

**BigFix Insights for Vulnerability Management
Quick Start Guide**



Special notice

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

Edition notice

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

Contents

- Chapter 1. BigFix Insights for Vulnerability Remediation.....5**
- Chapter 2. System requirements.....7**
- Chapter 3. Deployment and configuration..... 11**
 - Deployment and configuration for Tenable.io.....11
 - Deployment and configuration for Tenable.sc..... 18
 - Deployment and configuration for Qualys..... 25
- Chapter 4. IVR Fixlets and Tasks..... 33**
- Notices..... xl

Chapter 1. BigFix Insights for Vulnerability Remediation

Use this section to become familiar with BigFix Insights for Vulnerability Remediation infrastructure and key concepts necessary to understand how it works.

BigFix Insights for Vulnerability Remediation integrates BigFix with sources of vulnerability data. The purpose is to guide BigFix users on how to apply the best patch and configuration settings to remediate discovered vulnerabilities, and thus reduce risk and improve security.

BigFix Insights for Vulnerability Remediation uses advanced correlation algorithms to aggregate and process the vulnerability data with information from BigFix to drive analytics reports. The output of the analytics facilitates remediation through the Baseline Creation Wizard by recommending the latest available patches for the discovered vulnerabilities.

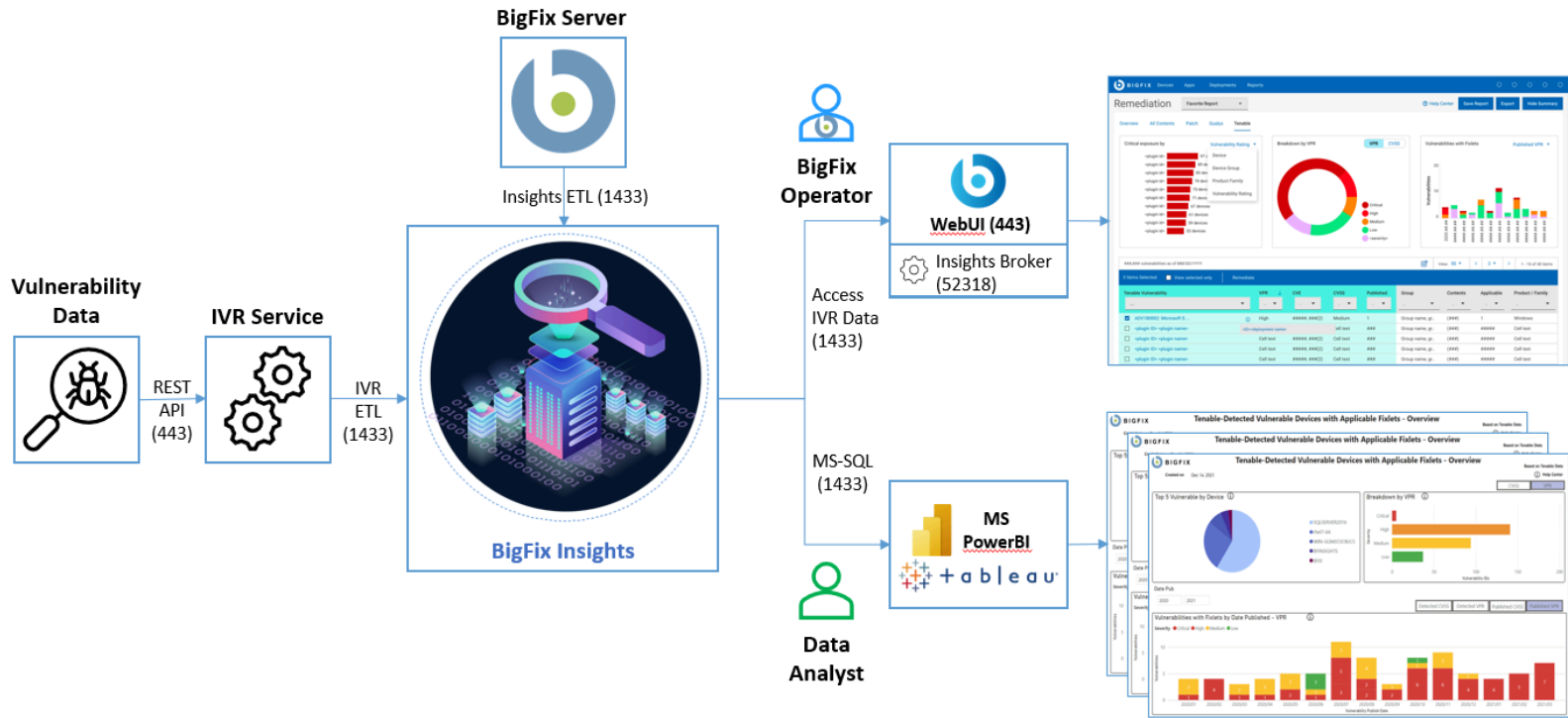
IVR data is available in:

