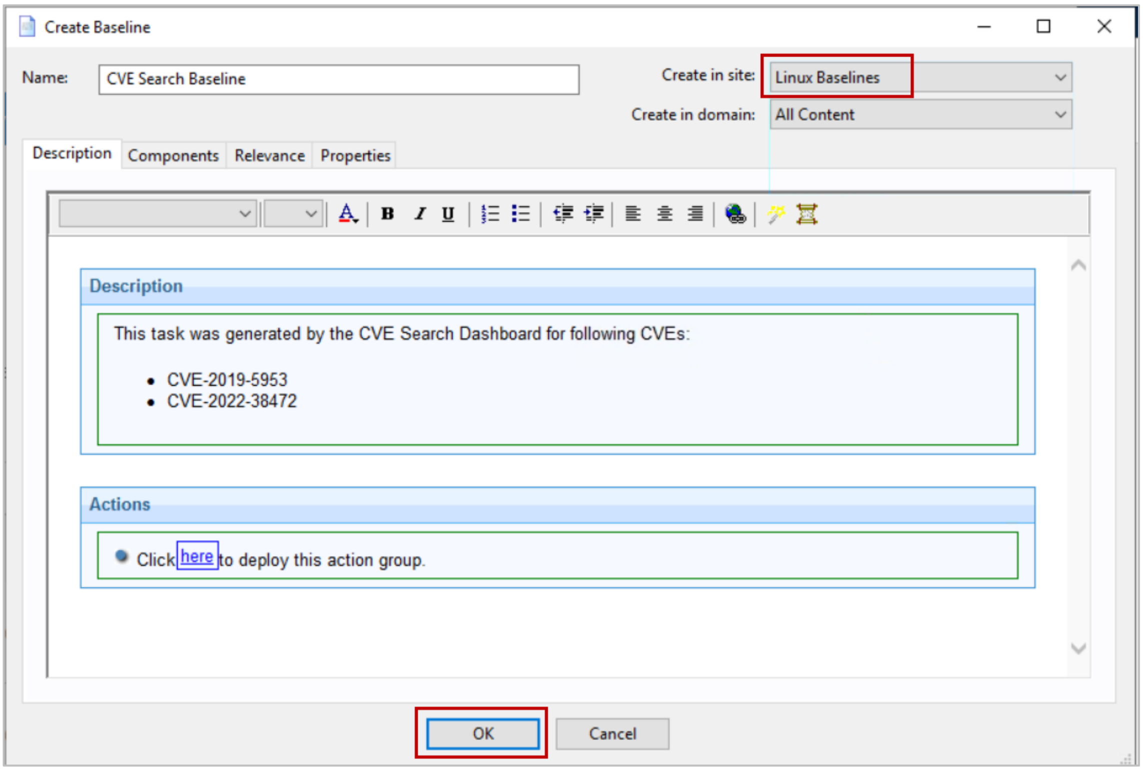


2 CVEs Selected ☑ Show Relevant Only □ Include Superseded Fixlets

☑	CVE	CVSSv3 Score	Fixlets Available	Vendor Project	Pr
☑	CVE-2019-5953	**(none)**	Partial Coverage	n/a	n/
☑	CVE-2022-38472	**(none)**	Partial Coverage	n/a	n/

10. Click **Create Content** at the top of the **CVE Search** dashboard. The Create Baseline window is displayed.

11. Select **Linux Baselines** from the **Create in site** drop-down box. Click **OK**.



Description

This task was generated by the CVE Search Dashboard for following CVEs:

- CVE-2019-5953
- CVE-2022-38472

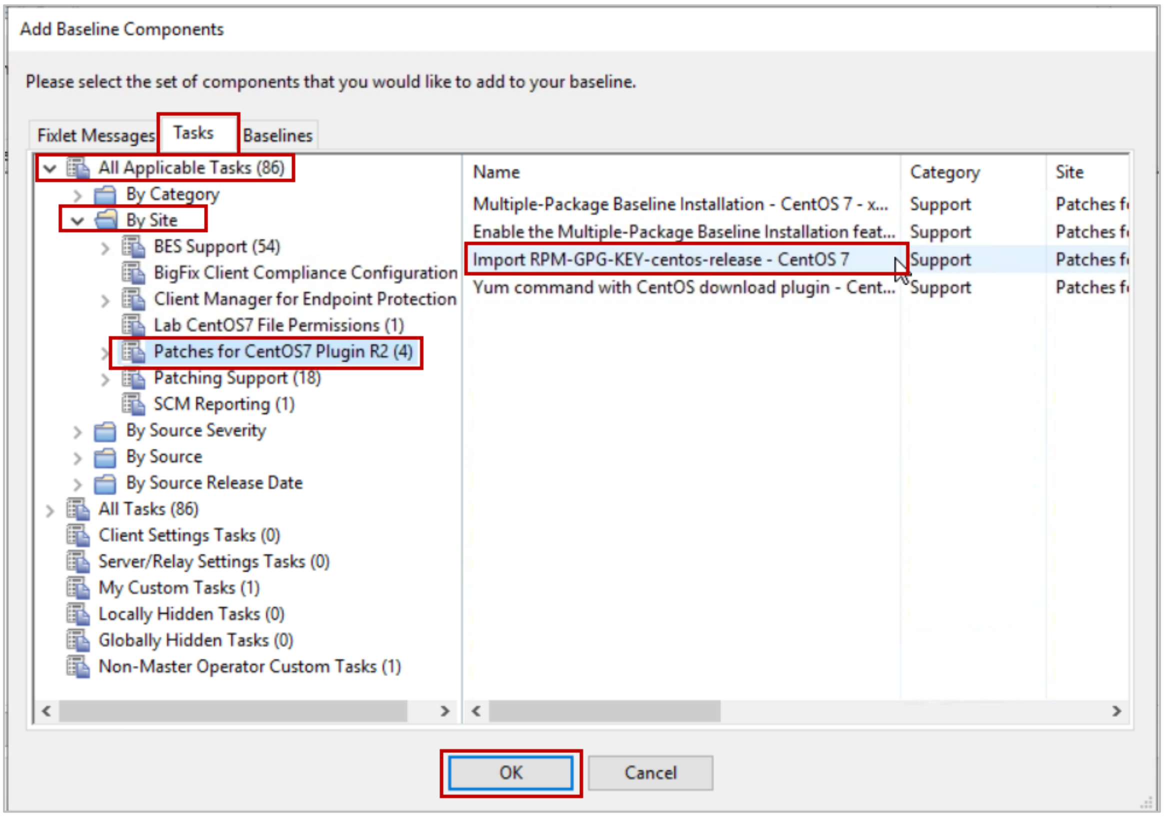
Actions

- Click here to deploy this action group.

The new baseline opens in the Console.

12. Click **Edit**. The Edit Baseline window opens.
13. Click the **Components** tab. The 2 Fixlets that were associated with the selected CVEs are shown in the Baseline.
14. Click the **[add components to group]** link. The Add Baseline Components window opens.
15. Click the **Tasks** tab, then expand the **All Applicable Tasks > By Site** nodes and select **Patches for CentOS7 Plugin R2.** A list of tasks associated with the Patches for CentOS7 site is displayed.

16. Select the **Import RPM-GPG-KEY-centos-release – CentOS 7** task from the list. Click **OK**.



Add Baseline Components

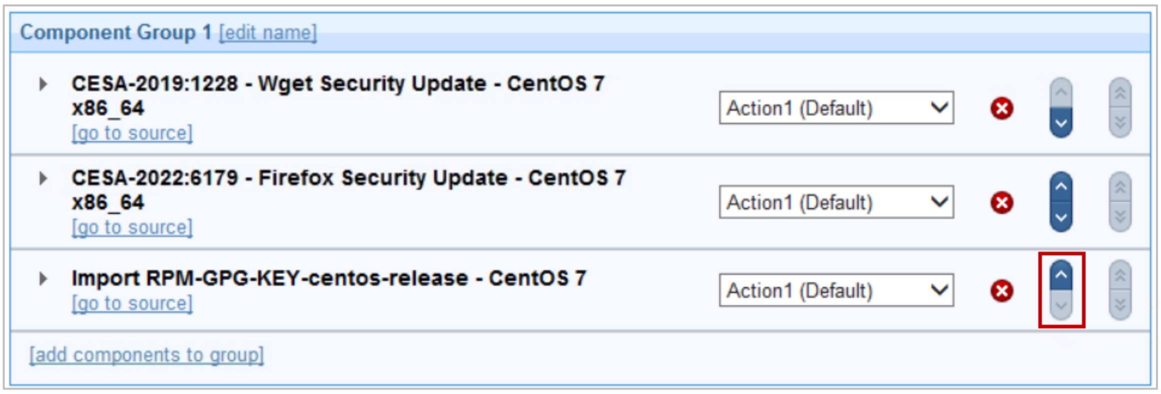
Please select the set of components that you would like to add to your baseline.

Fixlet Messages
Tasks
Baselines
All Applicable Tasks (86)
By Category
By Site
BES Support (54)
BigFix Client Compliance Configuration
Client Manager for Endpoint Protection
Lab CentOS7 File Permissions (1)
Patches for CentOS7 Plugin R2 (4)
Patching Support (18)
SCM Reporting (1)
By Source Severity
By Source
By Source Release Date
All Tasks (86)
Client Settings Tasks (0)
Server/Relay Settings Tasks (0)
My Custom Tasks (1)
Locally Hidden Tasks (0)
Globally Hidden Tasks (0)
Non-Master Operator Custom Tasks (1)
OK
Cancel

Name	Category	Site
Multiple-Package Baseline Installation - CentOS 7 - x...	Support	Patches f
Enable the Multiple-Package Baseline Installation feat...	Support	Patches f
Import RPM-GPG-KEY-centos-release - CentOS 7	Support	Patches f
Yum command with CentOS download plugin - Cent...	Support	Patches f

The Edit Baseline window is displayed and the selected task is added to the list of baseline components.

17. Move the **Import RPM-GPG-KEY-centos-release – CentOS 7** task to the top of the list of Baseline components by clicking the **up-arrow icon** to the right of the component name.



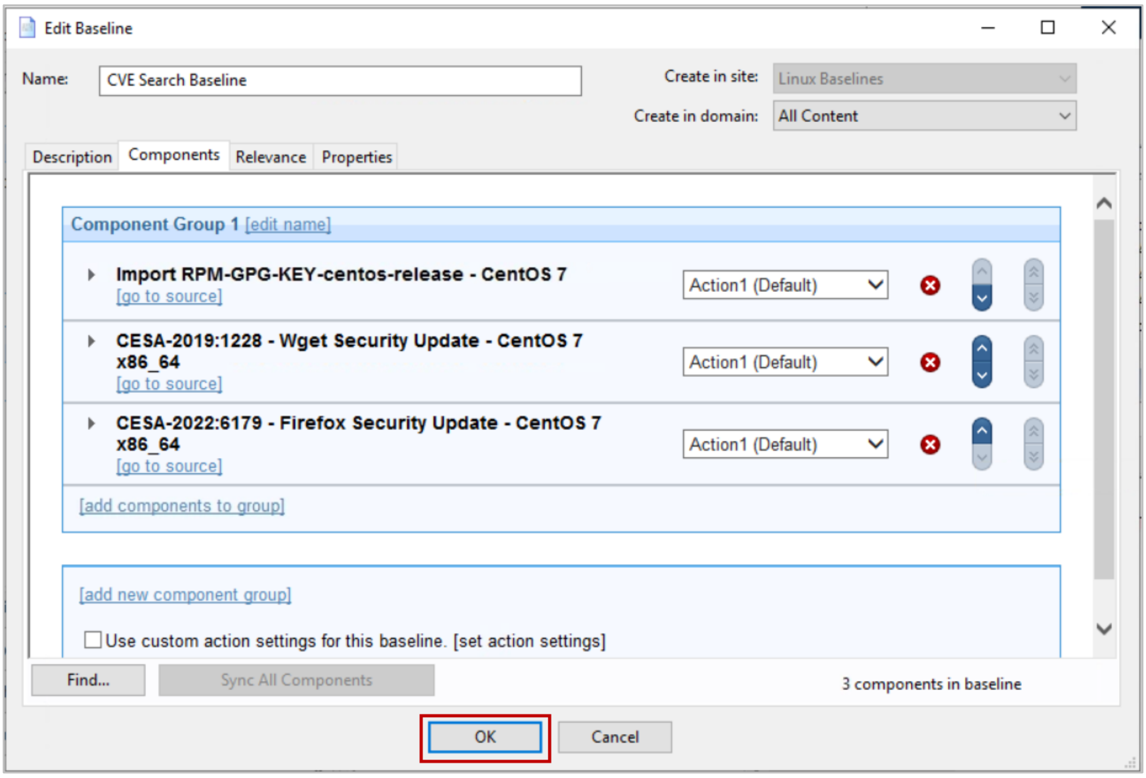
Component Group 1 [edit name]

- CESA-2019:1228 - Wget Security Update - CentOS 7 x86_64 [go to source] — Action1 (Default)
- CESA-2022:6179 - Firefox Security Update - CentOS 7 x86_64 [go to source] — Action1 (Default)
- Import RPM-GPG-KEY-centos-release - CentOS 7 [go to source] — Action1 (Default)

[add components to group]

Tip: Each time you click the up-arrow icon, the component is moved up 1 row. You must continue clicking the up-arrow until the Task is in the first position of the component list.

18. Click **OK**.



Edit Baseline

Name: CVE Search Baseline

Create in site: Linux Baselines

Create in domain: All Content

Component Group 1 [edit name]

Import RPM-GPG-KEY-centos-release - CentOS 7 [go to source] — Action1 (Default)

CESA-2019:1228 - Wget Security Update - CentOS 7 x86_64 [go to source] — Action1 (Default)

CESA-2022:6179 - Firefox Security Update - CentOS 7 x86_64 [go to source] — Action1 (Default)

[add components to group]

[add new component group]

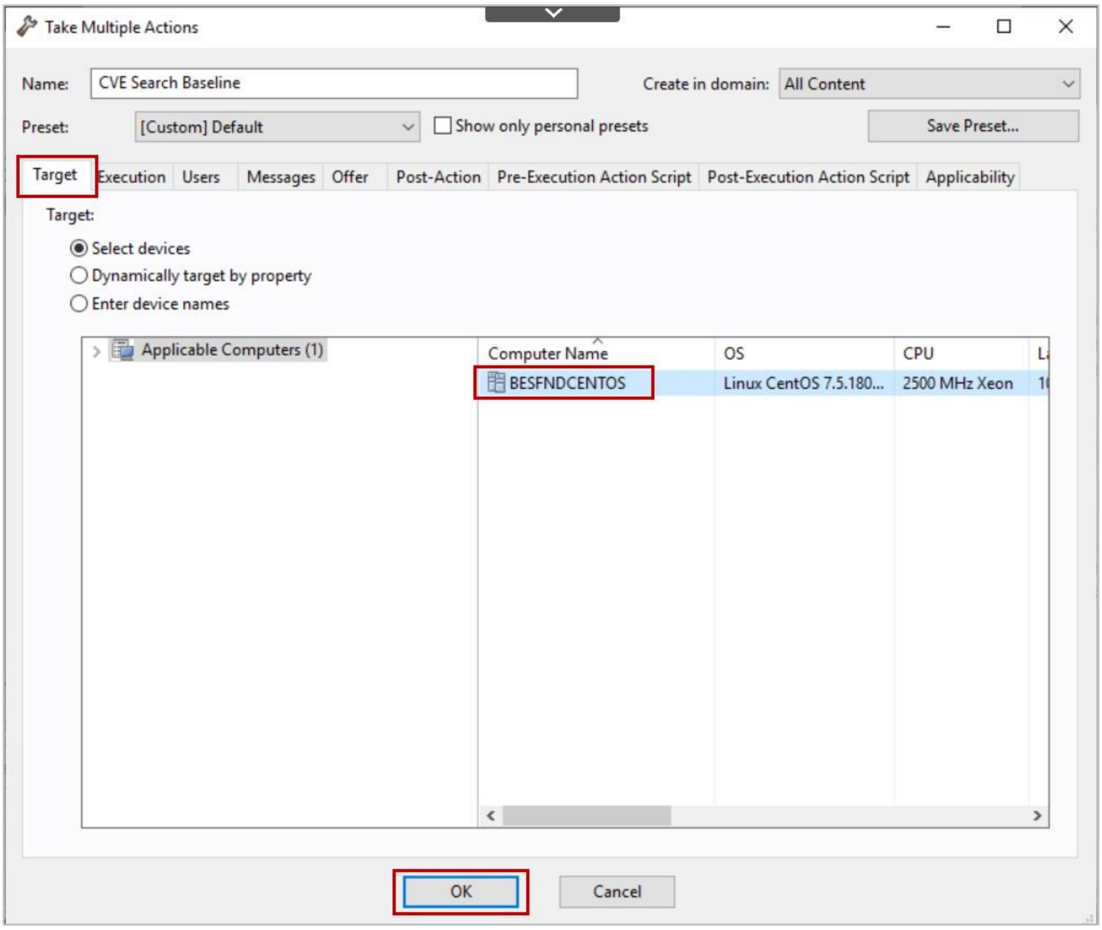
□ Use custom action settings for this baseline. [set action settings]

3 components in baseline

The Edit Baseline window closes and you are returned to the baseline.

19. Click the **Applicable Computers** tab and verify that the **BESFNDCENTOS** computer appears in the list of applicable targets. Wait until it appears before continuing to the next step.
20. Click **Take Action**. The Take Multiple Actions window opens.

21. Click the **Target** tab and select **BESFNDCENTOS** from the list of available targets. Click **OK**.



Name: CVE Search Baseline

Create in domain: All Content

Preset: [Custom] Default

□ Show only personal presets

Target:

● Select devices

○ Dynamically target by property

○ Enter device names

Computer Name	OS	CPU	L
BESFNDCENTOS	Linux CentOS 7.5.180...	2500 MHz Xeon	1

The Action window opens.

22. Monitor the status of the action and wait for it to change to **Completed** before proceeding.

You have now completed Exercise 11.

Exercise 12 – Creating a Saved Report in BigFix Compliance Analytics

BigFix Compliance helps to manage increasingly complex IT environments by providing detailed security reports.

In this exercise, you customize, create, and save a report using BigFix Compliance Analytics.

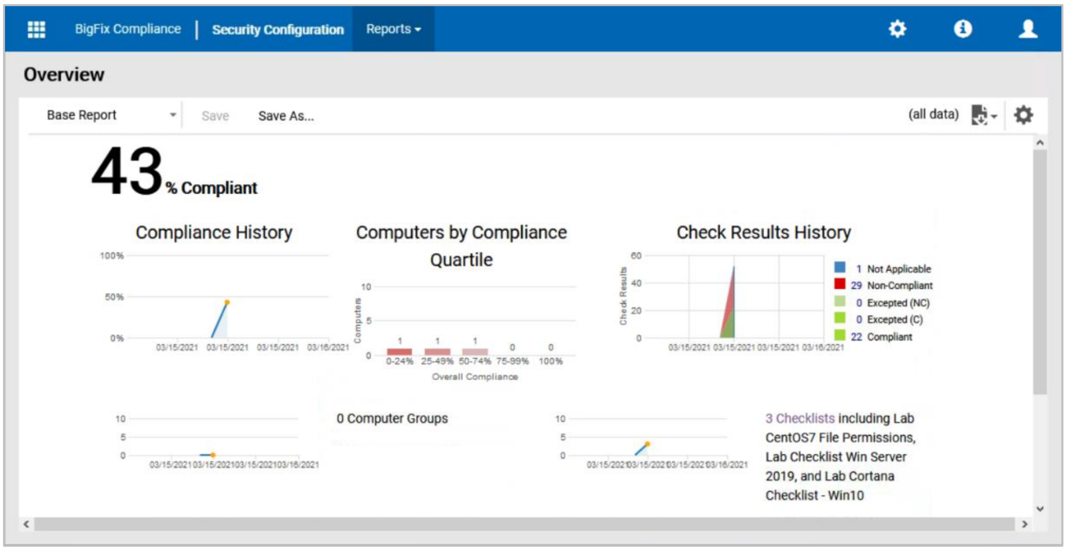
1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double click the **Firefox** icon on the desktop. The browser opens.
3. Enter the following URL in the address section of the browser: https://BESFNDWINROOT:9085

   Note: You might receive a security warning indicating that it is unsafe to continue to the page. Click the Advanced option, accept the risk and continue to the site.

   The BigFix Compliance login page opens.

4. Enter **adminmo** as the username with a password of **B1gfixrocks!**. Click **Login**. The Overview page opens.

   Note: The Overview page shows an overall Compliance percentage along with a variety of statistical widgets that pertain to various compliance categories. Your screen may look slightly different.

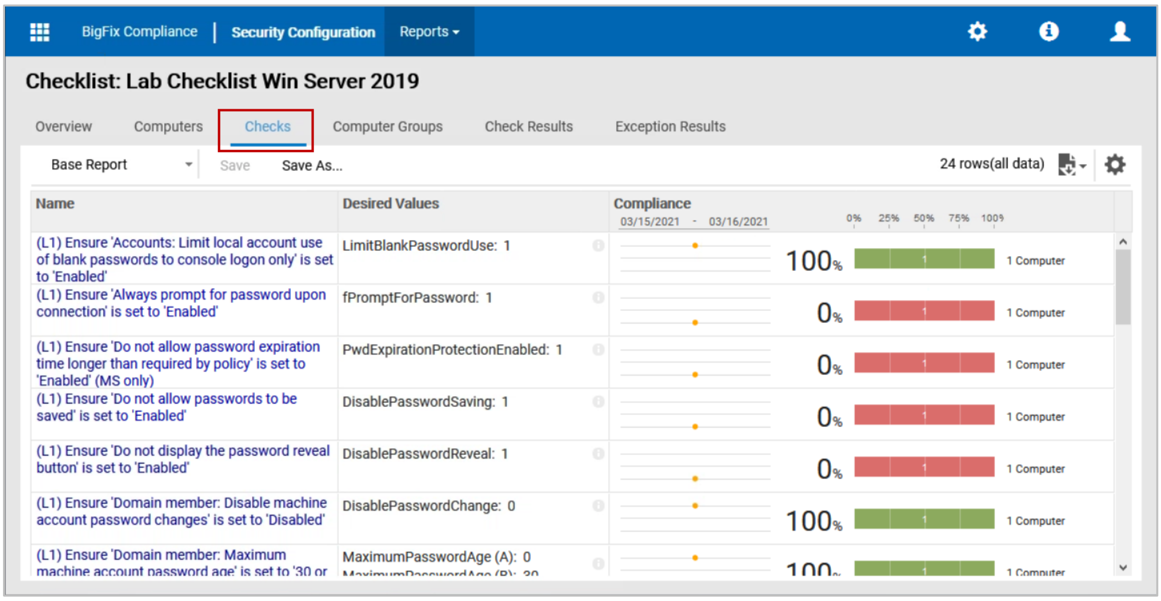


5. Select **Checklists** from the **Reports** menu at the top of the **Overview** page. The Checklist page opens and displays a list of the Custom Checklists that are enabled. You can also access the Checklists report by clicking the **## Checklists** link on the **Overview** report.
6. Review the compliance levels of the various checklists.

   Tip: You can sort the data that is displayed by clicking the title of the column header of the data that you wish to sort. You can toggle the sort order from ascending to descending by clicking the column header again.

7. Click the **link** for the **Lab Checklist Win Server 2019** checklist. An overview page for the selected checklist opens.

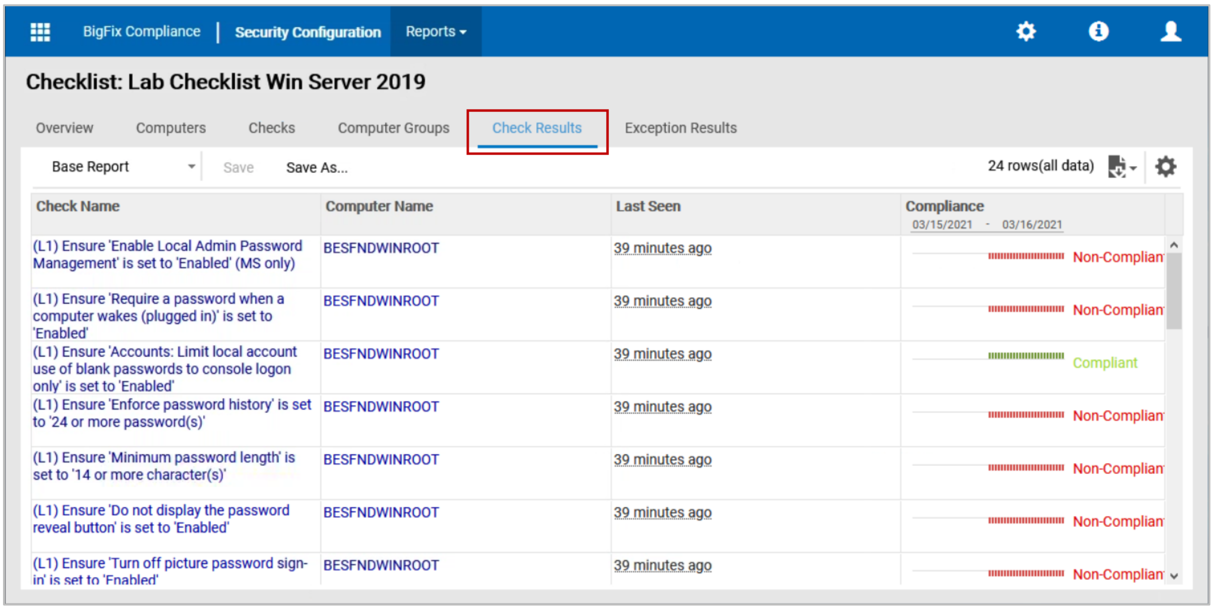
8. Click the **Checks** tab at the top of the Overview page. The Checks report for the selected checklist opens and shows the compliance percentage for each check in the checklist.