- WebUI IVR app - it is required to enable WebUI to access IVR data through Insights. For more information on installing IVR app, see [Setting up IVR App](#).
- BI Tools for Data Analysis - existing IVR reports in PowerBI and Tableau. Refer to the [link](#) to find out more about IVR reports.

IVR limitations:

- Only one source of vulnerability data for automatic ingestion is supported for a given BigFix Insights instance
- One BigFix WebUI instance can manage only one BigFix Insights database. This limitation means that you cannot simultaneously connect or manage multiple instances of BigFix Insights through one WebUI instance.

Figure 1. Architecture overview of BigFix Insights for Vulnerability Remediation



Chapter 2. System requirements

Learn more about the prerequisites and system requirements for BigFix Insights for Vulnerability Remediation (IVR) service.

Table 1. Prerequisites and system requirements for IVR service

Hardware requirements	
CPU	minimum 2 cores (recommended 4)
RAM	<p>On top of host OS requirements:</p> <ul style="list-style-type: none"> • < 1M Findings from Vulnerability Management Product = 16GB • < 2M Findings from Vulnerability Management Product = 32GB • < 3M Findings from Vulnerability Management Product = 48GB • < 4M Findings from Vulnerability Management Product = 64GB
Disc space	<ul style="list-style-type: none"> • < 1M Findings from Vulnerability Management Product = 4GB - 8GB preferred • < 2M Findings from Vulnerability Management Product = 8GB - 12GB preferred • < 3M Findings from Vulnerability Management Product = 12GB - 16GB preferred • < 4M Findings from Vulnerability Management Product = 16GB - 20GB preferred
Execution Time	<p>The overall run time of data synchronization and processing depends on:</p> <ul style="list-style-type: none"> • CPU Speed • Number of findings • Number of assets in insights • Number of patch sites loaded within the BFE environment • API latency • Conflicting workloads on IVR machine
Software requirements	

Table 1. Prerequisites and system requirements for IVR service (continued)



BigFix Component Requirements	<ul style="list-style-type: none"> • BigFix Insights WebUI App (v6) (minimum)
Prerequisites	<ul style="list-style-type: none"> • Microsoft VC++ Redistributable package 2012 https://www.microsoft.com/en-in/download/details.aspx?id=30679 • Microsoft® ODBC Driver 17 for SQL Server® https://www.microsoft.com/en-us/download/details.aspx?id=56567 <p> Note: The Fixlet will attempt to deploy the pre-requisites automatically.</p>
Operating system	<ul style="list-style-type: none"> • Microsoft Windows 2016 • Microsoft Windows 2019
Supported BigFix versions	<ul style="list-style-type: none"> • Windows - based BigFix Server, Version 10 <p> Note: BigFix Insights for Vulnerability Remediation does not currently support non-Windows-based BigFix Server environments.</p>
BigFix License Requirements	<ul style="list-style-type: none"> • BigFix Lifecycle • BigFix Compliance • BigFix Remediate
Supported Vulnerability Management Platforms	<ul style="list-style-type: none"> • Qualys VMDR v2 REST API: https://www.qualys.com/docs/qualys-api-vm-pc-user-guide.pdf • Tenable.SC versions from 5.17 up to 6.0.0. • Tenable.IO

Table 1. Prerequisites and system requirements for IVR service (continued)




	 Note: It is required to use Administrator user role within Tenable to enable the generation of API keys that are used by IVR to maintain the interface with Tenable.
BI tool	<ul style="list-style-type: none"> • Power BI Desktop/Server, 2021 + (Rec. May 2021)  Note: Microsoft offers two distinct products called Power BI desktop. Use the one that is optimized for Power BI Report Server: https://www.microsoft.com/en-us/download/details.aspx?id=56723 <ul style="list-style-type: none"> • Tableau Desktop/Server, 2020.4 +
Network requirements	<ul style="list-style-type: none"> • Connectivity to Vulnerability Management API Server URL (port 443 by default) • Connectivity to BigFix Insights SQL database (port 1433 by default)  Note: IVR now supports proxy-based connectivity. Refer to the link for more information. <ul style="list-style-type: none"> • By default WebUI IVR app listens on port 52318. It can be changed in the WebUI application configuration file with <code>_WebUIAppEnv_INSIGHT_BROKER_PORT</code> setting.

Table 1. Prerequisites and system requirements for IVR service (continued)

System limitations	<ul style="list-style-type: none">• Only one source of vulnerability data for automatic ingestion is supported for a given BigFix Insights instance• A single BigFix WebUI instance can manage only one BigFix Insights database.
---------------------------	--

Chapter 3. Deployment and configuration

This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution for:

[Tenable.io](#)

[Tenable.sc](#)

[Qualys](#)

Refer to the [link](#) to learn more about other Fixlets and Tasks available for BigFix Insights for Vulnerability Remediation solution.

Deployment and configuration for Tenable.io

This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution.

To install and configure BigFix Insights for Vulnerability Remediation service, perform below steps:




Note: To use the latest release build, uninstall the old version.

1. Enable a content site.

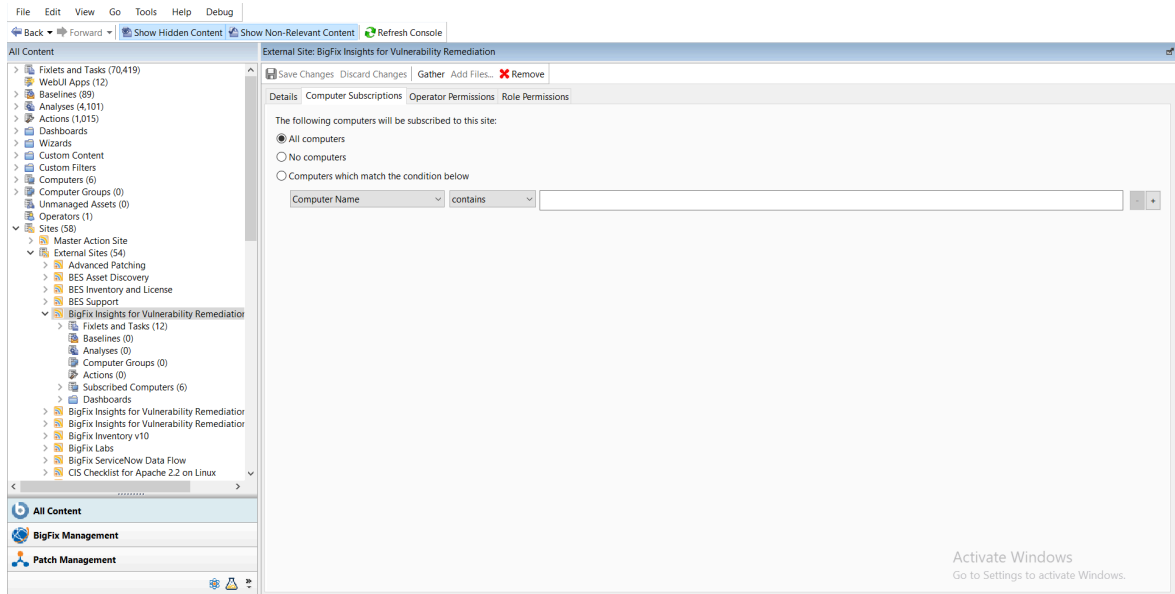
Navigate to BigFix License Overview Dashboard. In **Compliance/Lifecycle** panel, click **Enable BigFix Insights for Vulnerability Remediation** Fixlet to gather the required content.