Checklist: Lab Checklist Win Server 2019

Name	Desired Values	Compliance 03/15/2021 - 03/16/2021		
(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	LimitBlankPasswordUse: 1	100%	🟩	1 Computer
(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	fPromptForPassword: 1	0%	🟥	1 Computer
(L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)	PwdExpirationProtectionEnabled: 1	0%	🟥	1 Computer
(L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	DisablePasswordSaving: 1	0%	🟥	1 Computer
(L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	DisablePasswordReveal: 1	0%	🟥	1 Computer
(L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	DisablePasswordChange: 0	100%	🟩	1 Computer
(L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or	MaximumPasswordAge (A): 0 MaximumPasswordAge (B): 30	100%	🟩	1 Computer

9. Click the **Check Results** tab at the top of the Overview page. The Checks Results report for the selected checklist opens and shows whether each check is Compliant or Non-Compliant for each computer that is subscribed to the Checklist.



Checklist: Lab Checklist Win Server 2019

Check Name	Computer Name	Last Seen	Compliance 03/15/2021 - 03/16/2021
(L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)	BESFNDWINROOT	39 minutes ago	Non-Complian
(L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	BESFNDWINROOT	39 minutes ago	Non-Complian
(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	BESFNDWINROOT	39 minutes ago	Compliant
(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	BESFNDWINROOT	39 minutes ago	Non-Complian
(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	BESFNDWINROOT	39 minutes ago	Non-Complian
(L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	BESFNDWINROOT	39 minutes ago	Non-Complian
(L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled'	BESFNDWINROOT	39 minutes ago	Non-Complian

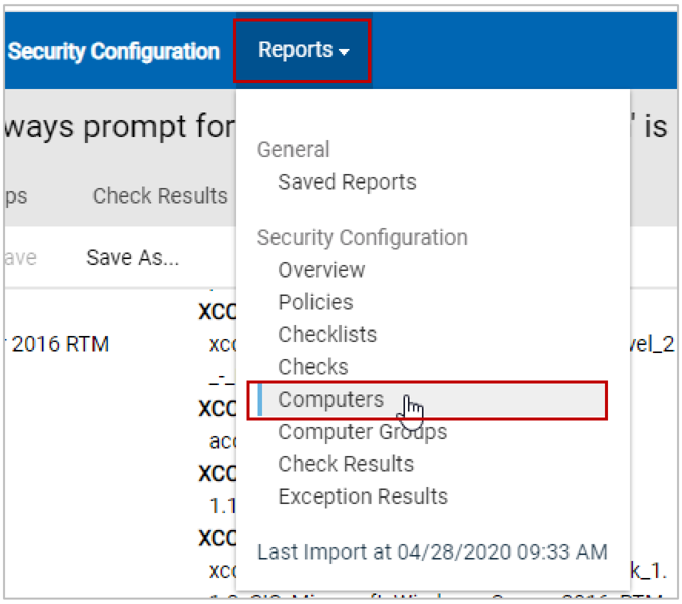
10. Click the **Check Name** column header. The checks are sorted by name in ascending alphabetical order.

    Tip: You can click the Check Name column header again to reverse the sort order.

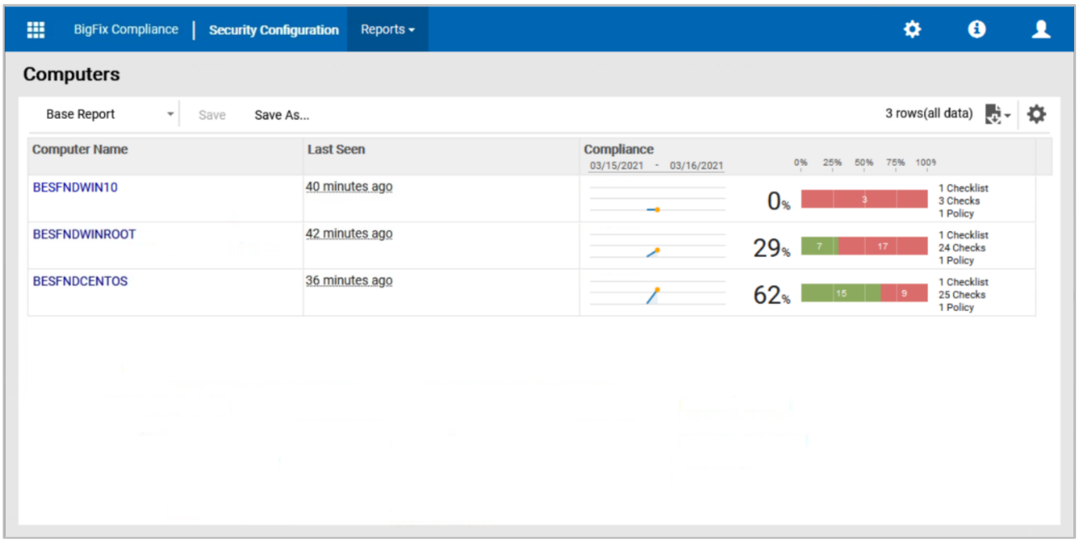
11. Locate the check named **(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'**. Observe whether the check is Compliant or Non-Compliant for **BESFNDWINROOT**.

12. Click the link for the check named **(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'**. The Overview report for the selected compliance check opens.

13. Review the details for the selected check on the **Overview** report. Note the Source, Source ID, Source Release Date and Description for the check.
14. Select **Computers** from the **Reports** menu at the top of the browser.



The Computers report opens and shows the compliance level for all computers.

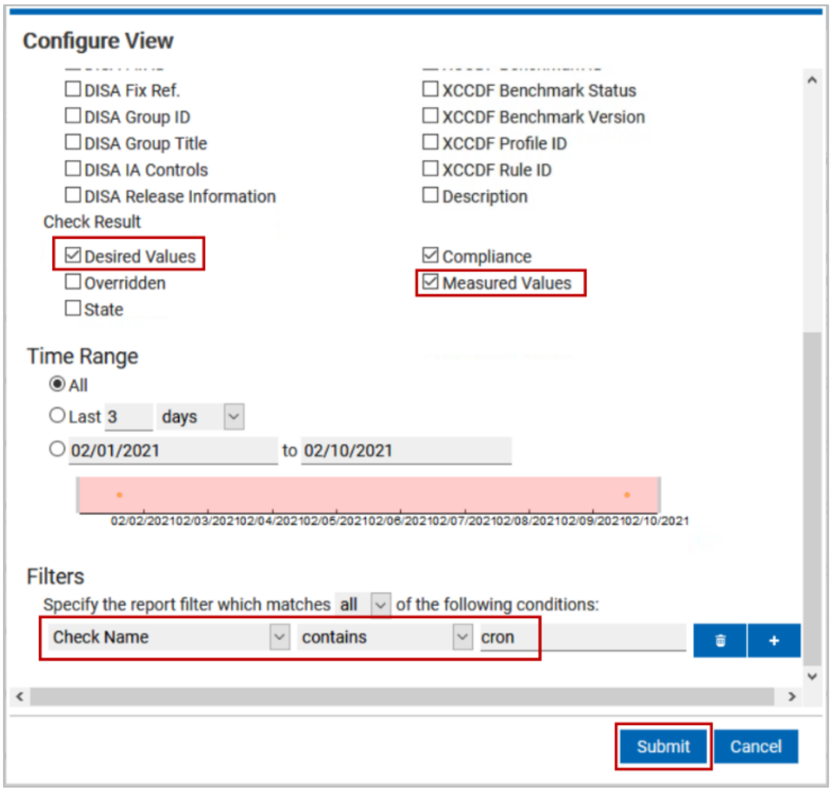


Computers

Computer Name	Last Seen	Compliance 03/15/2021 - 03/16/2021		
BESFNDWIN10	40 minutes ago	0%	3	1 Checklist 3 Checks 1 Policy
BESFNDWINROOT	42 minutes ago	29%	7 17	1 Checklist 24 Checks 1 Policy
BESFNDCENTOS	36 minutes ago	62%	15 9	1 Checklist 25 Checks 1 Policy

15. Click **BESFNDCENTOS** in the **Computer Name** column. The Overview report for the selected computer is displayed.
16. Click the **Check Results** tab at the top of the Overview report. Each Checklist and Check Name that the selected computer is subscribed to is shown in the Check Results report.
17. Click the **gear** icon in the upper-right portion of the Check Results report. The Configure View window opens.
18. Scroll down to the **Check Result** section. Place a check beside the **Desired Values**, and **Measured Values** checkbox. The selected columns are added to the report view.
19. Scroll to the bottom of the **Configure View** window and click the plus (**+**) sign in the **Filters** section.

20. Set the Filter criteria as follows, then click **Submit**:
    a. Select **Check Name** from the first drop-down box.
    b. Select **contains** from the second drop-down box.
    c. Enter **cron** in the text field.



Configure View

☐ DISA Fix Ref.
☐ DISA Group ID
☐ DISA Group Title
☐ DISA IA Controls
☐ DISA Release Information
☐ XCCDF Benchmark Status
☐ XCCDF Benchmark Version
☐ XCCDF Profile ID
☐ XCCDF Rule ID
☐ Description

Check Result

☑ Desired Values
☐ Overridden
☐ State
☑ Compliance
☑ Measured Values

Time Range

● All
○ Last 3 days
○ 02/01/2021 to 02/10/2021

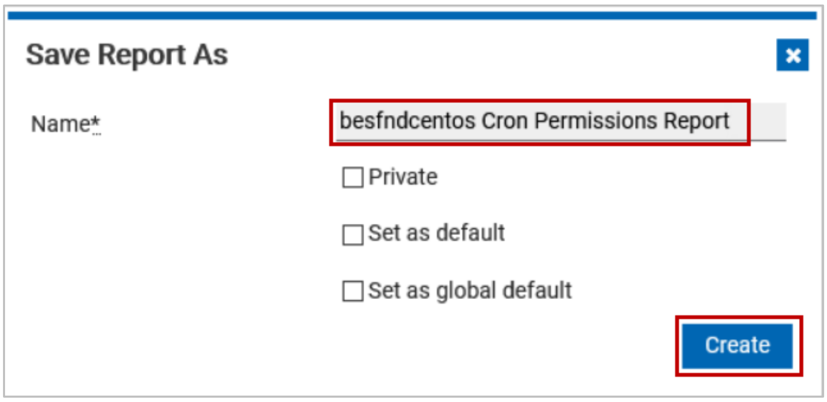
Filters

Specify the report filter which matches all of the following conditions:

Check Name | contains | cron

The Computers report updates to show only the checks whose name contains the string cron.

21. Click and drag the **Measured Values** column to the right of the **Desired Values** column.
22. Click **Save As**. The Save Report As window opens.
23. Enter **besfndcentos Cron Permissions Report** in the **Name** field.



Save Report As

Name*: besfndcentos Cron Permissions Report

☐ Private
☐ Set as default
☐ Set as global default

24. Click **Create**.
25. Select **Saved Reports** from the **Reports** menu at the top of the BigFix Compliance page. The besfndcentos Cron Permissions Report shows in the list Saved Reports list.

26. Click the report **link** in the **Name** field to view the saved report.
27. Optional – Investigate other compliance reports that were discussed during the presentation.

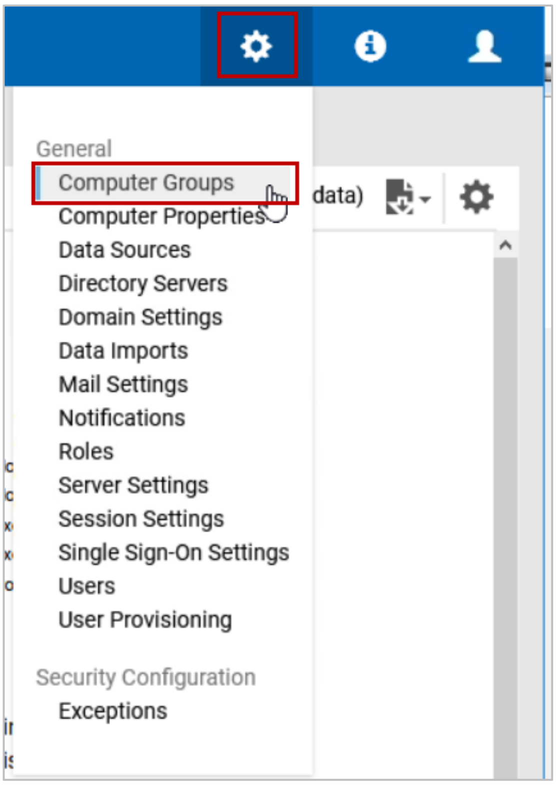
You have now completed Exercise 12.

Exercise 13 – Creating Computer Groups in SCA

Computer Groups can be created in SCA and used as reporting groups or used to limit access to specific users. These groups can be totally new groups that do not currently exist in the BigFix Console, or they can be linked to existing BigFix computer groups.

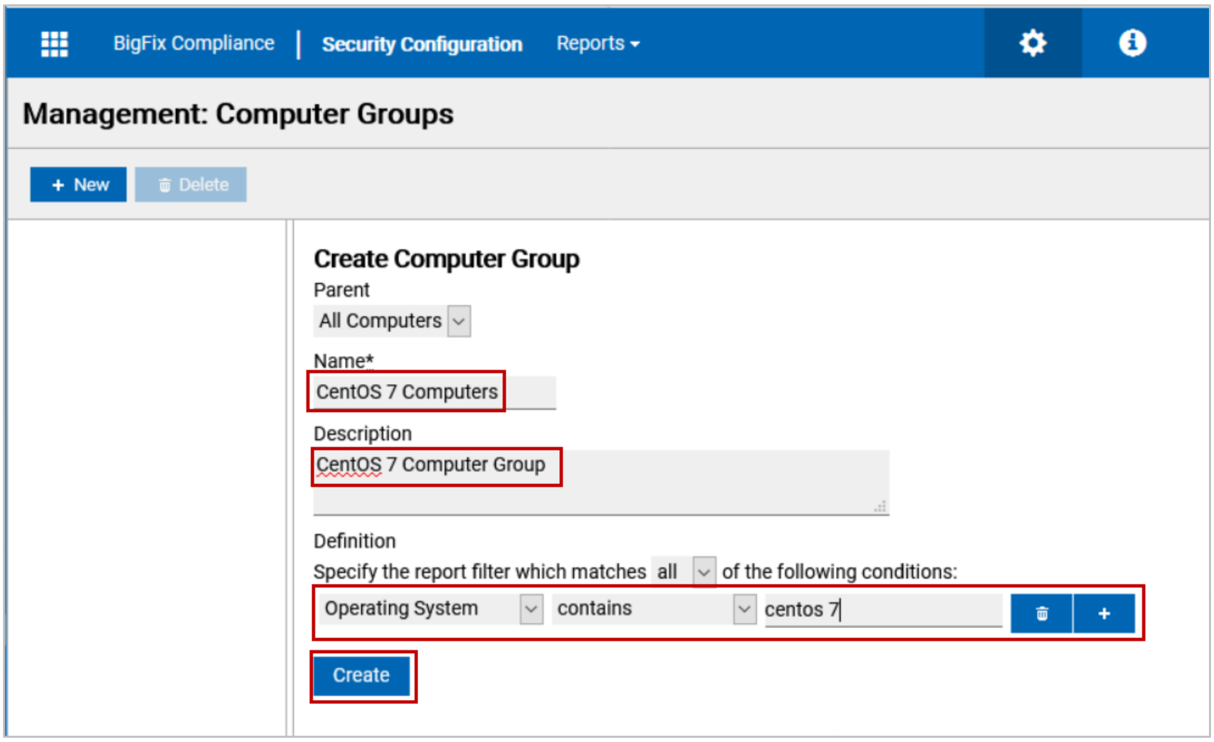
In this exercise, you create SCA reporting computer groups.

1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **adminmo** with a password of **B1gfixrocks!**.
2. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



3. Select **Computer Groups** from the Management menu. The Computer Groups page opens.
4. Click **New** in the upper-left portion of the **Computer Groups** page. The Create Computer Group pane opens.
5. Enter **CentOS7 Computers** in the **Name** field.
6. Enter **CentOS7 Computer Group** in the **Description** field.

7. Click the plus sign **(+)** in the **Definition** section. Define the group membership as follows;
   - Select **Operating System** from the first drop-down box.
   - Select **contains** from the second drop-down box.
   - Enter **centos 7** in the text field.



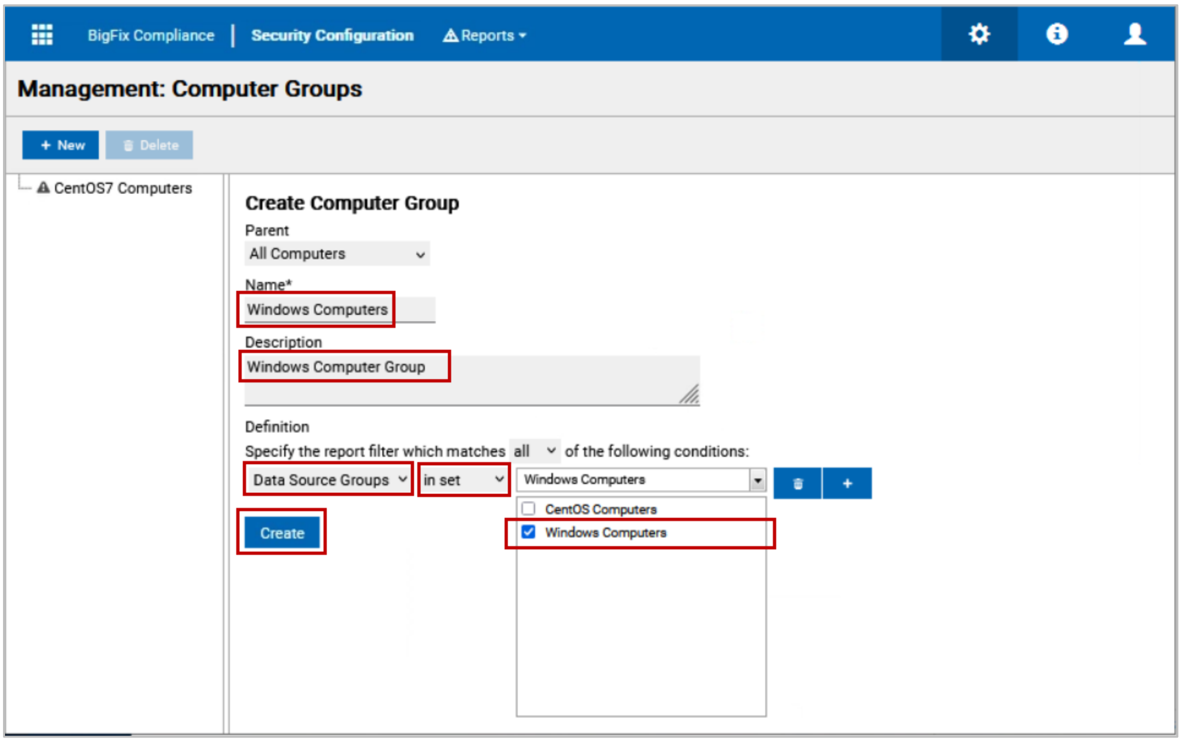
8. Click **Create**. A message is displayed indicating that the Computer Group was successfully created.

   Hint: The Group Name displays a warning triangle next to the name. This indicates that the group definition is not available for use until after the next Data Import is performed.

We now create a computer group based on an existing BigFix Automatic Computer Group.

9. Click **New** in the upper-left portion of the **Computer Groups** page. The Create Computer Group pane opens.
10. Enter **Windows Computers** in the **Name** field.
11. Enter **Windows Computer Group** in the **Description** field.

12. Click the plus sign **(+)** in the **Definition** section. Define the group membership as follows:
    - Select **Data Source Groups** from the first drop-down box.
    - Select **in set** from the second drop-down box.
    - Place a check beside **Windows Computers** from the third drop-down box.



Management: Computer Groups

Create Computer Group

Parent: All Computers

Name*: Windows Computers

Description: Windows Computer Group

Definition

Specify the report filter which matches all of the following conditions:

Data Source Groups | in set | Windows Computers

☐ CentOS Computers

☑ Windows Computers

Create

13. Click **Create**. A message is displayed indicating that the Computer Group was successfully created.

You have now completed Exercise 13.

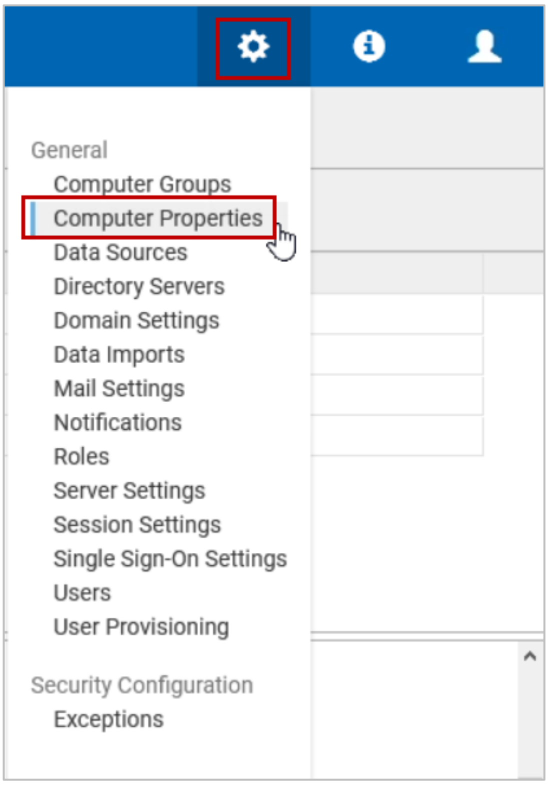
Exercise 14 – Creating Computer Properties

Computer Properties can be created in SCA by linking the properties from available Data Sources. These properties can be used in report filter definitions or can be included as additional columns in reports

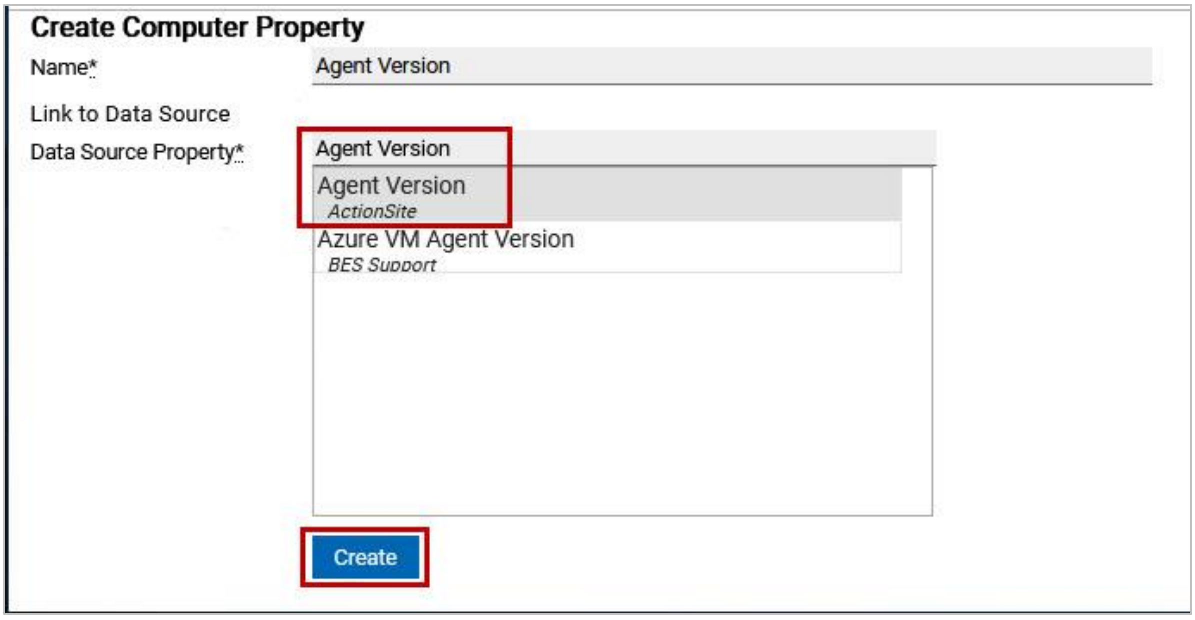
In this exercise, you create a Computer Property using the Computer Properties interface.

1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **adminmo** with a password of **B1gfixrocks!**.
2. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.

3. Select **Computer Properties** from the **Management** menu. The Computer Properties page opens.



4. Click **New** in the upper-left portion of the **Computer Properties** page. The Create Computer Property pane opens at the bottom of the page.
5. Begin typing the string **Agent Version** in the **Link to Data Source** field. As you type the name the properties are filtered. Locate **Agent Version** in the filtered list and select it.



Create Computer Property

Name* Agent Version

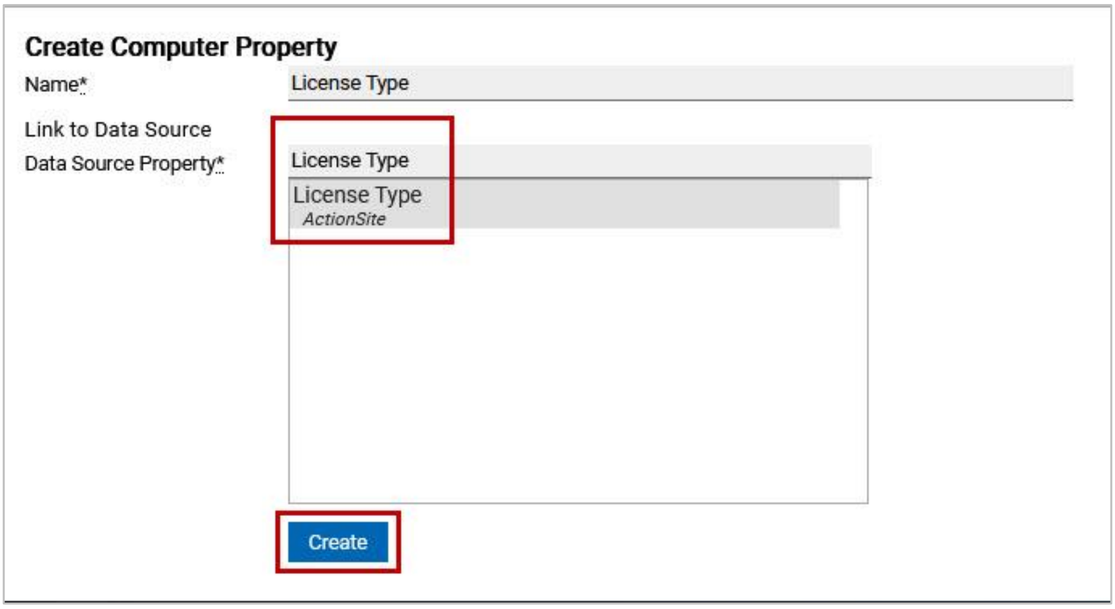
Link to Data Source

Data Source Property* Agent Version

6. Click **Create**. A message is displayed indicating that the Computer Property was successfully created.

Hint: The new property displays a warning triangle next to the name. This indicates that the property definition is not available for use until after the next Data Import is performed.

7. Click **New** in the upper-left portion of the **Computer Properties** page. The Create Computer Property pane opens at the bottom of the page.
8. Begin typing the string **License Type** in the **Link to Data Source** field. As you type the name the properties are filtered. Locate **License Type** in the filtered list and select the one that is associated with the ***ActionSite***.



Create Computer Property

Name*: License Type

Link to Data Source

Data Source Property*: License Type

9. Click **Create**. A message is displayed indicating that the Computer Property was successfully created.

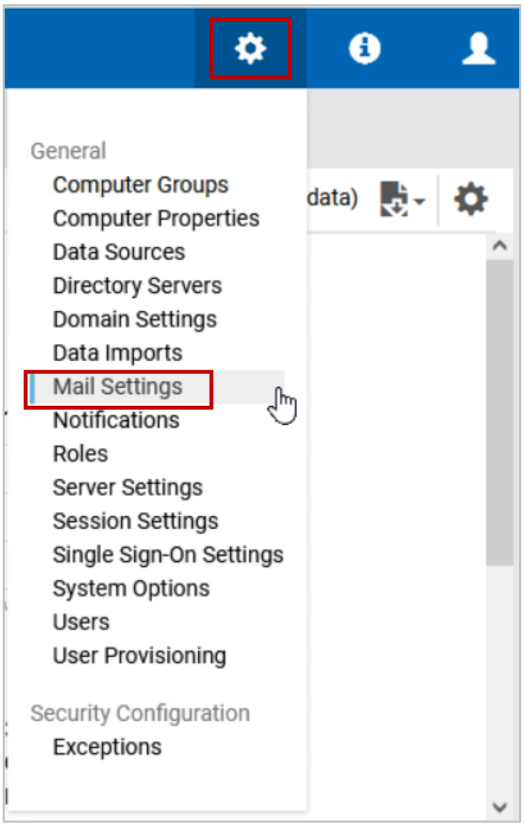
You have now completed Exercise 14.

Exercise 15 – Defining an Email SMTP Server

In this exercise, you define and outgoing email server so that you can create and send email alerts and schedule report distribution.

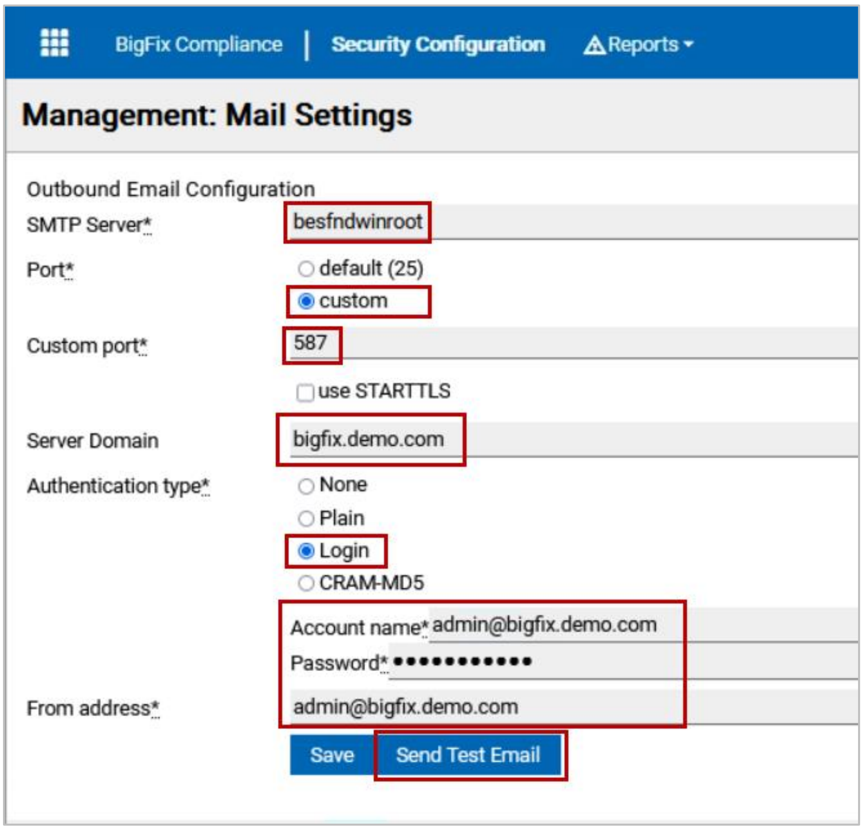
1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **adminmo** with a password of **B1gfixrocks!**.

2. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



3. Select **Mail Settings** from the **Management** menu. The Management: Mail Settings page opens.

4. Enter the following information in the **Outbound Email Configuration** form:
    - SMTP Server* field: Enter **10.0.0.1**
    - Port* field: Select the **custom** option
    - Custom port* field: Enter **587**
    - Server Domain: **bigfix.demo.com**
    - Authentication type*: Verify that the **Login** option is selected
    - Account name* field: Enter **admin@bigfix.demo.com**
    - Password* field: Enter **B1gfixrocks**
    - From address* field: Enter **admin@bigfix.demo.com**



Management: Mail Settings

Outbound Email Configuration

SMTP Server*: besfndwinroot

Port*: ○ default (25) ● custom

Custom port*: 587

□ use STARTTLS

Server Domain: bigfix.demo.com

Authentication type*: ○ None ○ Plain ● Login ○ CRAM-MD5

Account name*: admin@bigfix.demo.com

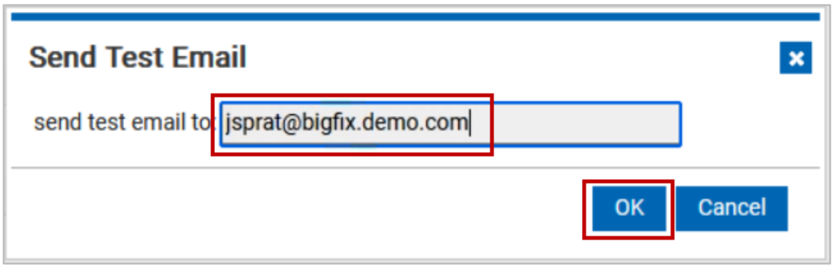
Password*: ●●●●●●●●●●●●

From address*: admin@bigfix.demo.com

5. Click **Send Test Email**. The Send Test Email window opens.

   Note: If the Save login browser pop-up opens click **Don't save**.

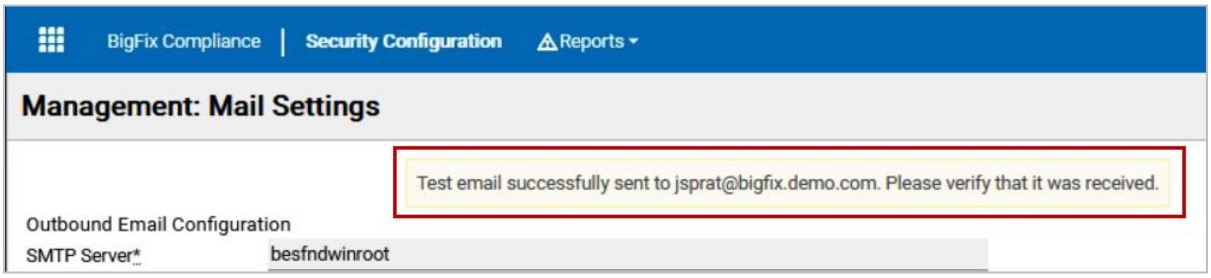
6. In the **send test email to:** field enter **jsprat@bigfix.demo.com** and click **OK**.



Send Test Email

send test email to: jsprat@bigfix.demo.com

A message is displayed indicating that the test email was successfully sent.



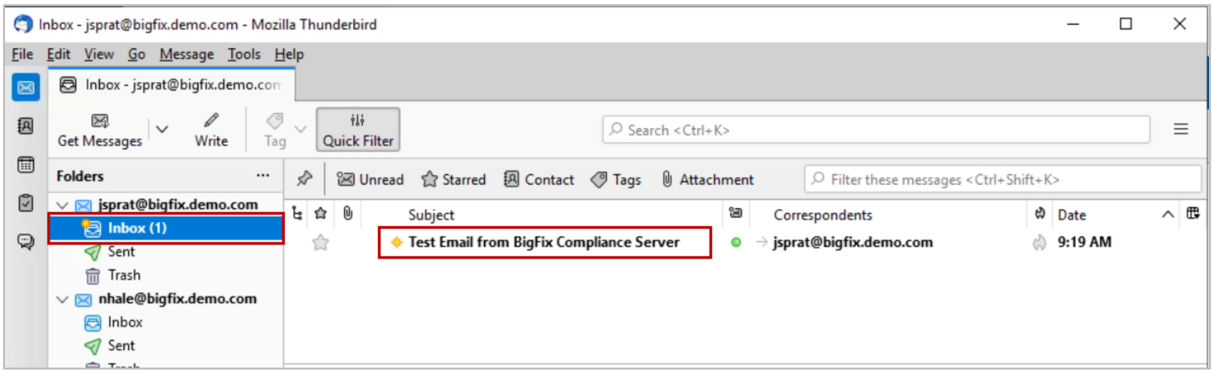
Management: Mail Settings

Test email successfully sent to jsprat@bigfix.demo.com. Please verify that it was received.

Outbound Email Configuration

SMTP Server* besfndwinroot

7. **Double-click** the **Mozilla Thunderbird** icon on the **Windows desktop**. The Mozilla Thunderbird application opens.
8. Select the **Inbox** for the **jsprat@bigfix.demo.com** account. Verify that the test message was received.



Subject	Correspondents	Date
Test Email from BigFix Compliance Server	jsprat@bigfix.demo.com	9:19 AM

9. Close **Mozilla Thunderbird**.
10. Return to the **Mail Settings** page in the **Firefox** browser and click **Save**. A message appears indicating that the Mail Settings were successfully saved.

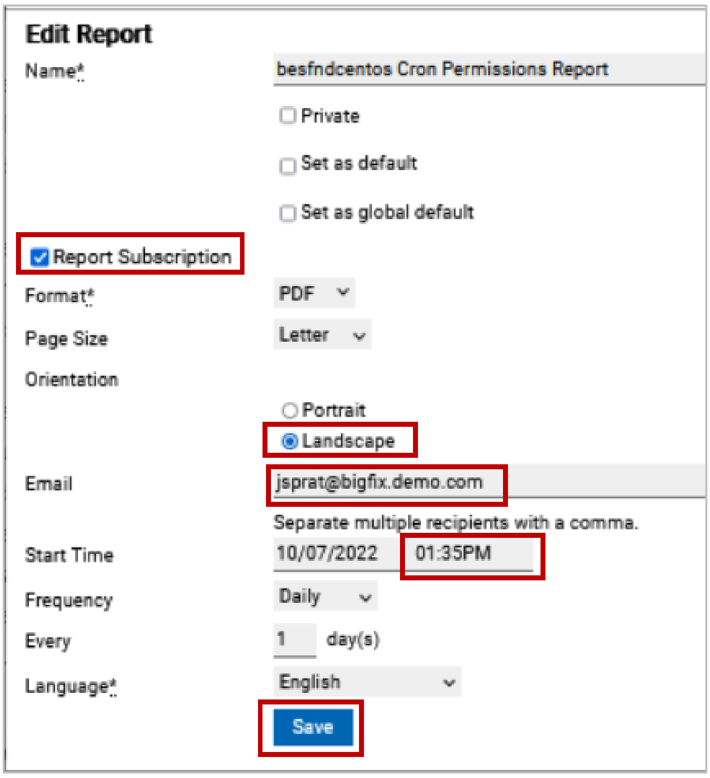
You have now completed Exercise 15.

Exercise 16 – Creating Notifications and Scheduling a Saved Report

In this exercise, you create an email notification to be sent when a failed import occurs. You also schedule the recurring email distribution of a saved report.

1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **adminmo** with a password of **B1gfixrocks!**.
2. Select **Saved Reports** from the **Reports** menu. The Saved Reports page opens with a list of the saved reports that you are allowed to see.
3. Click anywhere in the row for the **besfndcentos Cron Permissions Report**. The Edit Report pane opens at the bottom of the Saved Reports page.
4. Enter the following information in the Edit Reports pane:
    - Place a **check** beside the **Report Subscription** option.
    - Select the **Landscape** option in the **Orientation** section
    - Enter **jsprat@bigfix.demo.com** in the **Email** field.
    - Change the time in the **Start Time** field to be approximately **10 minutes** into the future.

5. Click **Save**.



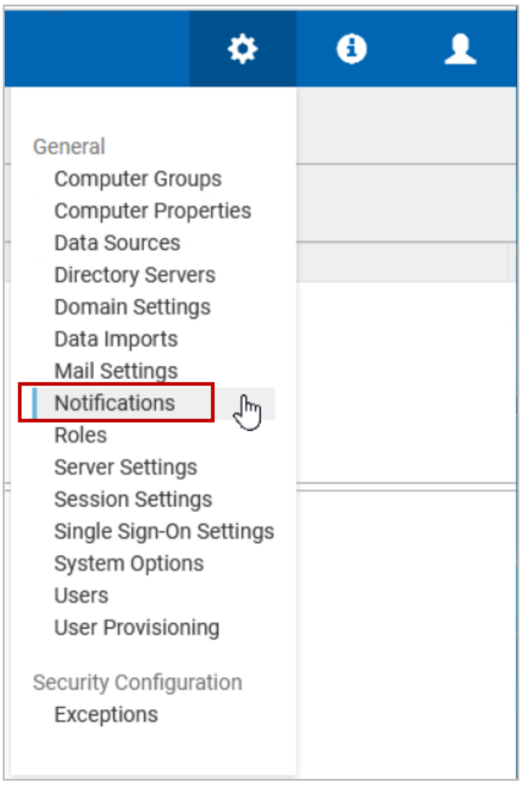
Edit Report

Name*	besfndcentos Cron Permissions Report
	□ Private
	□ Set as default
	□ Set as global default
☑ Report Subscription	
Format*	PDF
Page Size	Letter
Orientation	○ Portrait ● Landscape
Email	jsprat@bigfix.demo.com Separate multiple recipients with a comma.
Start Time	10/07/2022 01:35PM
Frequency	Daily
Every	1 day(s)
Language*	English

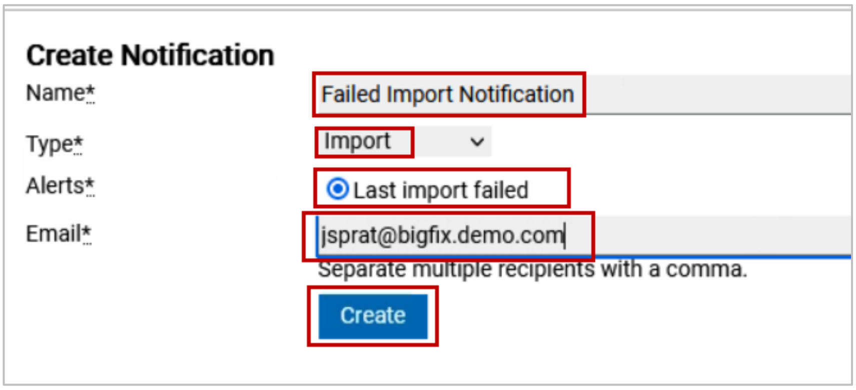
A message appears indicating that the report was successfully saved and the date and time of the scheduled export is shown in the Next Scheduled Export column on the Saved Reports page.

You now create an email notification for failed imports.

6. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



7. Select **Notifications** from the **Management** menu. The Management: Notifications page opens.
8. Click **New** in the upper-left portion of the **Notifications** page. The Create Notification pane opens below.
9. Enter the following information in the Create Notification pane to define the Failed Import notification:
   - Name* field: Enter **Failed Import Notification**
   - Type* field: Select **Import** from the dropdown box
   - Alerts* field: Select the **Last import failed** option
   - Email* field: Enter **jsprat@bigfix.demo.com**



Create Notification

Name* Failed Import Notification

Type* Import

Alerts* ● Last import failed

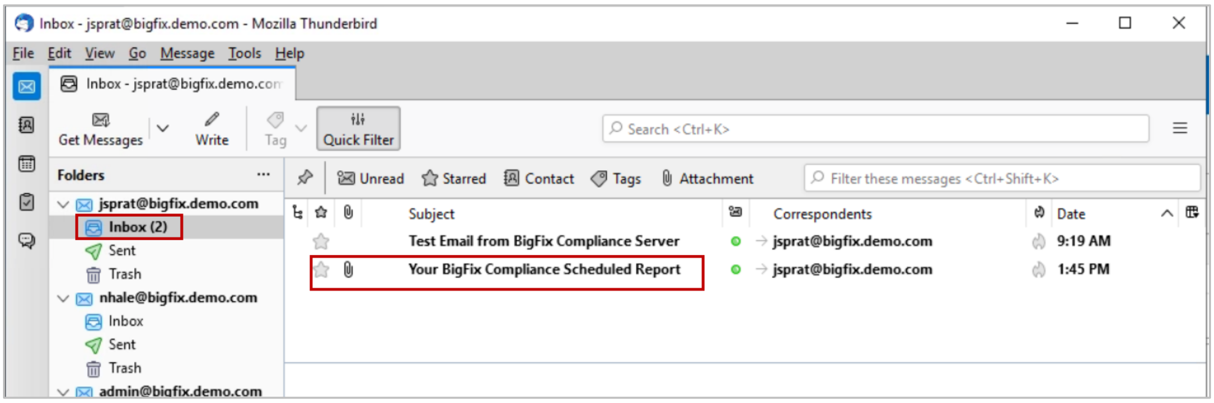
Email* jsprat@bigfix.demo.com

Separate multiple recipients with a comma.

10. Click **Create**. The Failed Import Notification is listed on the Notifications page.

You now verify that the scheduled export of the saved report was successful.

11. **Double-click** the **Mozilla Thunderbird** icon on the **Windows Desktop**.
12. Select the **Inbox** for **jsprat@bigfix.demo.com** and verify that the email with a **Subject** of **Your BigFix Compliance Scheduled Report** has been received.



Subject	Correspondents	Date
Test Email from BigFix Compliance Server	jsprat@bigfix.demo.com	9:19 AM
Your BigFix Compliance Scheduled Report	jsprat@bigfix.demo.com	1:45 PM

Important: If the scheduled report has not been received, verify that the scheduled time that was created for the report's distribution has passed. If not, then wait until the scheduled time has passed. You can click the Get Messages button in the upper-left portion of the Mozilla Thunderbird application.

13. (Optional) **Double-click** the **email** to open, then **double-click** the **attachment** located at the bottom of the email to view the report.
14. Close **Mozilla Thunderbird**.

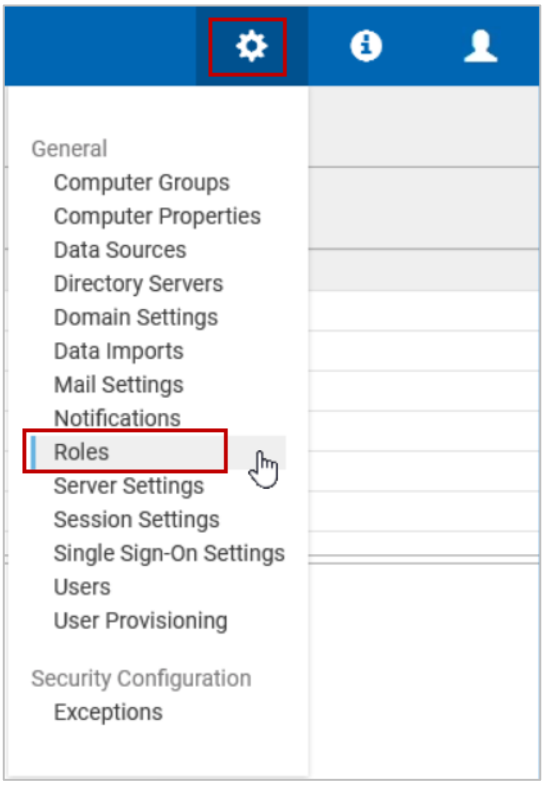
You have now completed exercise 16.

Exercise 17 – Creating Roles and Users

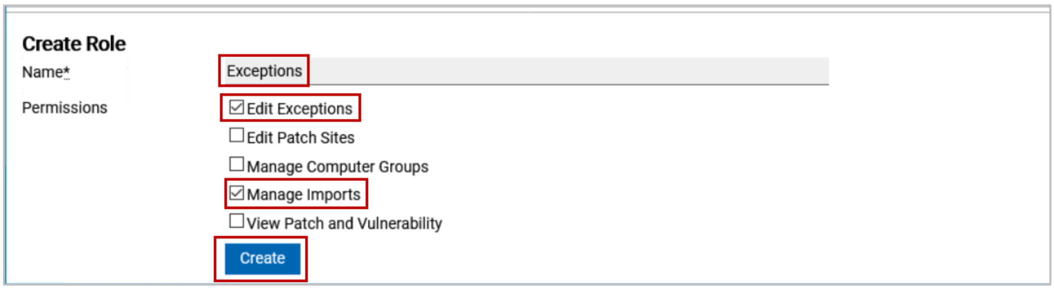
In this exercise, you create a custom Role in SCA. You then create a local user and assign that user Security Roles.

1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **adminmo** with a password of **B1gfixrocks!**.

2. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



3. Select **Roles** from the Management menu. The Management: Roles page opens and shows the existing Administrators Role
4. Click **New** in the upper-left portion of the page. The Create Role pane opens in the lower portion of the page.
5. Enter **Exceptions** in the **Name** field. Then select the following permissions from the list;
   - **Edit Exceptions**
   - **Manage Imports**



Create Role

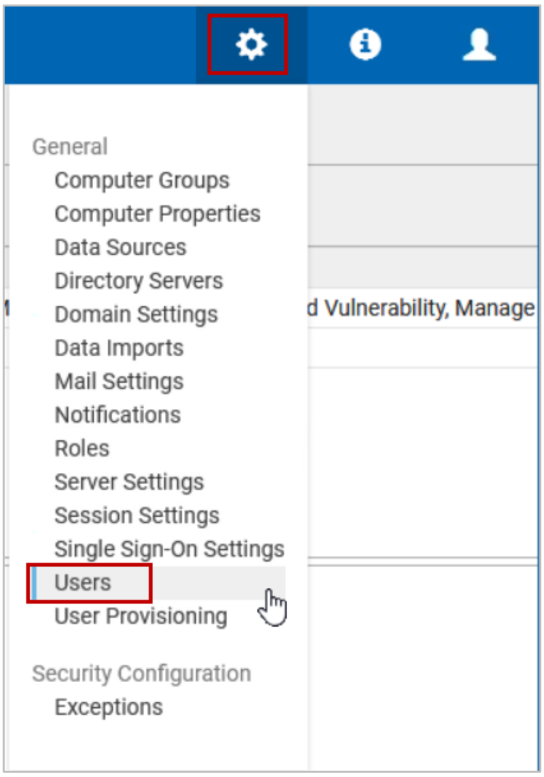
Name* Exceptions

Permissions
☑ Edit Exceptions
☐ Edit Patch Sites
☐ Manage Computer Groups
☑ Manage Imports
☐ View Patch and Vulnerability

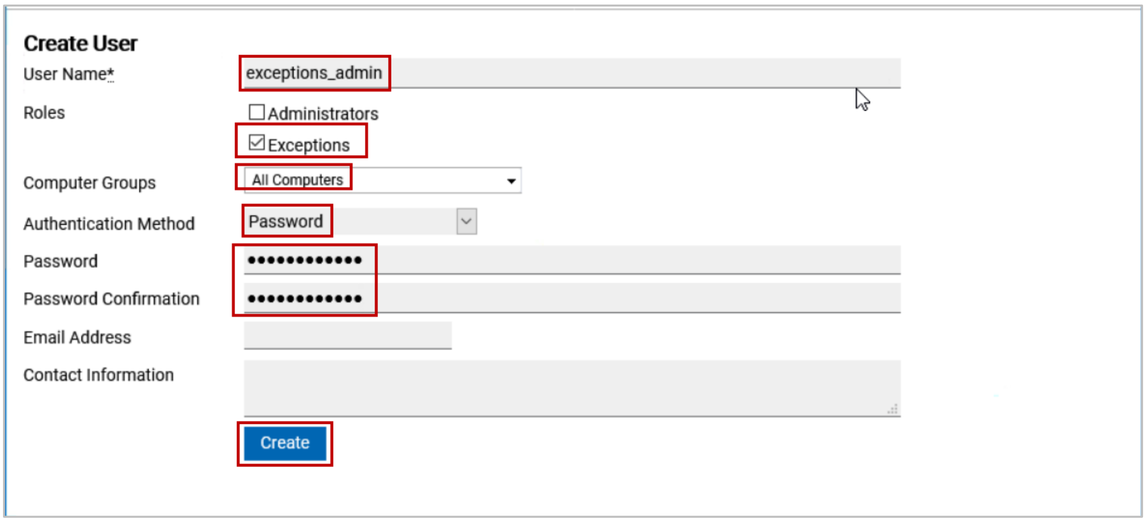
6. Click the **Create.** The Exceptions role is created and now appears in the list of available Roles that can be assigned when creating users.

You now create a local SCA User account and assign Roles and resources.

7. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



8. Select **Users** from the Management menu. The Management: Users page opens and shows the existing adminmo user.
9. Click **New** in the upper-left portion of the page. The Create User pane opens in the lower portion of the page.
10. Define the attributes for the new user by entering the information in the form as follows;
    - User Name: **exceptions_admin**
    - Roles: Select **Exceptions**
    - Computer Groups: Select **All Computers** from the drop-down menu
    - Authentication Method: Leave the default method **Password** selected.
    - Password: **B1gfixrocks!**
    - Password Confirmation: **B1gfixrocks!**
    - Email Address: Leave blank
    - Contact Information: Leave blank



Create User

User Name*: exceptions_admin

Roles: ☐ Administrators ☑ Exceptions

Computer Groups: All Computers

Authentication Method: Password

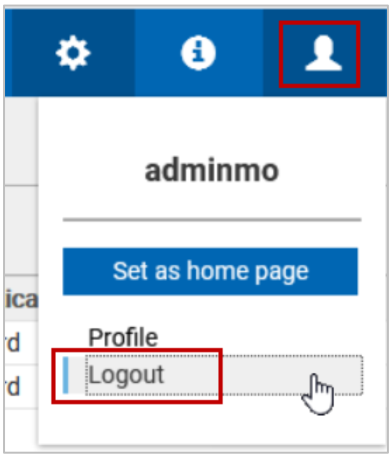
Password: ••••••••••••

Password Confirmation: ••••••••••••

Email Address:

Contact Information:

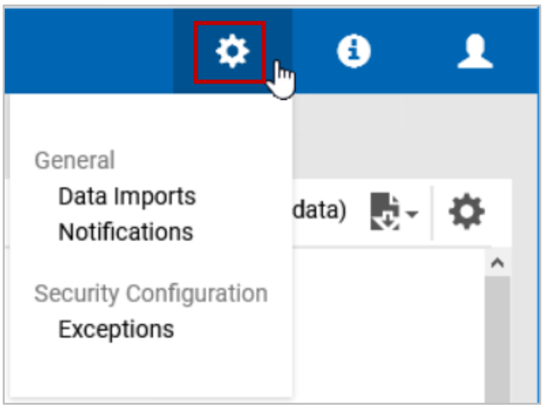
11. Click **Create**. The exceptions_admin user is included in the list of users on the Management: Users page.
12. Select the **User** icon in the upper-right portion of the page, then select **Logout**.



You are returned to the SCA login page.

13. Enter **exceptions_admin** as the username with a password of **B1gfixrocks!**. Click **Login**. The Overview page opens.

14. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



General
Data Imports
Notifications
Security Configuration
Exceptions

Observe that the **Management** menu only shows the options that the Role assigned to the exceptions_admin user allows.

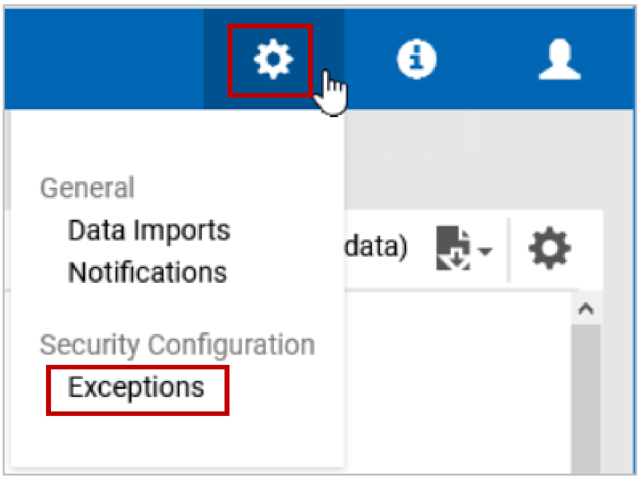
You have now completed exercise 17.

Exercise 18 – Creating Exceptions

Exceptions can be created that allow the specified endpoint to be excluded from certain compliance checks if they must adhere to older configuration standards. These endpoints can be excluded from all checks in a specified checklist, or from certain checks in a specified checklist.

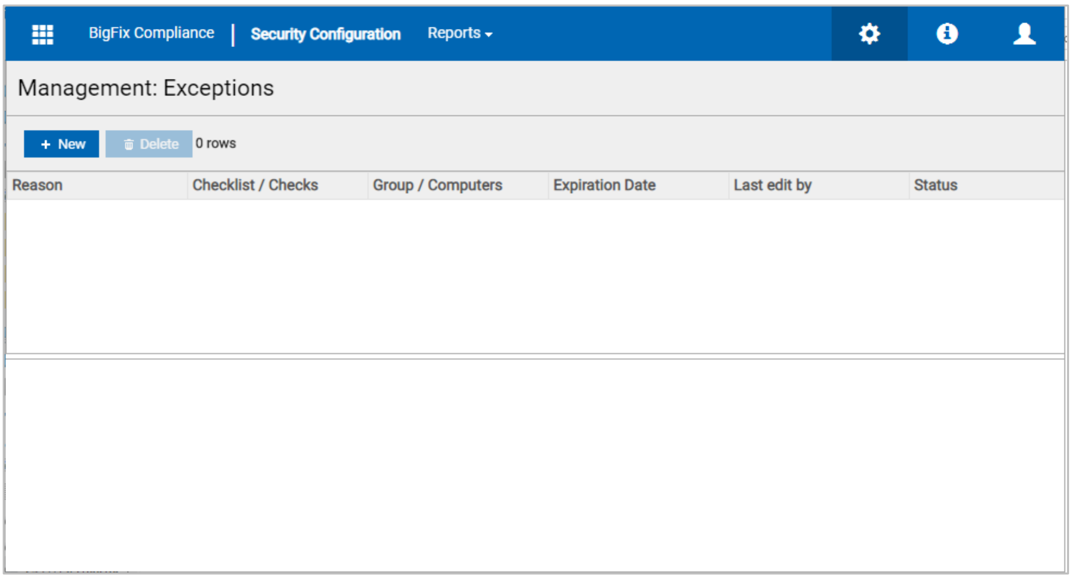
In this exercise, you create exceptions using the Exceptions interface while logged into SCA as the exceptions_admin user that was created in the previous exercise.

1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **exceptions_admin** with a password of **B1gfixrocks!**.
2. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



General
Data Imports
Notifications
Security Configuration
Exceptions

3. Select **Exceptions** from the Management menu. The Exceptions page opens.



Reason	Checklist / Checks	Group / Computers	Expiration Date	Last edit by	Status

4. Click **New** in the upper-left portion of the **Exceptions** page. The Create Exception window is displayed.
5. Enter the following text in the **Reason** field:

   Non-standard permissions on the bootloader config are required to support legacy applications.

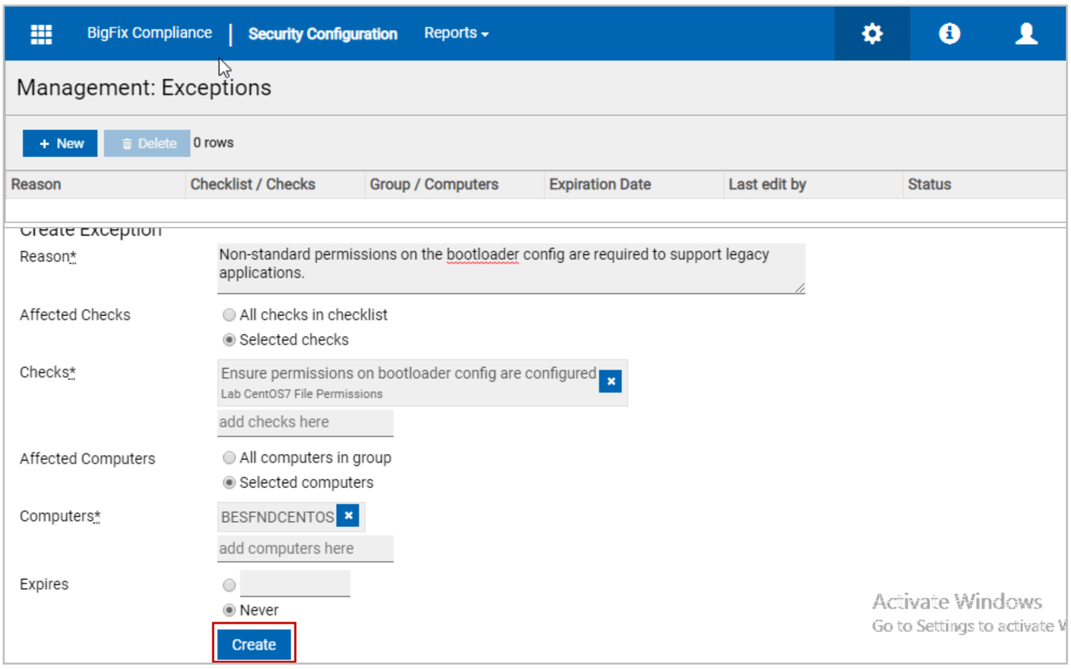
6. In the **Checks** field, begin typing the string **bootloader**. As you type, the checks are filtered to show only the checks that contain the search string. Select the check begins with the string **Ensure permissions on bootloader config**.

   Hint: IF you must apply this exception to multiple checks, you can continue to search for and add additional checks using the same search and select method.

7. In the **Affected Computers** section, verify that the **Selected computers** option is selected.
8. In the **Computers** field, begin typing **besfndcentos**. As you type, the computers list is filtered to show only those whose name contains the search string. Select **besfndcentos** from the filtered list of computers.
9. In the **Expires** section, select the **Never** option.

   Hint: You can specify an expiration date by selecting the blank option that shows in the Expires section. As you begin to enter a date in the text field, a calendar opens so that you can pick the expiration date.

10. Click **Create**.



Reason	Checklist / Checks	Group / Computers	Expiration Date	Last edit by	Status

Create Exception

Reason*: Non-standard permissions on the bootloader config are required to support legacy applications.

Affected Checks: ○ All checks in checklist ● Selected checks

Checks*: Ensure permissions on bootloader config are configured (Lab CentOS7 File Permissions)

Affected Computers: ○ All computers in group ● Selected computers

Computers*: BESFNDCENTOS

Expires: ○ ● Never

The exceptions is created and is listed on the Exceptions page. An import must be performed before the exception becomes active.

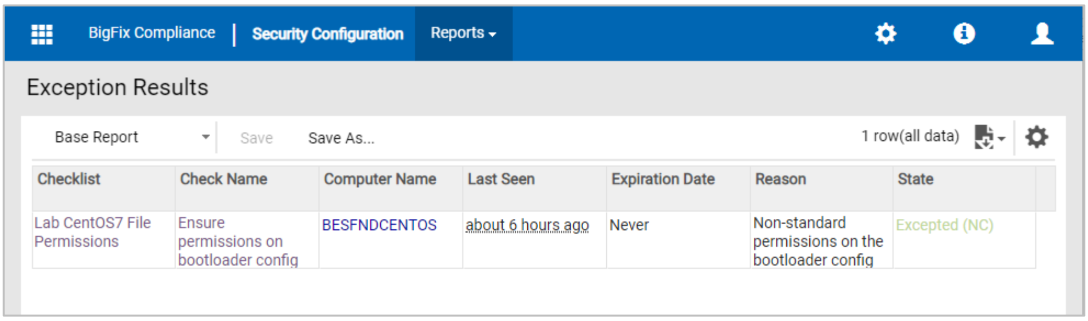
11. Perform an ad-hoc Data Import. Refer to **Exercise 7 – Import the Checklists into the Analytics Server** if you must refresh your memory on how to perform the Import.
12. Wait until the import successfully completes before continuing to the next exercise.

You have now successfully completed Exercise 18.

Exercise 19 – Viewing the Exception Results report

In this exercise, you view the Exception Results report. You also view the checklist overview report to observe how creating the exception is reflected in the overall compliance.

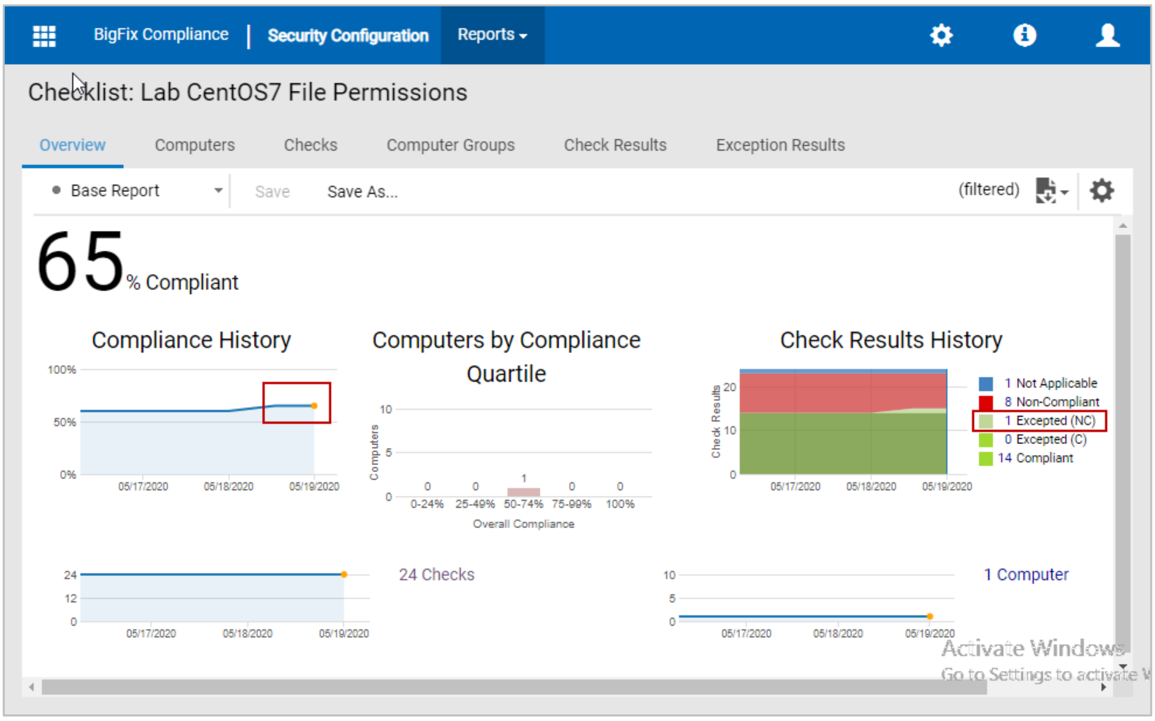
1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **exceptions_admin** with a password of **B1gfixrocks!**.
2. Select **Exceptions Results** from the **Reports** menu at the top of the page. The Exceptions Results report is displayed.



Checklist	Check Name	Computer Name	Last Seen	Expiration Date	Reason	State
Lab CentOS7 File Permissions	Ensure permissions on bootloader config	BESFNDCENTOS	about 6 hours ago	Never	Non-standard permissions on the bootloader config	Excepted (NC)

3. Click the **Lab CentOS7 File Permissions** link in the Checklist column. The Checklist Overview report opens.

4. Review the Overview report and observe that the **Compliance History** section shows that the overall compliance increased as a result of the exception. In addition, you observe that the **Check Results History** section now shows the exception as **1 Excepted (NC)**.



Hint: Exceptions are classified with one of the following types:

- Excepted (NC) – A check is non-compliant but excepted through a manually created exception.
- Excepted (C) - A check is compliant but excepted through a manually created exception.

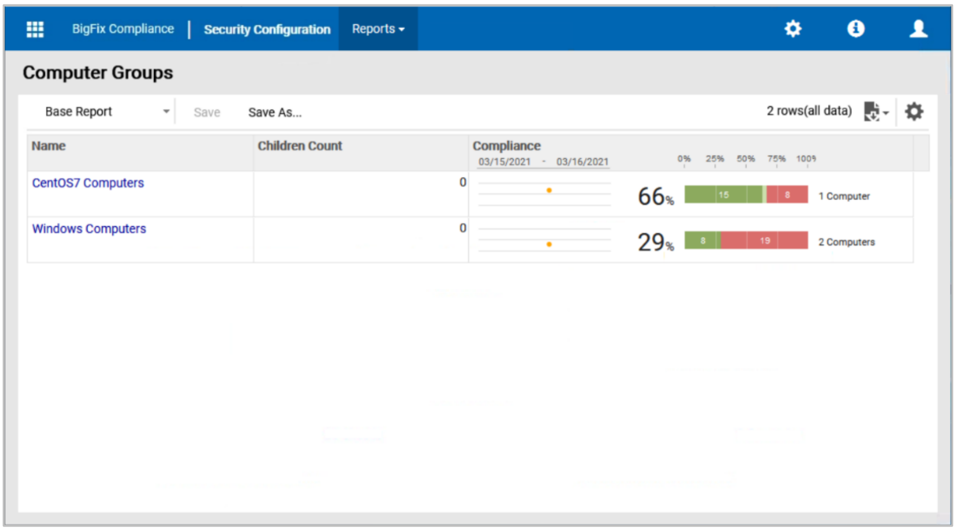
You have now completed Exercise 19.

Exercise 20 – Using Computer Groups and Computer Properties

In this exercise, you explore the Computer Groups report and use the Computer Properties that were created in the previous exercises for reporting and filtering.

1. Return to the Compliance Analytics web interface. If the session has timed out, login again as **exceptions_admin** with a password of **B1gfixrocks!**.

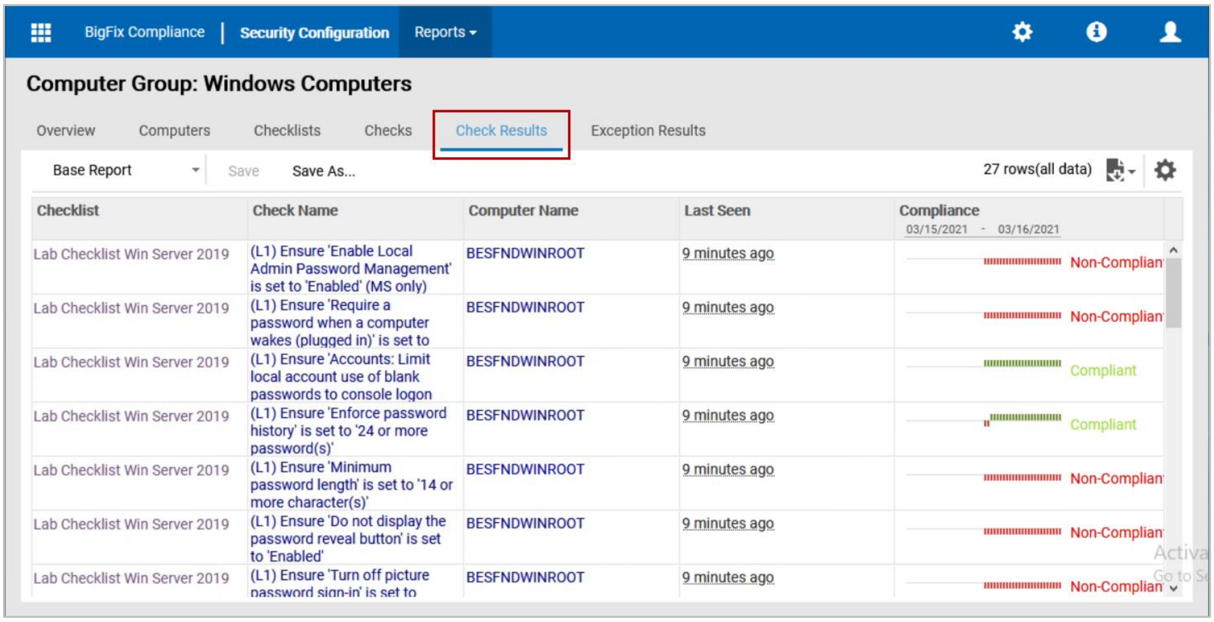
2. Select **Computer Groups** from the **Reports** menu at the top of the page. The Computer Groups report is displayed.



Computer Groups

Name	Children Count	Compliance 03/15/2021 - 03/16/2021	
CentOS7 Computers	0	66% 15 8	1 Computer
Windows Computers	0	29% 8 19	2 Computers

3. Click the **Windows Computers** link in the **Name** column. The Computer Group: Windows Computers report opens.
4. Click the **Check Results** tab located at the top of the **Windows Computers** report page. The Check Results page opens and shows the results of the configuration checks for every computer that is associated with the Windows Computers Group.

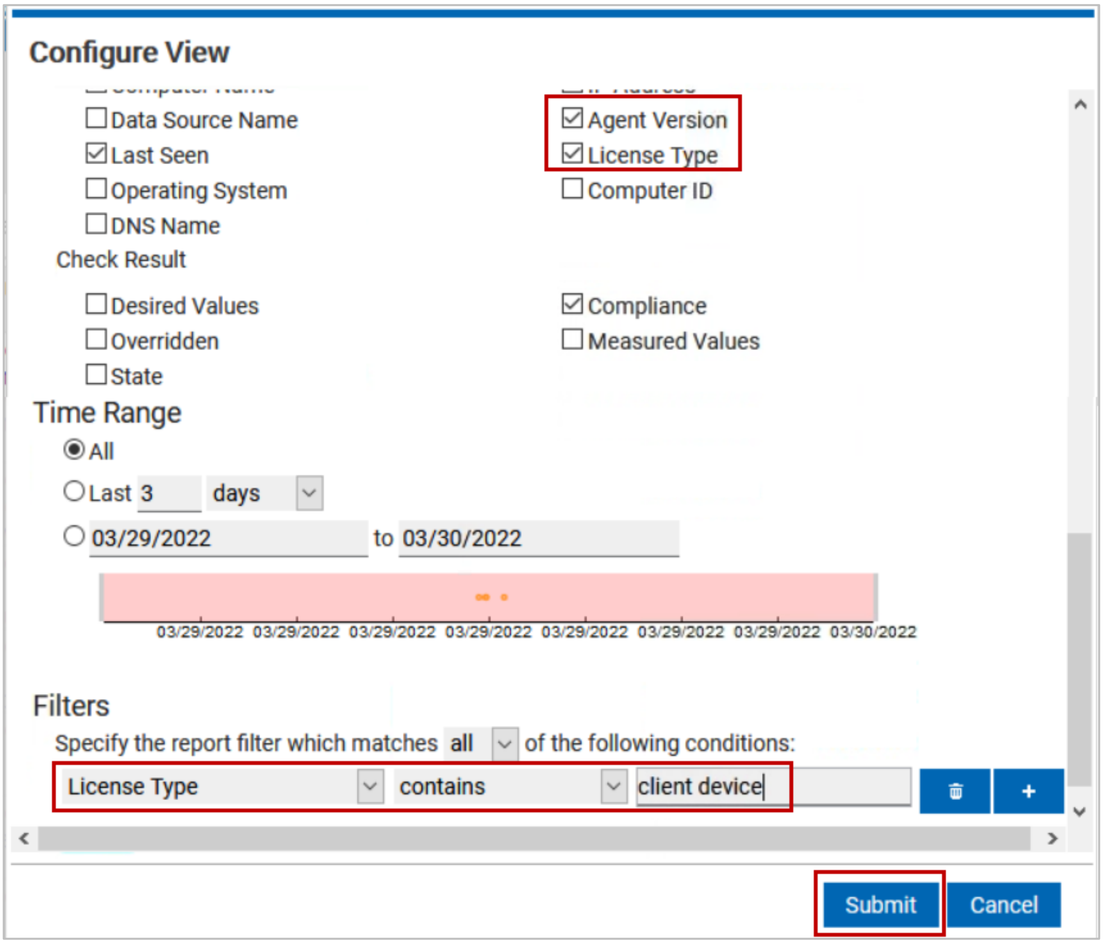


Computer Group: Windows Computers

Checklist	Check Name	Computer Name	Last Seen	Compliance 03/15/2021 - 03/16/2021
Lab Checklist Win Server 2019	(L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)	BESFNDWINROOT	9 minutes ago	Non-Complian
Lab Checklist Win Server 2019	(L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to	BESFNDWINROOT	9 minutes ago	Non-Complian
Lab Checklist Win Server 2019	(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon	BESFNDWINROOT	9 minutes ago	Compliant
Lab Checklist Win Server 2019	(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	BESFNDWINROOT	9 minutes ago	Compliant
Lab Checklist Win Server 2019	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	BESFNDWINROOT	9 minutes ago	Non-Complian
Lab Checklist Win Server 2019	(L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	BESFNDWINROOT	9 minutes ago	Non-Complian
Lab Checklist Win Server 2019	(L1) Ensure 'Turn off picture password sign-in' is set to	BESFNDWINROOT	9 minutes ago	Non-Complian

5. Click the **Gear** icon that is located just above the **Compliance** column header in the **Windows Computers** report. The Configure View window opens.
6. Scroll down to the **Computer** section in the **Configure View** window. Place a check beside the **Agent Version** and **License Type** checkboxes. These items represent the custom Computer Properties that were created in a previous exercise.
7. Scroll down to the **Filters** section of the **Configure View** window. Click the plus **(+)** to add a report filter.

8. Define the filter using the following information;
    - Select **License Type** from the first drop-down box.
    - Select **contains** from the second drop-down box.
    - Enter the string **client device** in the text field



Configure View

□ Data Source Name	☑ Agent Version
☑ Last Seen	☑ License Type
□ Operating System	□ Computer ID
□ DNS Name	

Check Result

□ Desired Values	☑ Compliance
□ Overridden	□ Measured Values
□ State	

Time Range

● All

○ Last 3 days

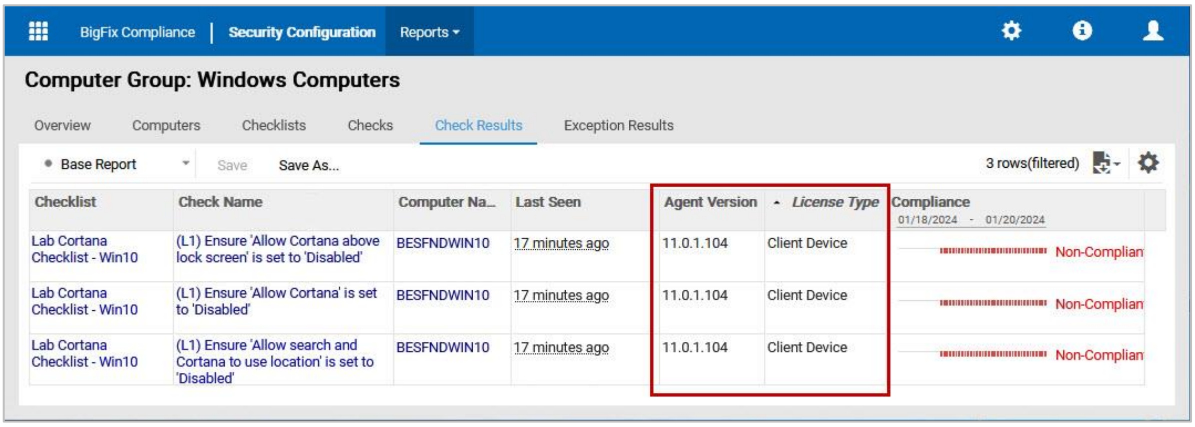
○ 03/29/2022 to 03/30/2022

Filters

Specify the report filter which matches all of the following conditions:

License Type | contains | client device

9. Click **Submit**. The report is updated to display the **Agent Version** and **License Type** columns and the filter has been applied so the report only shows the check results for the Windows 10 systems based on the Workstation License Type.

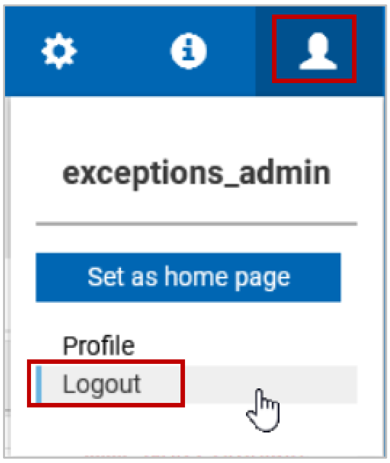


Computer Group: Windows Computers

3 rows(filtered)

Checklist	Check Name	Computer Na...	Last Seen	Agent Version	License Type	Compliance 01/18/2024 - 01/20/2024
Lab Cortana Checklist - Win10	(L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	BESFNDWIN10	17 minutes ago	11.0.1.104	Client Device	Non-Complian
Lab Cortana Checklist - Win10	(L1) Ensure 'Allow Cortana' is set to 'Disabled'	BESFNDWIN10	17 minutes ago	11.0.1.104	Client Device	Non-Complian
Lab Cortana Checklist - Win10	(L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled'	BESFNDWIN10	17 minutes ago	11.0.1.104	Client Device	Non-Complian

10. Select the **User** icon in the upper-right portion of the page, then select **Logout**.



exceptions_admin

You are returned to the SCA login page.

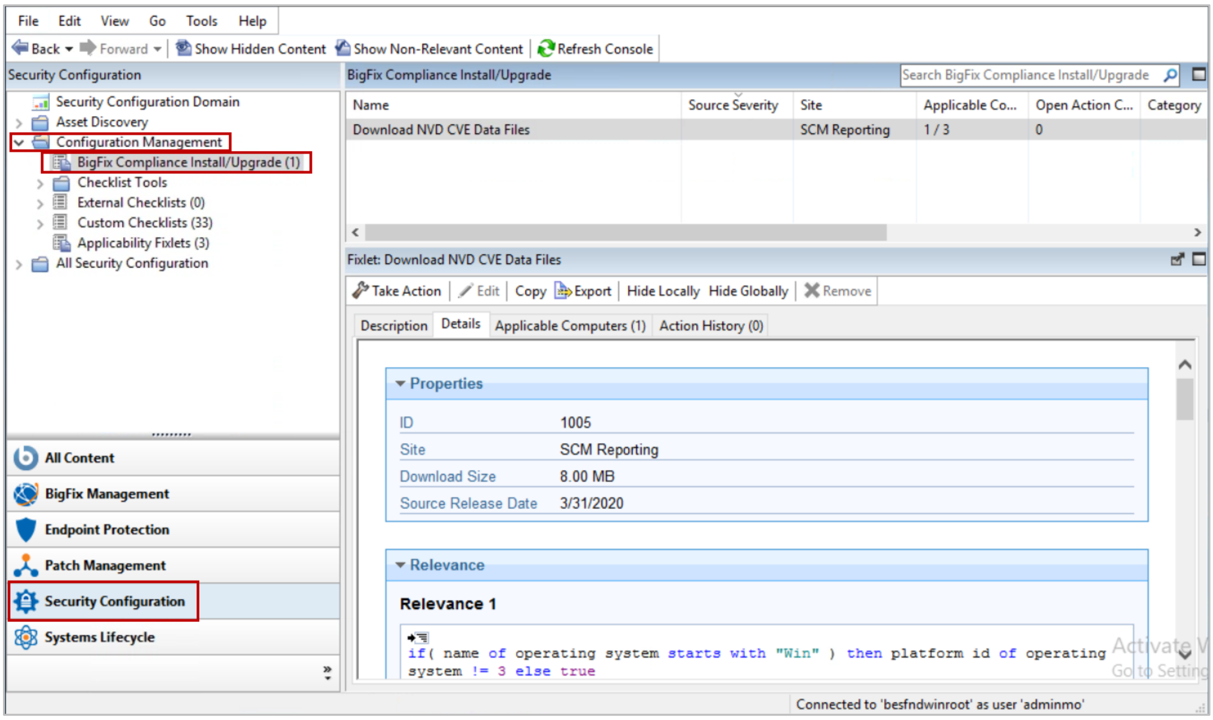
You have now completed Exercise 20.

Exercise 21 – Enabling Patch and Vulnerabilities Reporting

In this exercise, you download the National Vulnerability Database data and enable the Patch and Vulnerability report domains.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens.
4. Select the **Security Configuration** domain in the lower-left portion of the **Console**. The Navigation pane updates to show Security Configuration.

5. In the **Navigation pane**, expand the **Configuration Management** node and select **BigFix Compliance Install/Upgrade**. A list of Fixlets and Tasks is displayed in the List Area in the upper-right portion of the Console.


File Edit View Go Tools Help
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
Security Configuration
Security Configuration Domain
Asset Discovery
Configuration Management
BigFix Compliance Install/Upgrade (1)
Checklist Tools
External Checklists (0)
Custom Checklists (33)
Applicability Fixlets (3)
All Security Configuration
All Content
BigFix Management
Endpoint Protection
Patch Management
Security Configuration
Systems Lifecycle
BigFix Compliance Install/Upgrade
Search BigFix Compliance Install/Upgrade
Fixlet: Download NVD CVE Data Files
Take Action Edit Copy Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (1) Action History (0)
Properties
Relevance
Relevance 1
Activate W
Go to Setting

Name	Source Severity	Site	Applicable Co...	Open Action C...	Category
Download NVD CVE Data Files		SCM Reporting	1 / 3	0	

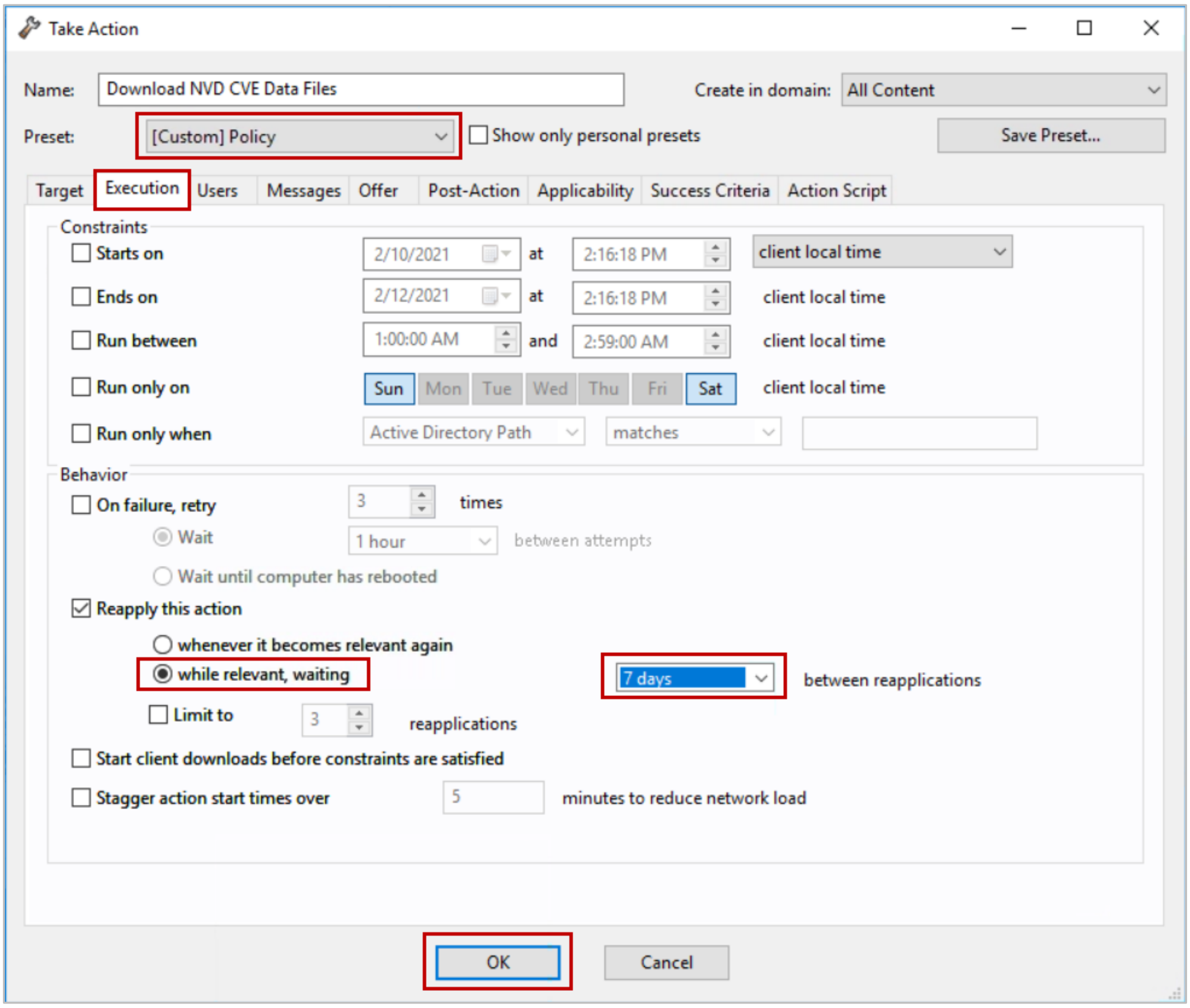
ID 1005
Site SCM Reporting
Download Size 8.00 MB
Source Release Date 3/31/2020

```
if( name of operating system starts with "Win" ) then platform id of operating
system != 3 else true
```

Connected to 'besfndwinroot' as user 'adminmo'

6. Select the **Download NVD CVE Data Files** Fixlet in the List area. The details for the select Fixlet are displayed in the Work area below.
7. Click the **Description** tab and review the description for the selected Fixlet.
8. Click **Take Action**. The Take Action window opens.
9. Click the **Target** tab. Verify that the Select devices option is select and then select the **BESFNDWINROOT** computer from the list of available targets.
10. Click the **Execution** tab.
11. Select **Policy** from the **Preset** drop-down box at the top of the **Take Action** window. The execution parameters are modified to allow this action to stay open until it is manually stopped by an operator.

12. In the **Behavior** section of the **Execution** tab, select the **while relevant, waiting** option then select **7 days** from the between reapplications drop-down box.



Name: Download NVD CVE Data Files

Create in domain: All Content

Preset: [Custom] Policy

□ Show only personal presets

Constraints

□ Starts on 2/10/2021 at 2:16:18 PM client local time

□ Ends on 2/12/2021 at 2:16:18 PM client local time

□ Run between 1:00:00 AM and 2:59:00 AM client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time

□ Run only when Active Directory Path matches

Behavior

□ On failure, retry 3 times

○ Wait 1 hour between attempts

○ Wait until computer has rebooted

☑ Reapply this action

○ whenever it becomes relevant again

● while relevant, waiting 7 days between reapplications

□ Limit to 3 reapplications

□ Start client downloads before constraints are satisfied

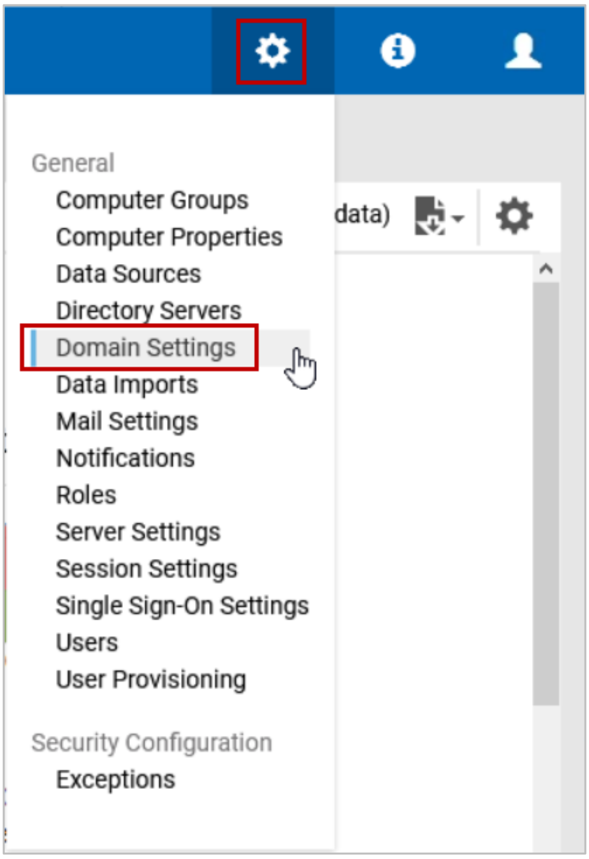
□ Stagger action start times over 5 minutes to reduce network load

13. Click **OK**. The Action pane opens.
14. Monitor the status of the action until it changes to **Fixed**.
15. Minimize the **Console**.
16. Double click the **Firefox** icon on the desktop if it is not already open. The browser opens.
17. Enter the following URL in the address section of the browser:
    https://BESFNDWINROOT:9085

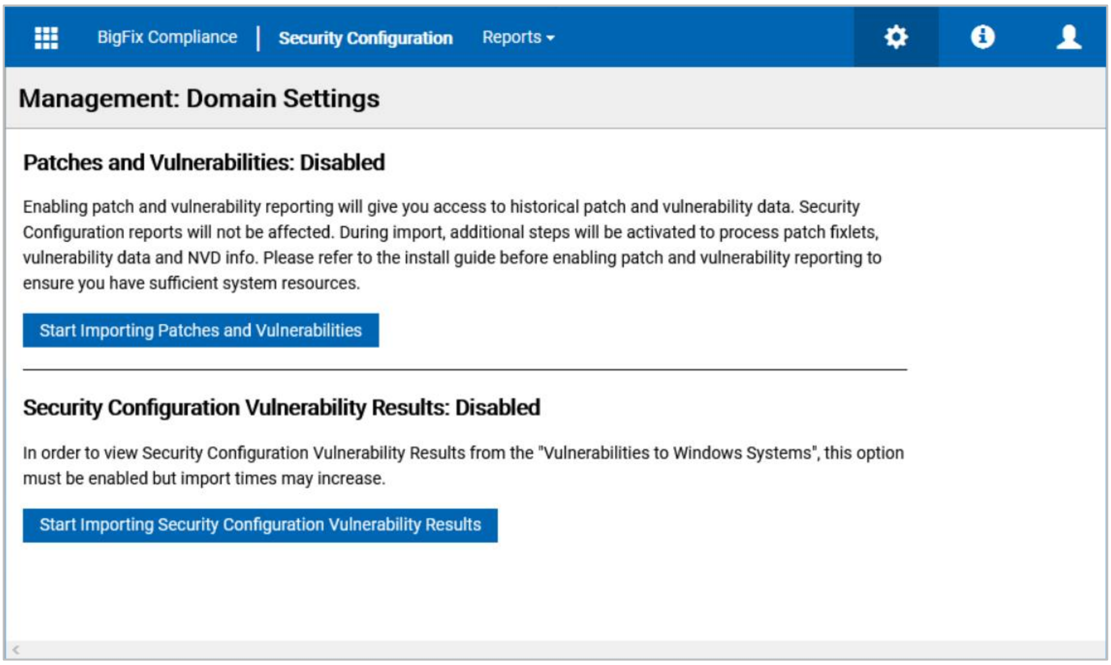
    Note: You might receive a security warning indicating that it is unsafe to continue to the page. Click the Advanced option, accept the risk and continue to the site.

    The BigFix Compliance login page opens.
18. Enter **adminmo** as the username with a password of **B1gfixrocks!**. Click **Login**. The Overview page opens.

19. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



20. Select **Domain Settings** from the Management menu. The Domain Settings page opens.



Management: Domain Settings

Patches and Vulnerabilities: Disabled

Enabling patch and vulnerability reporting will give you access to historical patch and vulnerability data. Security Configuration reports will not be affected. During import, additional steps will be activated to process patch fixlets, vulnerability data and NVD info. Please refer to the install guide before enabling patch and vulnerability reporting to ensure you have sufficient system resources.

Security Configuration Vulnerability Results: Disabled

In order to view Security Configuration Vulnerability Results from the "Vulnerabilities to Windows Systems", this option must be enabled but import times may increase.

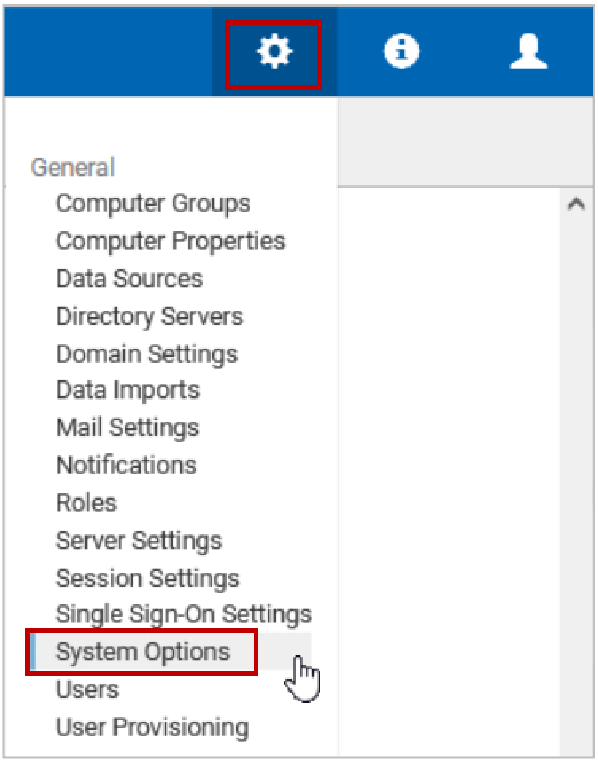
Start Importing Security Configuration Vulnerability Results

21. Click **Start Importing Patches and Vulnerabilities**. The Confirm Changes window opens.
22. Click **Yes, include** in the Confirm Changes window. The Confirm Changes window closes.

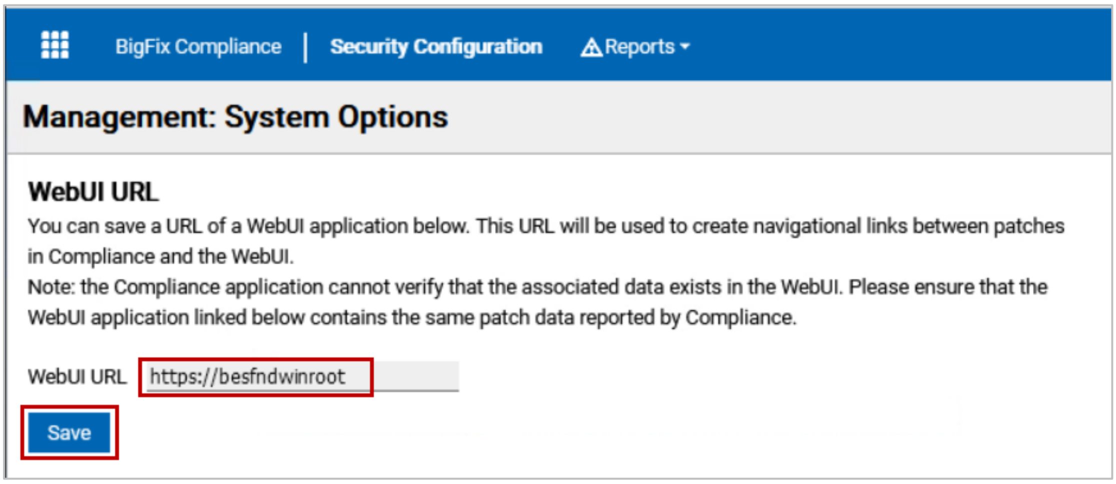
23. Click **Start Importing Security Configuration Vulnerability Results**. The Confirm Changes window opens.
24. Click **Yes, include** in the Confirm Changes window. The Confirm Changes window closes.

    Note: A Data Import must now be performed to import the Patch and Vulnerability Results that you just enabled.

25. Click the **gear** icon in the upper-right portion of the BigFix Compliance header. The **Management** menu opens.



26. Select **System Options** from the Management menu. The System Options page opens.
27. In the **WebUI URL** field enter the WebUI address as follows: https://besfndwinroot
28. Click **Save**. The WebUI address is saved.



Management: System Options

WebUI URL

You can save a URL of a WebUI application below. This URL will be used to create navigational links between patches in Compliance and the WebUI.

Note: the Compliance application cannot verify that the associated data exists in the WebUI. Please ensure that the WebUI application linked below contains the same patch data reported by Compliance.

WebUI URL https://besfndwinroot

29. Perform an ad-hoc **Data Import**. Refer to **Exercise 7 – Import the Checklists into the Analytics Server** if you must refresh your memory on how to perform the Import.

    Important: The initial Data Import that is performed after enabling the Patch and Vulnerability Results might take several hours to complete. Let it continue to run in the background. If time permits, you can perform the optional exercise at the end of the course to review the Patch and Vulnerability reports.

You have now completed Exercise 21.

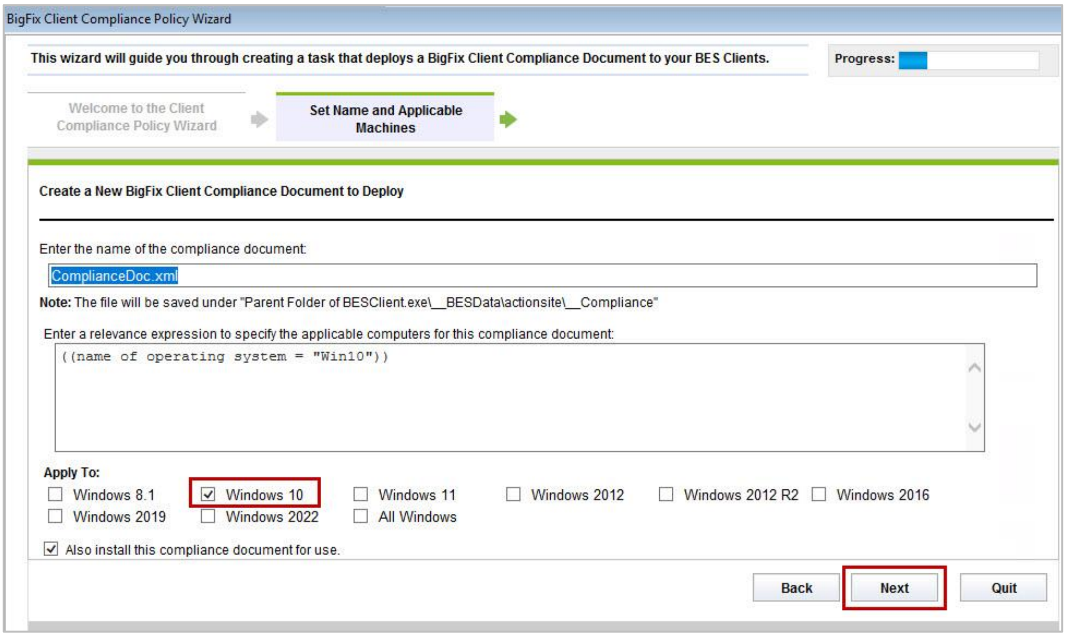
Exercise 22 - Create and Deploy a Client Compliance Document

In this exercise, you use the BigFix Client Compliance Policy Wizard to develop a Client Compliance Document and setup a policy to deploy it.

Note: A recent change to the BES Support content has created an issue with the Task that is generated by the BigFix Client Compliance Policy Wizard. As a temporary work around for the purpose of the lab, a custom Task has been provided so that you are able to successfully complete the exercise.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. If the Console is not already open, double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens.
4. Click **Endpoint Protection** in the lower-left portion of the Console. The navigation pane updates to show the BigFix Content that pertains to Endpoint Protection.
5. In the navigation pane, expand the **Network Self-Quarantine > Create Compliance Policies** nodes, then select the **Client Compliance Policy Wizard**. The BigFix Client Compliance Policy Wizard opens.
6. Select the **Create a new BigFix Client Compliance Document to Deploy** option in the wizard then click **Next**.

7. Select the **checkbox** beside the **Windows 10** option in the **Apply To:** section of the wizard, then click **Next**.



BigFix Client Compliance Policy Wizard

This wizard will guide you through creating a task that deploys a BigFix Client Compliance Document to your BES Clients.

Progress:

Welcome to the Client Compliance Policy Wizard → Set Name and Applicable Machines →

Create a New BigFix Client Compliance Document to Deploy

Enter the name of the compliance document: ComplianceDoc.xml

Note: The file will be saved under "Parent Folder of BESClient.exe__BESData\actionsite__Compliance"

Enter a relevance expression to specify the applicable computers for this compliance document:

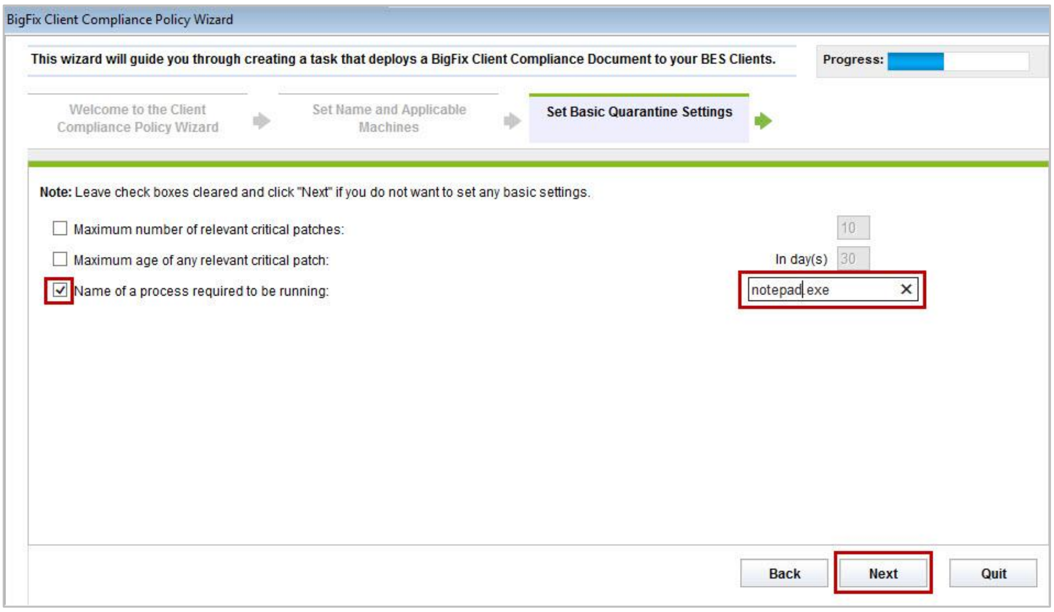
```
((name of operating system = "Win10"))
```

Apply To:

☐ Windows 8.1 ☑ Windows 10 ☐ Windows 11 ☐ Windows 2012 ☐ Windows 2012 R2 ☐ Windows 2016
☐ Windows 2019 ☐ Windows 2022 ☐ All Windows

☑ Also install this compliance document for use.

8. Select the **checkbox** beside **Name of a process required to be running** and enter **notepad.exe** in the text box. Click **Next**.



BigFix Client Compliance Policy Wizard

This wizard will guide you through creating a task that deploys a BigFix Client Compliance Document to your BES Clients.

Progress:

Welcome to the Client Compliance Policy Wizard → Set Name and Applicable Machines → Set Basic Quarantine Settings →

Note: Leave check boxes cleared and click "Next" if you do not want to set any basic settings.

☐ Maximum number of relevant critical patches: 10

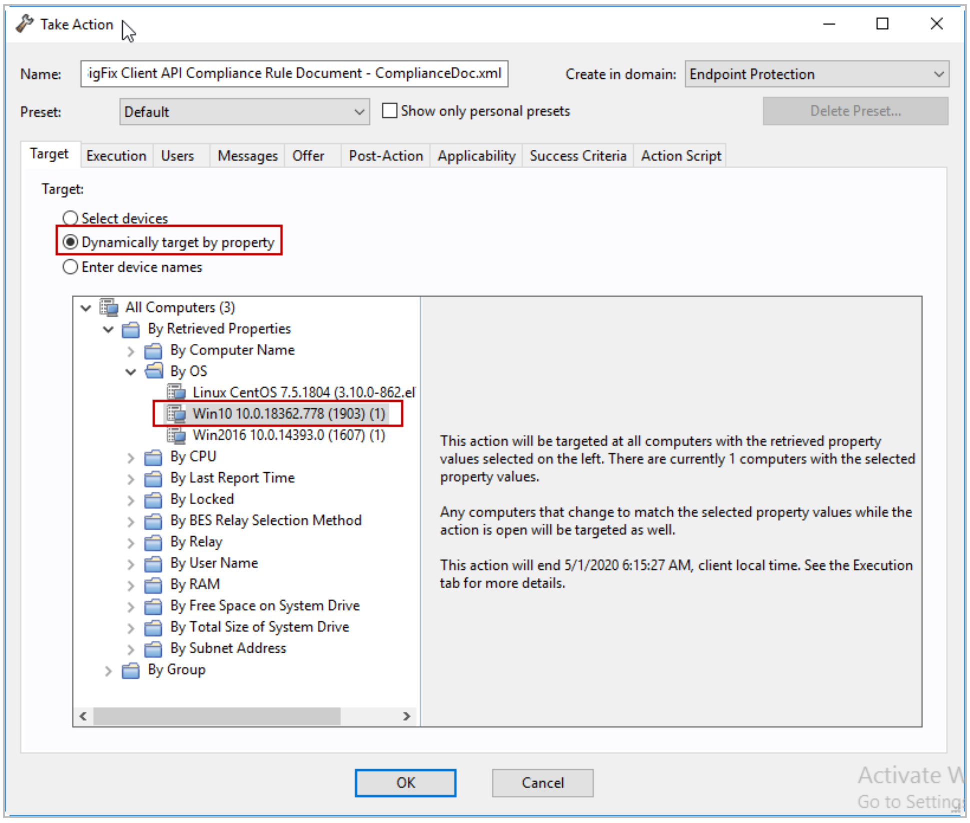
☐ Maximum age of any relevant critical patch: In day(s) 30

☑ Name of a process required to be running: notepad.exe

9. Click **Next** to accept the default Anti-Virus Quarantine Settings.
10. Click **Finish**. The Create Task window opens. If you receive a Security Warning message, click Continue.
11. Click **OK**. The Task is created in the Master Action Site.
12. Click **Compliance Policies** in the navigation pane. Locate the **Create and Deploy BigFix Client API Compliance Rule Document – ComplianceDoc.xml** Task. Click **Take Action**. The Take Action window opens.

Tip: You might have to wait a few minutes for the Task to be evaluated and become Relevant for it to be visible unless the Show Non-Relevant Content button is toggled on.

13. Select the **Target** tab if it is not already selected and set the following options:
    - Select the **Dynamically target by property** option
    - Expand the **All Computers > By Retrieved Properties > By OS** nodes, then select the **Win10** node.



Take Action

Name: igFix Client API Compliance Rule Document - ComplianceDoc.xml

Create in domain: Endpoint Protection

Preset: Default

□ Show only personal presets

Target:

○ Select devices

● Dynamically target by property

○ Enter device names

- All Computers (3)
  - By Retrieved Properties
    - By Computer Name
    - By OS
      - Linux CentOS 7.5.1804 (3.10.0-862.el
      - Win10 10.0.18362.778 (1903) (1)
      - Win2016 10.0.14393.0 (1607) (1)
    - By CPU
    - By Last Report Time
    - By Locked
    - By BES Relay Selection Method
    - By Relay
    - By User Name
    - By RAM
    - By Free Space on System Drive
    - By Total Size of System Drive
    - By Subnet Address
  - By Group

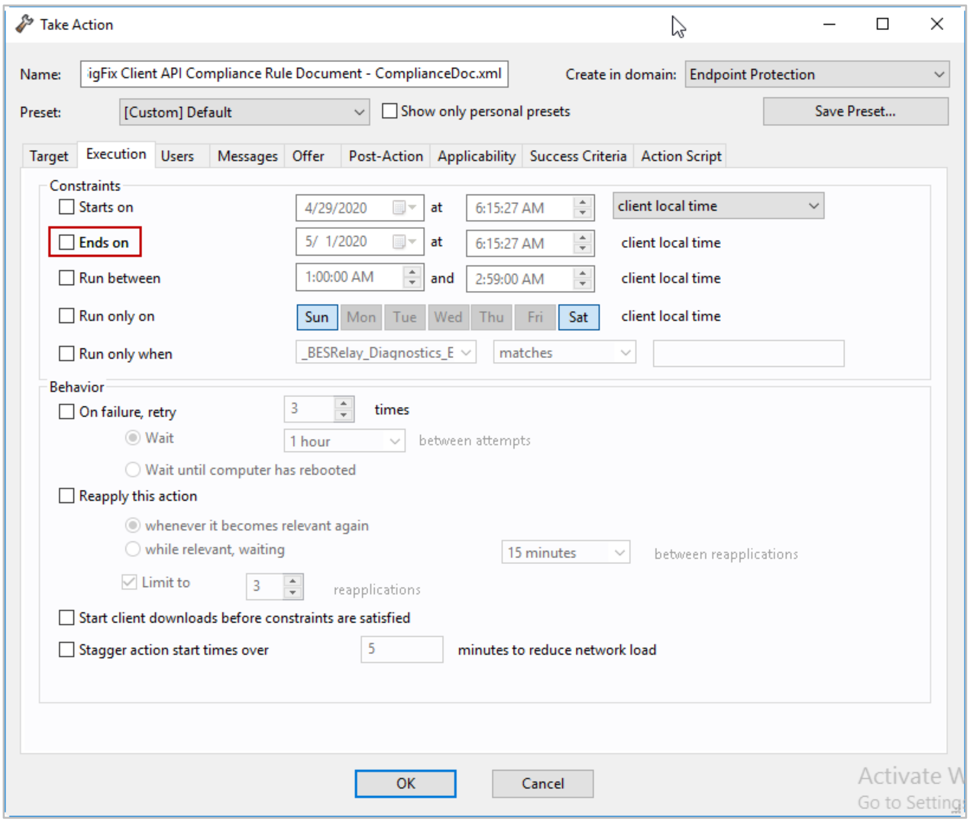
This action will be targeted at all computers with the retrieved property values selected on the left. There are currently 1 computers with the selected property values.

Any computers that change to match the selected property values while the action is open will be targeted as well.

This action will end 5/1/2020 6:15:27 AM, client local time. See the Execution tab for more details.

14. Select the **Execution** tab.

15. Uncheck the **Ends On** option.



Take Action

Name: igFix Client API Compliance Rule Document - ComplianceDoc.xml

Create in domain: Endpoint Protection

Preset: [Custom] Default

□ Show only personal presets

Save Preset...

Target | Execution | Users | Messages | Offer | Post-Action | Applicability | Success Criteria | Action Script

Constraints

□ Starts on 4/29/2020 at 6:15:27 AM client local time

□ Ends on 5/ 1/2020 at 6:15:27 AM client local time

□ Run between 1:00:00 AM and 2:59:00 AM client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time

□ Run only when _BESRelay_Diagnostics_E matches

Behavior

□ On failure, retry 3 times

● Wait 1 hour between attempts

○ Wait until computer has rebooted

□ Reapply this action

● whenever it becomes relevant again

○ while relevant, waiting 15 minutes between reapplications

☑ Limit to 3 reapplications

□ Start client downloads before constraints are satisfied

□ Stagger action start times over 5 minutes to reduce network load

OK Cancel

16. Review the other tabs in the **Take Action** window but do not change any settings.
17. Select the **Target** tab. Verify that the **Win10** systems are targeted.
18. Click **OK** to initiate the action.

You have successfully completed Exercise 22.

Exercise 23 - Deploy Assessment and Quarantine Policy

In this exercise, you leverage the BigFix Client Compliance (IPSec Framework) content to assess an endpoints compliance with the Compliance Document that was deployed in the previous exercise. You also Quarantine the endpoint if it is out of compliance.

The **Quarantine - Determine Compliance** Fixlet evaluates the compliance of the endpoints with the Client Compliance Document and records the results to the registry. The actions taken on the **Quarantine – Quarantine Needed** Fixlet creates firewall rules to quarantine the endpoint by only allowing communication on port 52311 if the endpoint is flagged as non-compliant.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. If the Console is not already open, double click the **BigFix Console** icon on the desktop. The login screen opens.
3. Verify that the user name is set to **adminmo** and enter the password **B1gfixrocks**. Click **Login**. The Console opens.
4. Verify that the **BESFNDWIN10** endpoint is not in a **Pending Restart** state by performing the following steps;

a) Select the **All Content** domain in the lower-left portion of the Console. The Navigation pane updates to show All Content.

b) Click the **Fixlets and Tasks** node. A list of Fixlets and Tasks are shown in the List pane.

c) Enter the string **restart needed** in the live search field in the upper-right portion of the Console. The list of Fixlets and Tasks is filtered to show only those that match this string.

d) Select the **Restart Needed** Fixlet. The details of the selected Fixlet are shown in the work area below.

   Hint: You might have to click the Show Non-Relevant Content button at the top of the Console for the Fixlet to be displayed.

e) Click the **Applicable Computers** tab in the work area and verify that the **BESFNDWIN10** computer is **NOT** listed.

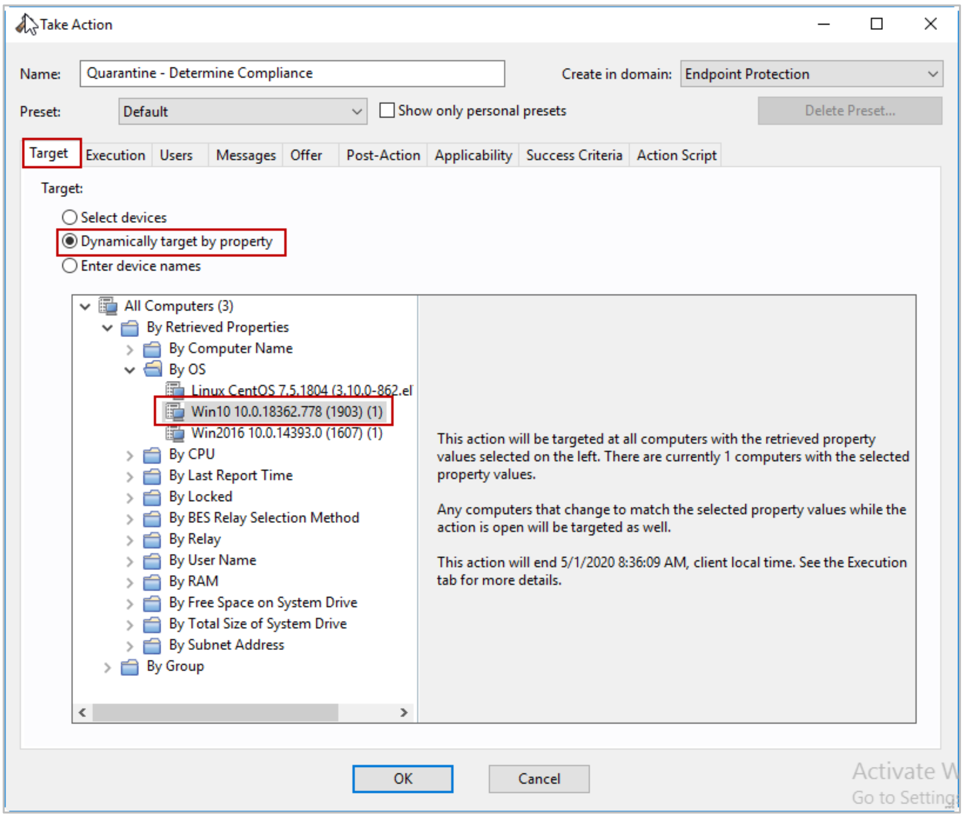
f) If **BESFNDWIN10** is listed on the **Applicable Computers** tab, please restart the **BESFNDWIN10** computer until it no longer is listed on the **Applicable Computers** tab of the **Restart Needed** Fixlet before continuing to the next step.

5. Click **Endpoint Protection** in the lower-left portion of the Console. The navigation pane updates to show the BigFix Content that pertains to Endpoint Protection.
6. In the navigation pane, expand **Network Self-Quarantine -> Computer Status -> Analysis**
7. Select any Analyses that are currently in **Not Activated** status. **Right-click** and select **Activate** from the Context menu.

   Hint: You might have to toggle on the Show Non-Relevant Content button at the top of the Console so that you can verify that status of all Analyses. You can toggle it off again after activating the Analyses.

8. Click **All Content** in the lower-left portion of the Console. The navigation pane updates to show all the BigFix Content.
9. In the navigation pane, expand the **Sites > External Sites > BigFix Client Compliance (IPSec Framework)** nodes, then select the **Fixlets and Tasks**. A list of Fixlets and Tasks is displayed in the list area in the upper-right portion of the Console
10. Select the **Quarantine – Determine Compliance** Fixlet in the list area. The details for the selected Fixlet are shown in the work area below.
11. Click **Take Action**, then select **Click here to evaluate compliance**. The Take Action window opens.

12. Select the **Target** tab if it is not already selected and set the following options:
    a) Select the **Dynamically target by property** option
    b) Expand the **All Computers > By Retrieved Properties > By OS** nodes, then select the **Win10** node.



Take Action

Name: Quarantine - Determine Compliance

Create in domain: Endpoint Protection

Preset: Default

☐ Show only personal presets

Target:

○ Select devices

● Dynamically target by property

○ Enter device names

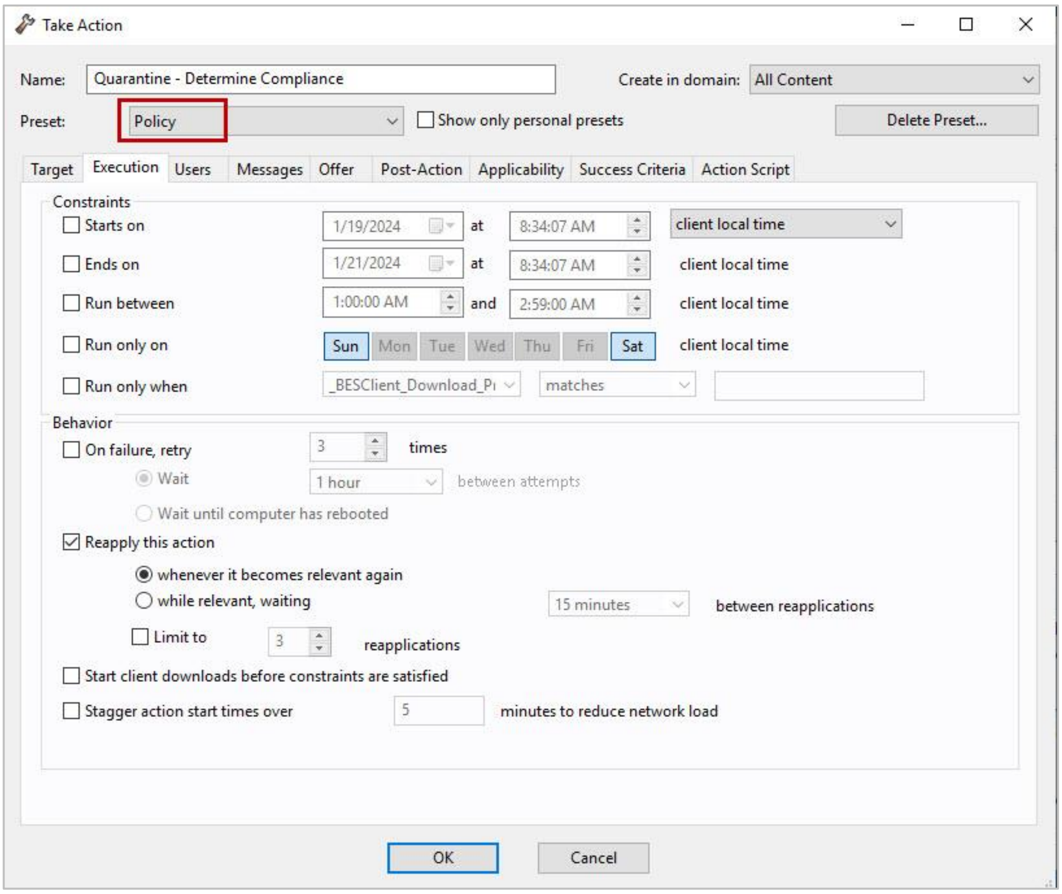
All Computers (3)
By Retrieved Properties
By Computer Name
By OS
Linux CentOS 7.5.1804 (3.10.0-862.el
Win10 10.0.18362.778 (1903) (1)
Win2016 10.0.14393.0 (1607) (1)
By CPU
By Last Report Time
By Locked
By BES Relay Selection Method
By Relay
By User Name
By RAM
By Free Space on System Drive
By Total Size of System Drive
By Subnet Address
By Group

This action will be targeted at all computers with the retrieved property values selected on the left. There are currently 1 computers with the selected property values.

Any computers that change to match the selected property values while the action is open will be targeted as well.

This action will end 5/1/2020 8:36:09 AM, client local time. See the Execution tab for more details.

13. Select the **Execution** tab, then select **Policy** from the **Preset** dropdown box.



Take Action

Name: Quarantine - Determine Compliance

Create in domain: All Content

Preset: Policy

□ Show only personal presets

Constraints

□ Starts on 1/19/2024 at 8:34:07 AM client local time

□ Ends on 1/21/2024 at 8:34:07 AM client local time

□ Run between 1:00:00 AM and 2:59:00 AM client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time

□ Run only when _BESClient_Download_Pı matches

Behavior

□ On failure, retry 3 times

○ Wait 1 hour between attempts

○ Wait until computer has rebooted

☑ Reapply this action

● whenever it becomes relevant again

○ while relevant, waiting 15 minutes between reapplications

□ Limit to 3 reapplications

□ Start client downloads before constraints are satisfied

□ Stagger action start times over 5 minutes to reduce network load

14. Review the other tabs in the **Take Action** window but do not change any settings.
15. Select the **Target** tab. Verify that the **Win10** systems are targeted.
16. Click **OK** to initiate the action.
17. Monitor the status of the action and wait for it to change to **Fixed** before continuing.

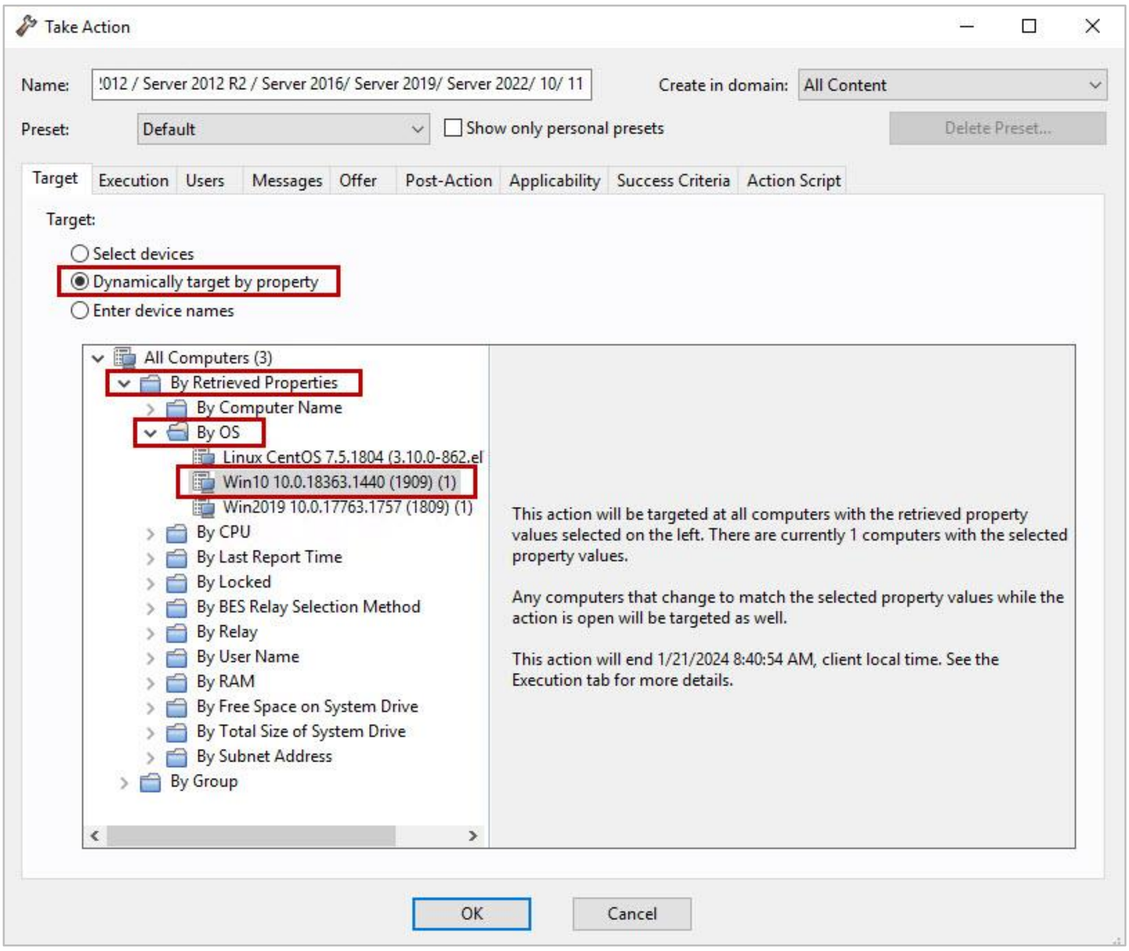
You have now successfully deployed the Compliance Assessment Policy. In the next section, you setup Policy Actions to automatically Quarantine non-compliant systems and Un-Quarantine previously Quarantined systems that are now compliant.

18. Click **All Content** in the lower-left portion of the Console. The navigation pane updates to show all the BigFix Content.
19. In the navigation pane, expand the **Sites > External Sites > BigFix Client Compliance (IPSec Framework)** nodes, then select the **Fixlets and Tasks** node. A list of Fixlets and Tasks is displayed in the list area in the upper-right portion of the Console.
20. Select the **Quarantine – Quarantine No Longer Needed – Windows 8.1 / Sever 2012 / Server 2012 R2 / Server 2016 / Server 2019 / Server 2022 / 10 / 11** Fixlet from the list pane. The details for the Fixlet are shown in the work area below.

    Hint: If the out of compliance condition has not been determined by the client, you might have to click **Show Non-Relevant Content** at the top of the Console to see the Fixlet.

21. Click **Take Action**, then select **Click here to remove client computers from quarantine**. The Take Action window opens.

22. Select the **Target** tab if it is not already selected and set the following options:
    - Select the **Dynamically target by property** option
    - Expand the **All Computers > By Retrieved Properties > By OS** nodes, then select the **Win10** node.



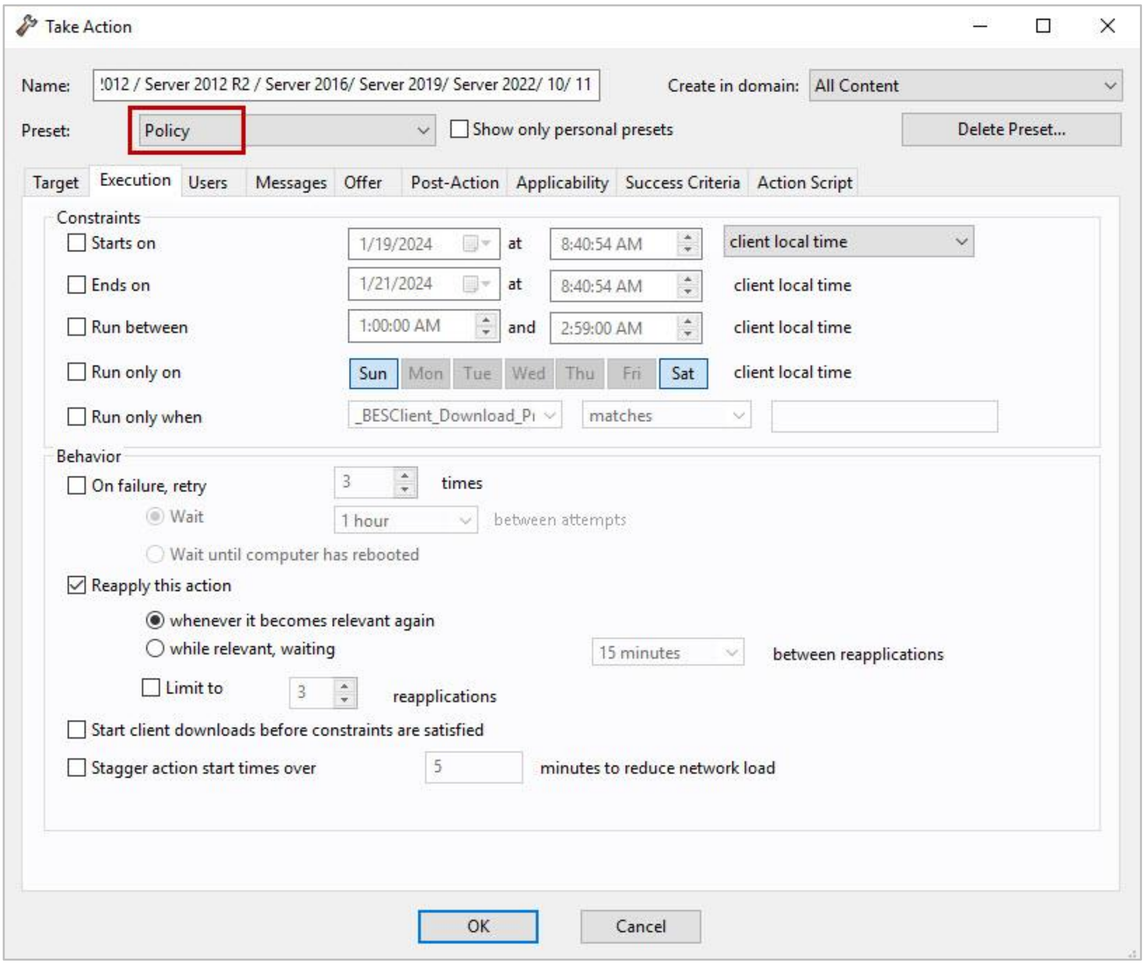
Take Action
Name: !012 / Server 2012 R2 / Server 2016/ Server 2019/ Server 2022/ 10/ 11
Create in domain: All Content
Preset: Default
□ Show only personal presets
Delete Preset...
Target
Execution
Users
Messages
Offer
Post-Action
Applicability
Success Criteria
Action Script
Target:
○ Select devices
● Dynamically target by property
○ Enter device names
All Computers (3)
By Retrieved Properties
By Computer Name
By OS
Linux CentOS 7.5.1804 (3.10.0-862.el
Win10 10.0.18363.1440 (1909) (1)
Win2019 10.0.17763.1757 (1809) (1)
By CPU
By Last Report Time
By Locked
By BES Relay Selection Method
By Relay
By User Name
By RAM
By Free Space on System Drive
By Total Size of System Drive
By Subnet Address
By Group
OK
Cancel

This action will be targeted at all computers with the retrieved property values selected on the left. There are currently 1 computers with the selected property values.

Any computers that change to match the selected property values while the action is open will be targeted as well.

This action will end 1/21/2024 8:40:54 AM, client local time. See the Execution tab for more details.

23. Select the **Execution** tab, then select **Policy** from the **Preset** dropdown box.



Name: !012 / Server 2012 R2 / Server 2016/ Server 2019/ Server 2022/ 10/ 11

Create in domain: All Content

Preset: Policy

□ Show only personal presets

Constraints

□ Starts on 1/19/2024 at 8:40:54 AM client local time

□ Ends on 1/21/2024 at 8:40:54 AM client local time

□ Run between 1:00:00 AM and 2:59:00 AM client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time

□ Run only when _BESClient_Download_Pı matches

Behavior

□ On failure, retry 3 times

○ Wait 1 hour between attempts

○ Wait until computer has rebooted

☑ Reapply this action

● whenever it becomes relevant again

○ while relevant, waiting 15 minutes between reapplications

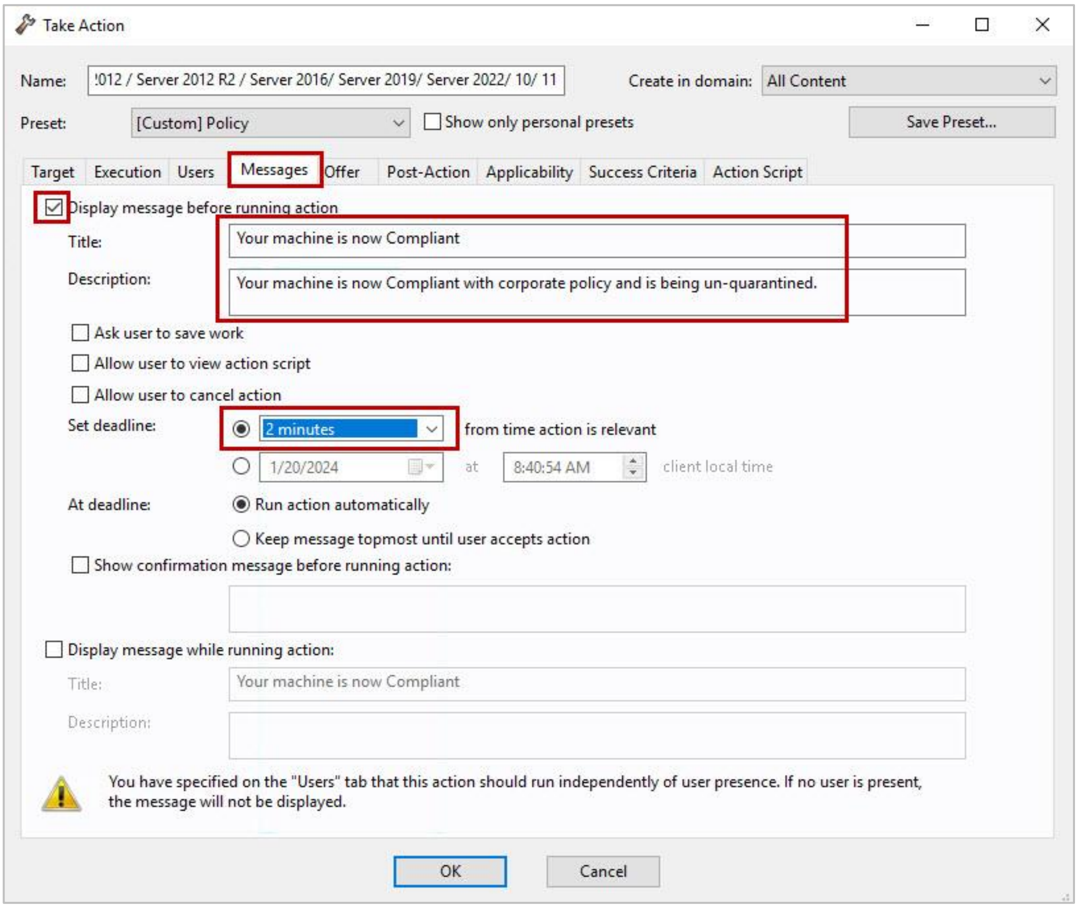
□ Limit to 3 reapplications

□ Start client downloads before constraints are satisfied

□ Stagger action start times over 5 minutes to reduce network load

24. Select the **Users** tab. Review the default settings but do not change them.
25. Select the **Messages** tab.

26. Select the **Display message before running action** option, then configure the message as follows:
    - Title: **Your machine is now Compliant.**
    - Description: **Your machine is now Compliant with corporate policy and is being un-quarantined.**
    - Set deadline: **2 minutes**
    - At deadline: **Run action automatically**



Take Action

Name: !012 / Server 2012 R2 / Server 2016/ Server 2019/ Server 2022/ 10/ 11

Create in domain: All Content

Preset: [Custom] Policy

□ Show only personal presets

Save Preset...

Target | Execution | Users | Messages | Offer | Post-Action | Applicability | Success Criteria | Action Script

☑ Display message before running action

Title: Your machine is now Compliant

Description: Your machine is now Compliant with corporate policy and is being un-quarantined.

□ Ask user to save work

□ Allow user to view action script

□ Allow user to cancel action

Set deadline: ● 2 minutes from time action is relevant

○ 1/20/2024 at 8:40:54 AM client local time

At deadline: ● Run action automatically

○ Keep message topmost until user accepts action

□ Show confirmation message before running action:

□ Display message while running action:

Title: Your machine is now Compliant

Description:

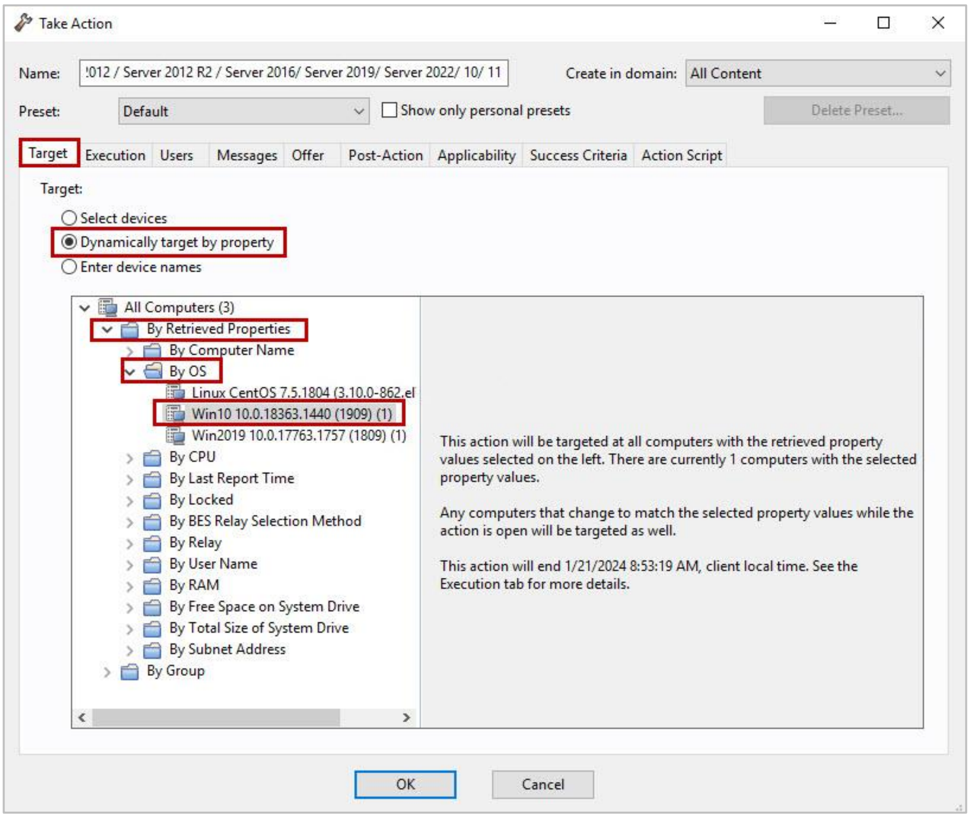
You have specified on the "Users" tab that this action should run independently of user presence. If no user is present, the message will not be displayed.

OK | Cancel

27. Review the other tabs in the **Take Action** window but do not change any settings.
28. Select the **Target** tab. Verify that the **Win10** systems are targeted.
29. Click **OK** to initiate the action.
30. Click **All Content** in the lower-left portion of the Console if it is not already selected. The navigation pane updates to show all the BigFix content.
31. In the navigation pane, expand the **Sites > External Sites > BigFix Client Compliance (IPSec Framework)**nodes, then select the **Fixlets and Tasks** node. A list of Fixlets and Tasks is displayed in the list area in the upper-right portion of the Console
32. Select the **Quarantine – Quarantine Needed – Windows 8.1 / Sever 2012 / Server 2012 R2 / Server 2016 / Server 2019 / Server 2022 / 10 / 11** Fixlet from the list pane. The details for the Fixlet are shown in the work area below.

    Hint: If the out of compliance condition has not been determined by the client, you might need to click **Show Non-Relevant Content** at the top of the Console to see the Fixlet.

33. Click **Take Action**, then select **Click here to quarantine the selected computers**. The Take Action window opens.
34. Select the **Target** tab if it is not already selected and set the following options:
    - Select the **Dynamically target by property** option
    - Expand the **All Computers > By Retrieved Properties > By OS** nodes, then select the **Win10** node.



Name: !012 / Server 2012 R2 / Server 2016/ Server 2019/ Server 2022/ 10/ 11

Create in domain: All Content

Preset: Default

□ Show only personal presets

Target:

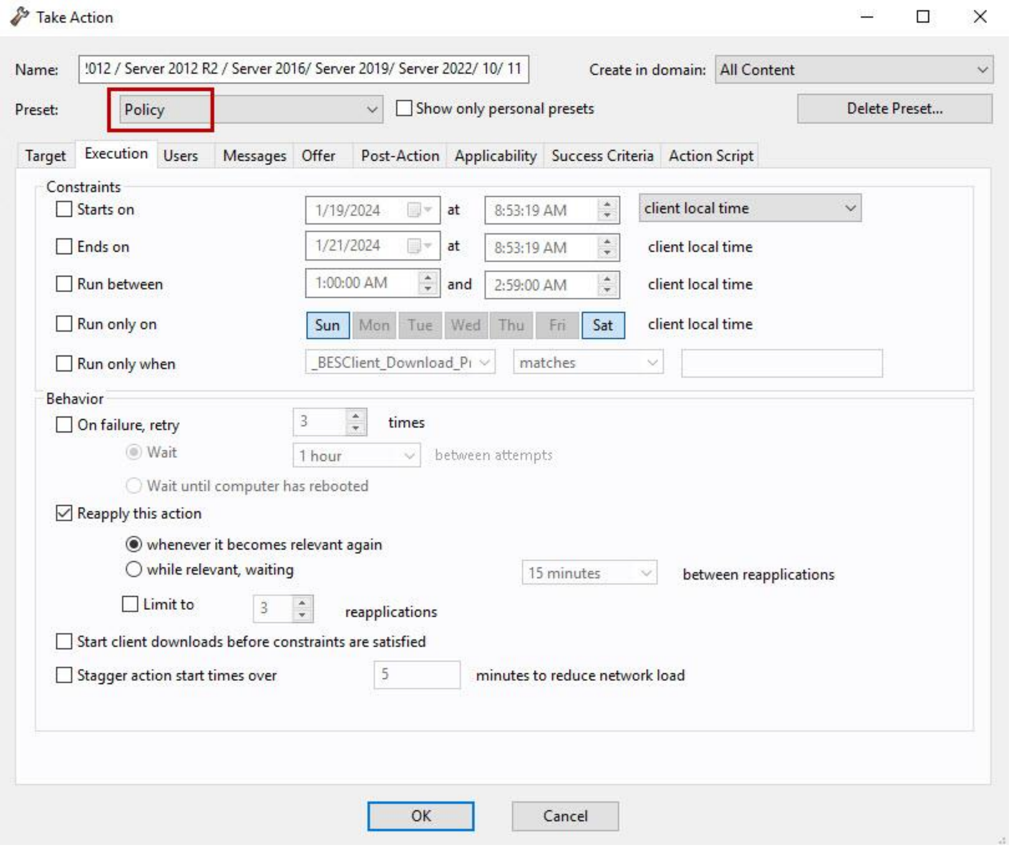
○ Select devices
● Dynamically target by property
○ Enter device names

This action will be targeted at all computers with the retrieved property values selected on the left. There are currently 1 computers with the selected property values.

Any computers that change to match the selected property values while the action is open will be targeted as well.

This action will end 1/21/2024 8:53:19 AM, client local time. See the Execution tab for more details.

35. Select the **Execution** tab, then select **Policy** from the **Preset** dropdown box.



Take Action

Name: !012 / Server 2012 R2 / Server 2016/ Server 2019/ Server 2022/ 10/ 11

Create in domain: All Content

Preset: Policy

□ Show only personal presets

Constraints

□ Starts on 1/19/2024 at 8:53:19 AM client local time

□ Ends on 1/21/2024 at 8:53:19 AM client local time

□ Run between 1:00:00 AM and 2:59:00 AM client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time

□ Run only when _BESClient_Download_Pı matches

Behavior

□ On failure, retry 3 times

● Wait 1 hour between attempts

○ Wait until computer has rebooted

☑ Reapply this action

● whenever it becomes relevant again

○ while relevant, waiting 15 minutes between reapplications

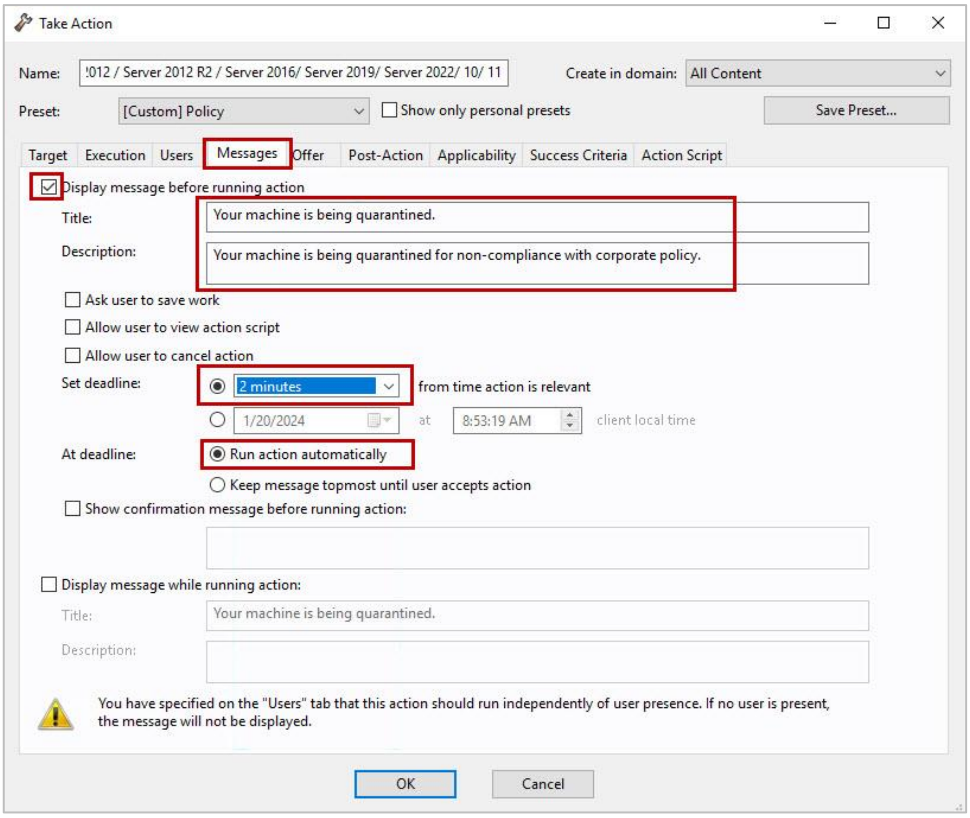
□ Limit to 3 reapplications

□ Start client downloads before constraints are satisfied

□ Stagger action start times over 5 minutes to reduce network load

36. Select the **Users** tab. Review the default settings but do not change them.
37. Select the **Messages** tab.

38. Select the **Display message before running action** option, then configure the message as follows:
    - Title: **Your machine is being quarantined.**
    - Description: **Your machine is being quarantined for non-compliance with corporate policy.**
    - Set deadline: **2 minutes**
    - At deadline: **Run action automatically**



Take Action

Name: !012 / Server 2012 R2 / Server 2016/ Server 2019/ Server 2022/ 10/ 11

Create in domain: All Content

Preset: [Custom] Policy

□ Show only personal presets

☑ Display message before running action

Title: Your machine is being quarantined.

Description: Your machine is being quarantined for non-compliance with corporate policy.

□ Ask user to save work

□ Allow user to view action script

□ Allow user to cancel action

Set deadline: ● 2 minutes from time action is relevant

○ 1/20/2024 at 8:53:19 AM client local time

At deadline: ● Run action automatically

○ Keep message topmost until user accepts action

□ Show confirmation message before running action:

□ Display message while running action:

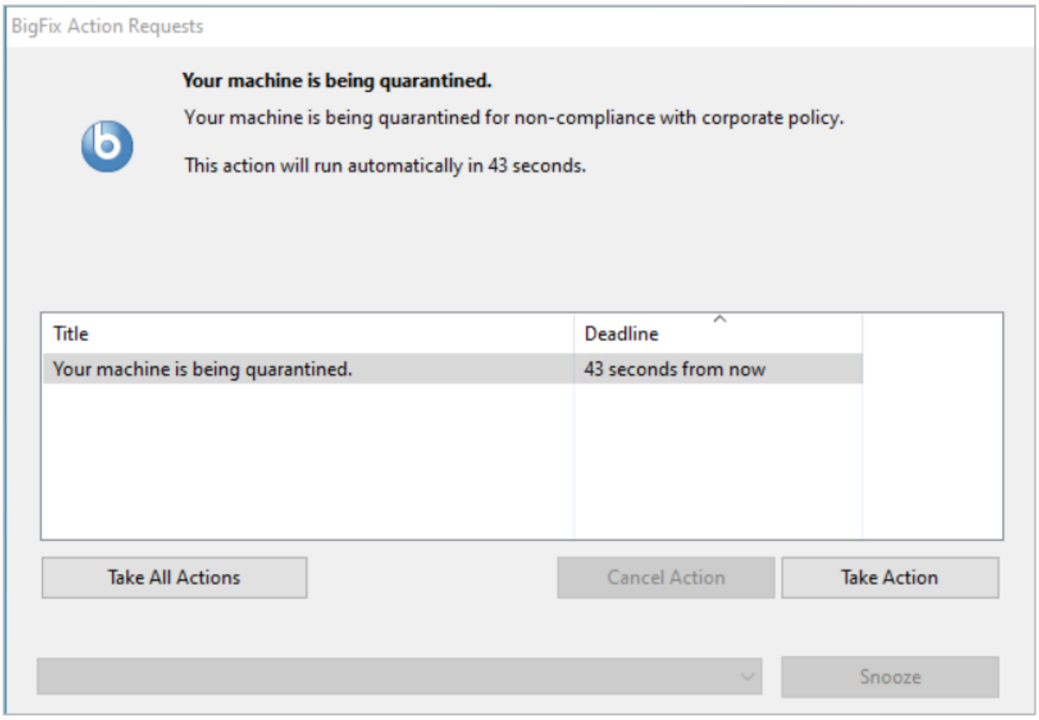
Title: Your machine is being quarantined.

Description:

You have specified on the "Users" tab that this action should run independently of user presence. If no user is present, the message will not be displayed.

39. Review the other tabs in the **Take Action** window but do not change any settings.
40. Select the **Target** tab. Verify that the **Win10** systems are targeted.
41. Click **OK** to initiate the action. Wait until the becomes Relevant to the **BESFNDWIN10** virtual machine before continuing.
42. Switch to the **BESFNDWIN10** virtual machine. If you are not already logged in, log in with the user name of **tecuser** and a password of **bigfixrocks**.

43. Observe the BigFix notification that the machine is about to be quarantined.



Your machine is being quarantined.

Your machine is being quarantined for non-compliance with corporate policy.

This action will run automatically in 43 seconds.

Title	Deadline
Your machine is being quarantined.	43 seconds from now

44. Double-click the **Microsoft Edge** icon on the **Windows Desktop**. The browser opens.
45. Attempt to connect to the Internet using the browser by entering the following URL in the address bar:

    `https://google.com`

    Were you able to successfully connect to the Google home page?

46. Try connecting to other Internet pages. Were you successful?

You have now successfully completed Exercise 23.

Exercise 24 – Bring Quarantined Computer into Compliance

In this exercise, you return the BESFNDWIN10 system to compliance by starting Notepad and observe the behavior.

1. Switch to the Windows 10 virtual machine: **BESFNDWIN10**. If you are logged off, log in to the server as **tecuser** with a password of **bigfixrocks**.
2. Begin entering the string **Notepad** in the **search** field located in the lower-left portion of the taskbar. Select the **Notepad** app to start it. A blank Notepad file is opened.
3. Double-click the **baretail** icon on the **Windows Desktop**. The baretail app opens.
4. Click **Open** and navigate to the BigFix Client logfile directory as follows:

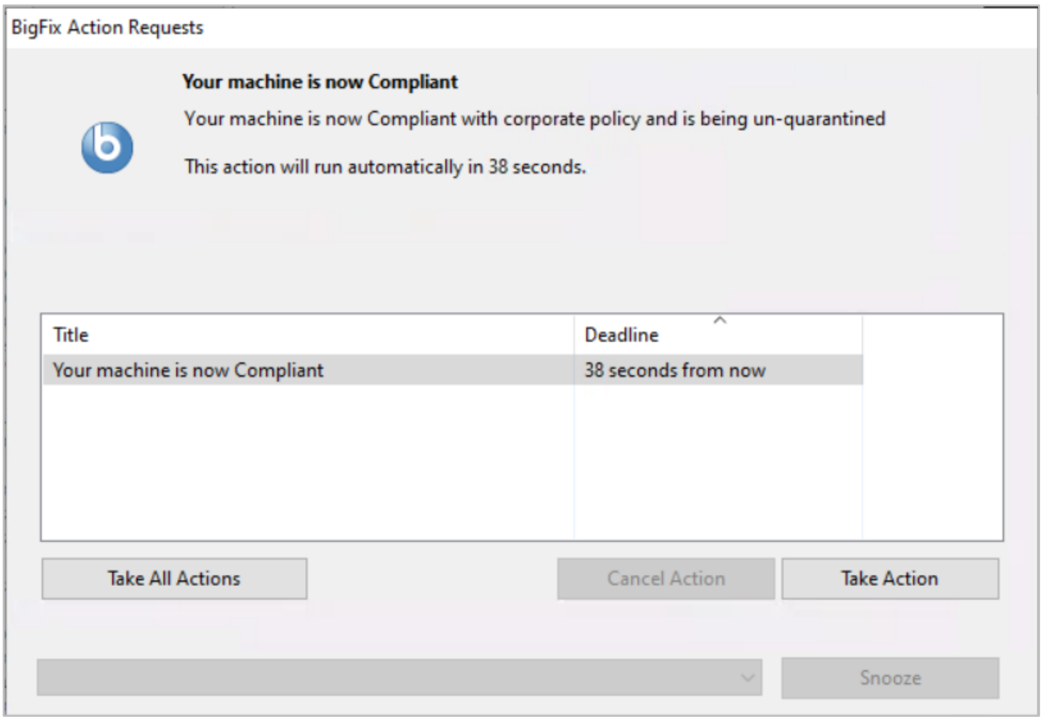
    ```
    C:\Program Files (x86)\BigFix Enterprise\BES
    Client\__BESData\__Global\Logs
    ```

5. Open the logfile represented by today's date. The logfile names are in the following format: **yyyymmdd.log**

6. Monitor the logfile until you see the **Quarantine – Determine Compliance** action run. This Policy Action is set to run every 5 minutes, so you might have to wait several minutes for it to run again.

   Important: For the Un-Quarantine task to become Relevant, the target system must not be in a Pending Restart state. You can verify whether the BESFNDWIN10 system requires a restart by reviewing the **Applicable Computers** tab of the **Restart Needed** Task that is located in the BES Support site. Restart BESFNDWIN10 if required and verify that a restart is no longer needed. Make sure to restart the Notepad application after restarting to ensure that the system is still compliant.

7. Since the process **notepad.exe** is running the system is now compliant with the Compliance Document that was previously distributed. Observe the BigFix notification that the machine is now compliant.



BigFix Action Requests

Your machine is now Compliant

Your machine is now Compliant with corporate policy and is being un-quarantined

This action will run automatically in 38 seconds.

Title	Deadline
Your machine is now Compliant	38 seconds from now

8. Click **Take Action** or wait until the deadline passes before continuing.
9. Attempt to connect to the Internet using the browser by entering the following URL in the address bar:

   https://google.com

   Were you able to successfully connect to the Google home page now?

You have now successfully completed Exercise 24.

Exercise 25 (optional) – Reviewing the Patch and Vulnerability Reports

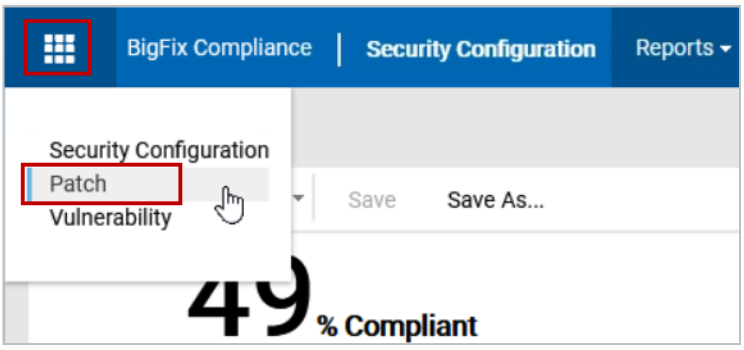
In this optional exercise, you review the Patch and Vulnerability reports that are now available after enabling them in Exercise 21 – Enabling Patch and Vulnerabilities Reporting on page 73. Verify that the last ad-hoc Data Import has completed before beginning this optional exercise.

1. Switch to the BigFix Server virtual machine: **BESFNDWINROOT**. If you are logged off, log in to the server as **Administrator** with a password of **bigfixrocks**.
2. Double click the **Firefox** icon on the desktop. The browser opens.
3. Enter the following URL in the address section of the browser:

   https://BESFNDWINROOT:9085

   Note: You might receive a security warning indicating that it is unsafe to continue to the page. Click the **Advanced** option, accept the risk and continue to the site.

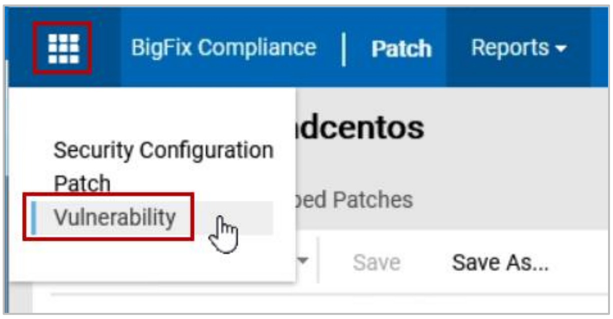
   The BigFix Compliance login page opens.
4. Enter **adminmo** as the username with a password of **B1gfixrocks!**. Click **Login**. The Overview page opens.
5. Select **Patch** from the menu in the upper-left portion of the Overview page. The Patch Base Report opens.



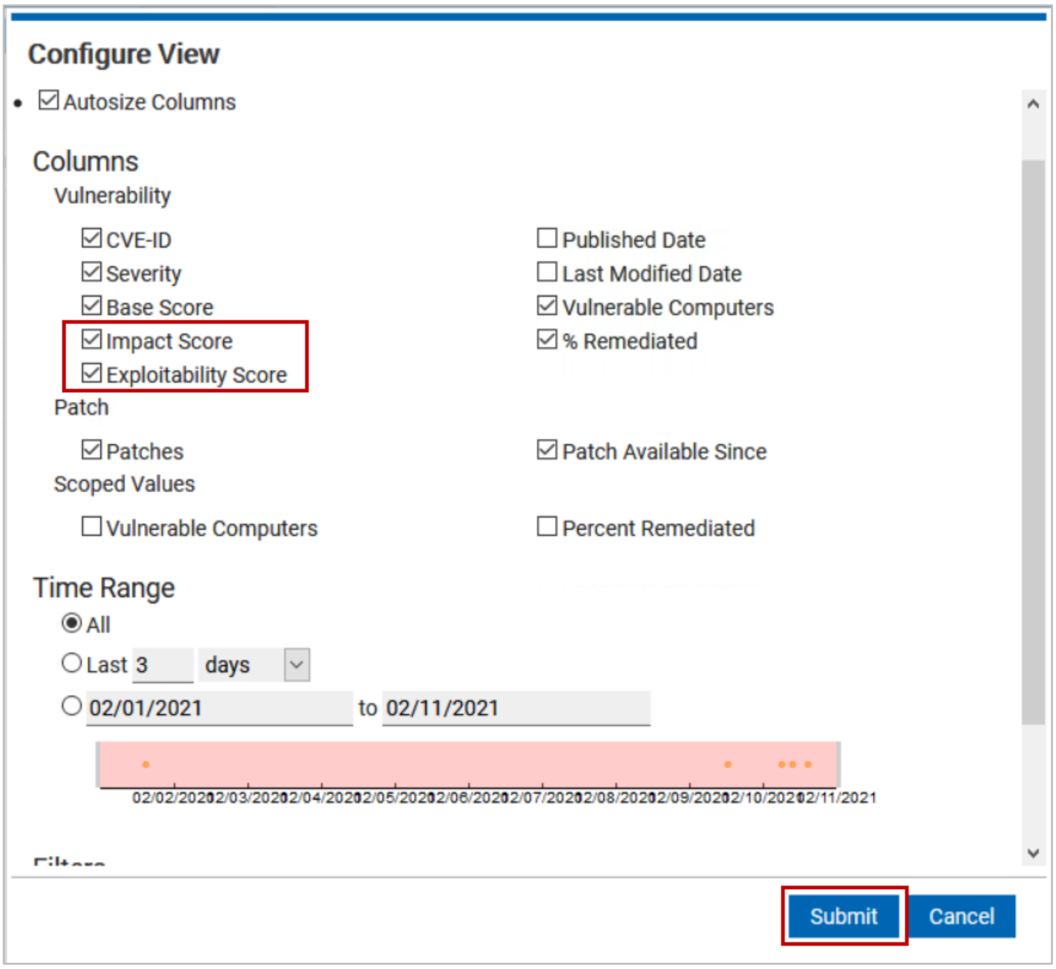
6. Scroll to the bottom of the report and locate the **Most Unaddressed Computers** section. Review the **% Remediated** column.
7. Click the **besfndcentos** computer link.

   What is the number of remediations required for this computer?

8. Select **Vulnerability** from the menu in the upper-left portion of the page header. The Vulnerability Overview report opens.



9. Review the data that is presented in each section of the **Vulnerability Overview** report.
10. Review the numbers of Vulnerabilities for each severity in the **Unpatched Vulnerability Instances** section of the report.
11. Click the **link** to the left of **Critical** severity vulnerabilities. This number represents the number of Critical vulnerabilities that exist in the environment. The Critical Vulnerabilities page opens.
12. Click the **gear** icon in the upper-right portion of the **Vulnerabilities** report. The Configure View pane opens.
13. Locate the **Vulnerability** section and place a check beside the **Impact Score** and **Exploitability Score** options.



Configure View

- ☑ Autosize Columns

Columns

Vulnerability

☑ CVE-ID
☑ Severity
☑ Base Score
☑ Impact Score
☑ Exploitability Score

☐ Published Date
☐ Last Modified Date
☑ Vulnerable Computers
☑ % Remediated

Patch

☑ Patches
☑ Patch Available Since

Scoped Values

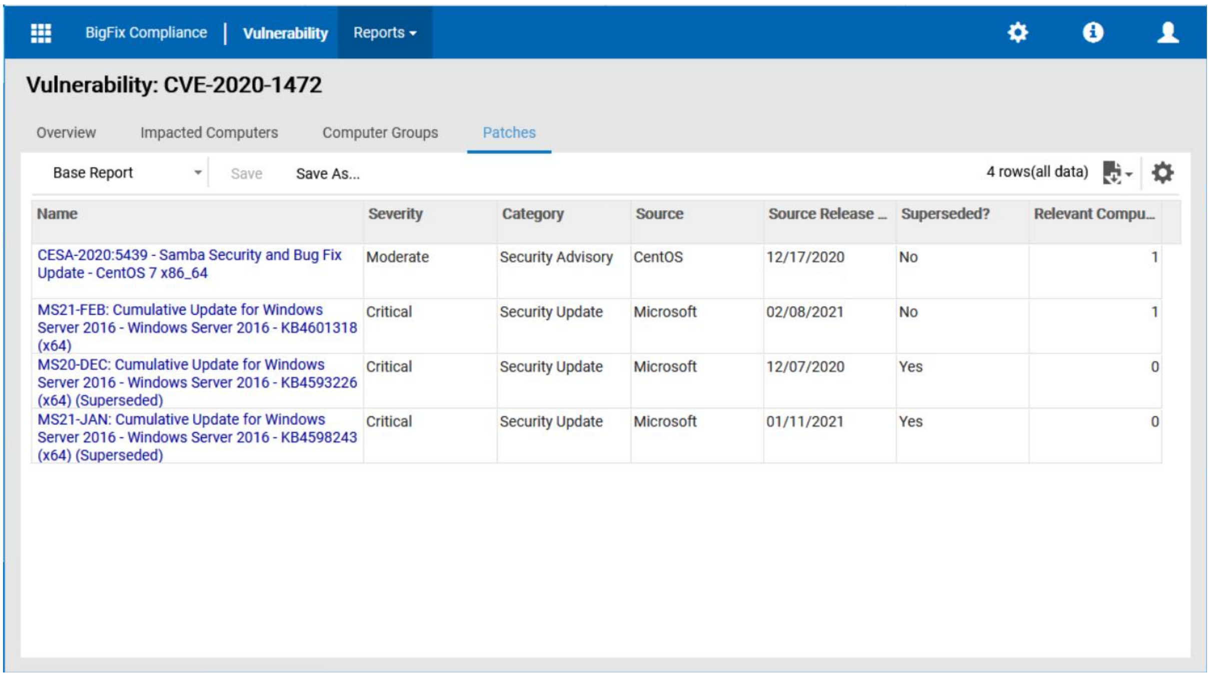
☐ Vulnerable Computers
☐ Percent Remediated

Time Range

● All
○ Last 3 days
○ 02/01/2021 to 02/11/2021

14. Click **Submit**. The Impact Score and Exploitability Score columns are added to the Vulnerabilities report.
15. Click the link in the **Patches** column for any list vulnerability where the number shown in the **Vulnerable Computers** column is greater than **0**.

16. Click the **link** in the **Patches** column. The detailed report for the selected CVE opens and lists the patches that are associated with the selected vulnerability.

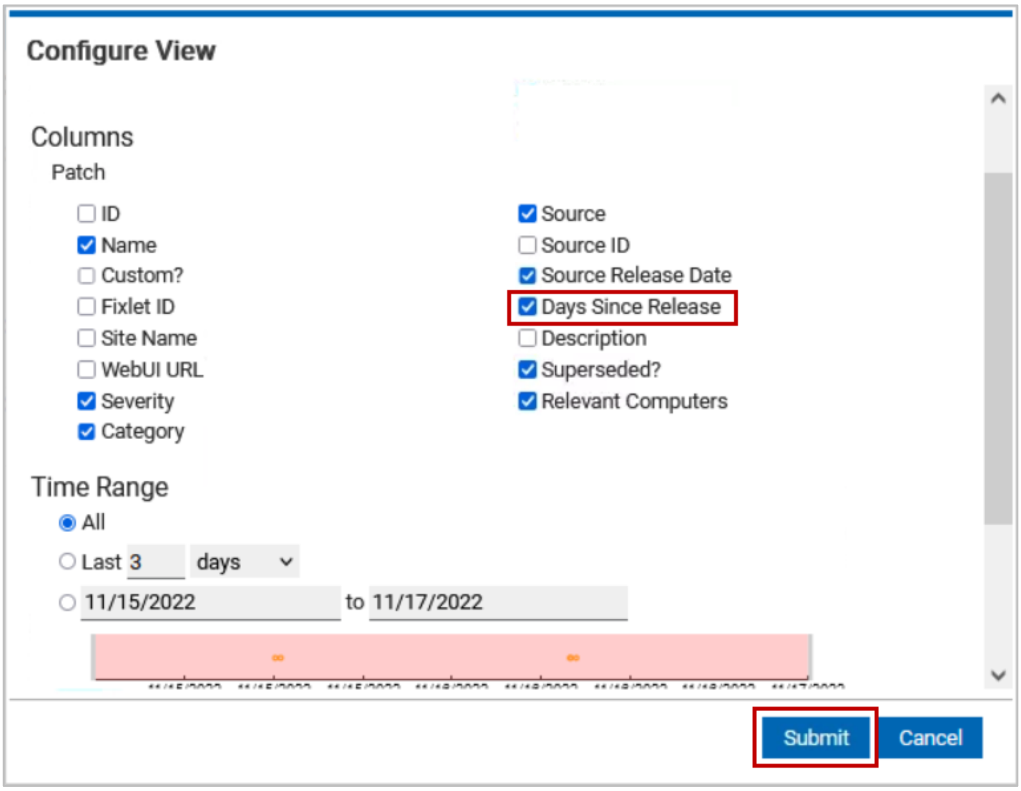


Vulnerability: CVE-2020-1472

Name	Severity	Category	Source	Source Release ...	Superseded?	Relevant Compu...
CESA-2020:5439 - Samba Security and Bug Fix Update - CentOS 7 x86_64	Moderate	Security Advisory	CentOS	12/17/2020	No	1
MS21-FEB: Cumulative Update for Windows Server 2016 - Windows Server 2016 - KB4601318 (x64)	Critical	Security Update	Microsoft	02/08/2021	No	1
MS20-DEC: Cumulative Update for Windows Server 2016 - Windows Server 2016 - KB4593226 (x64) (Superseded)	Critical	Security Update	Microsoft	12/07/2020	Yes	0
MS21-JAN: Cumulative Update for Windows Server 2016 - Windows Server 2016 - KB4598243 (x64) (Superseded)	Critical	Security Update	Microsoft	01/11/2021	Yes	0

17. Select the **Impacted Computers** tab at the top of the **Vulnerability** report. A list of computers that are vulnerable to the selected CVE is displayed.
18. Click the **Patches** tab located at the top of the selected vulnerability page. A list of patches associated with the selected vulnerability is displayed.
19. Click the **gear** icon in the upper-right portion of the **current** page. The Configure View pane opens.

20. Place a check beside the **Days Since Release** option. Click **Submit**.



Configure View

Columns

Patch

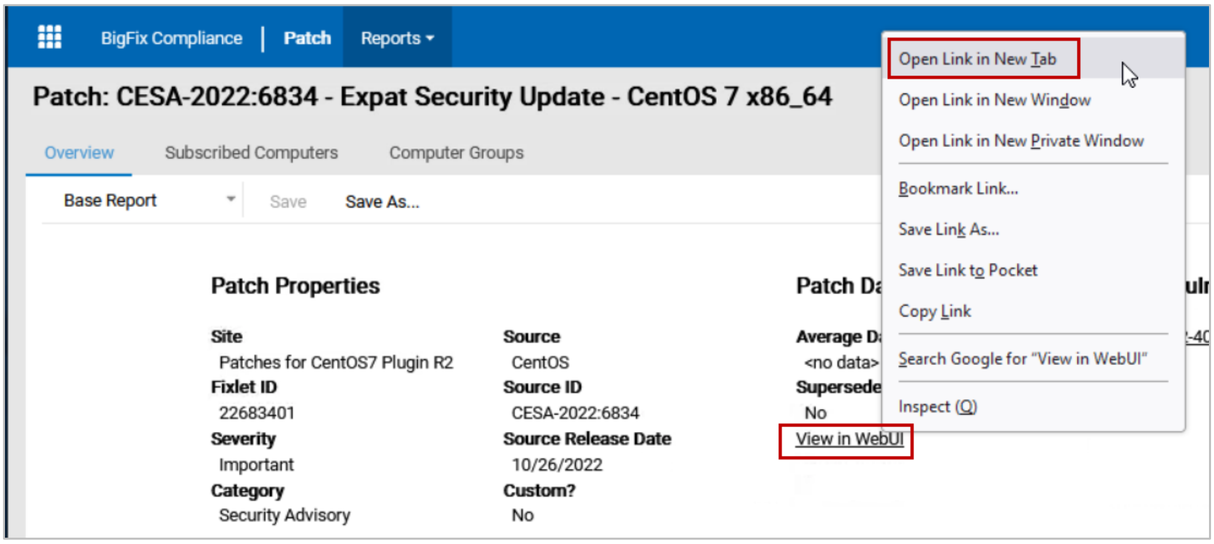
- ☐ ID
- ☑ Name
- ☐ Custom?
- ☐ Fixlet ID
- ☐ Site Name
- ☐ WebUI URL
- ☑ Severity
- ☑ Category
- ☑ Source
- ☐ Source ID
- ☑ Source Release Date
- ☑ Days Since Release
- ☐ Description
- ☑ Superseded?
- ☑ Relevant Computers

Time Range

- ● All
- ○ Last 3 days
- ○ 11/15/2022 to 11/17/2022

The Days Since Release column is added to the report.

21. Click the **link** in the **Name** column for any patch listed where the number shown in the **Relevant Computers** column is greater than **0**. The Overview page for the selected patch opens.
22. Review the information on the **Overview** page for the selected patch.
23. Right-click the **View in WebUI** link the **Patch Data** column on the overview report page and select **Open Link in New Tab** from the context menu.



Patch: CESA-2022:6834 - Expat Security Update - CentOS 7 x86_64

Patch Properties

Site Patches for CentOS7 Plugin R2	**Source** CentOS
Fixlet ID 22683401	**Source ID** CESA-2022:6834
Severity Important	**Source Release Date** 10/26/2022
Category Security Advisory	**Custom?** No

Patch Da

Average D
<no data>

Supersede
No

View in WebUI

The WebUI login page opens in the new browser tab.

Note: You might receive a security risk message. If so, click **Advanced** and then click **Accept the Risk and Continue**.

24. Enter **adminmo** as the **Username** with a **password** of **B1gfixrocks**. Click **Login**. The WebUI page opens to the selected patch. From this page an operator could deploy the selected patch to remediate the Vulnerability.

    Note: Since this is the first time that the WebUI has been opened it might take several minutes for the cache to be updated and the page to load.

    This completes the lab exercises for the BigFix BESFNDC301 course.