The screenshot shows the BigFix Console interface. On the left is a navigation pane with categories like Deployment Overview, License Overview, Warnings, BES Deployment Management, Maintenance Window Management, Baselines, Analyses, Actions, Custom Content, Custom Filters, Computer Management, Unmanaged Assets, Operators, and Manage Sites. The main area is titled 'BigFix License Overview' and shows a table of licenses. The table has columns for status, name, and count. The 'BigFix Insights for Vulnerability Remediation' license is highlighted with a green box.

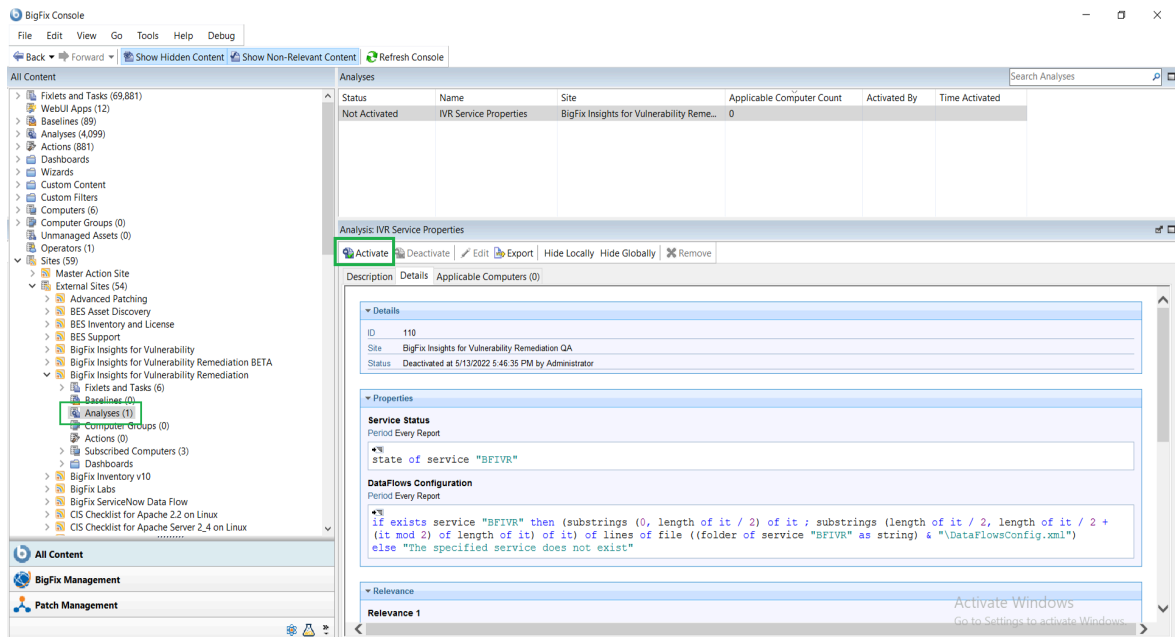
STATUS	LICENSE NAME	COUNT
ENABLED	Patches for Ubuntu 1804	0
ENABLED	Patches for Windows	19
ENABLED	Patching Support	21
ENABLED	Power Management	20
ENABLED	Remote Control	21
ENABLED	Server Automation	65
ENABLED	Software Distribution	21
ENABLED	Updates for Mac Applications	0
ENABLED	Updates for Windows Applications	19
ENABLED	Updates for Windows Applications Extended	19
ENABLED	Virtual Endpoint Manager	21
ENABLED	Vulnerability Reporting	0
ENABLED	Windows Point of Sale	0
ENABLE	BigFix Insights for Vulnerability Remediation	
ENABLE	Client Manager for Application Virtualization	
ENABLE	Client Manager for TPM/OSD	
ENABLE	MaaS360 Mobile Device Management	
ENABLE	OS Deployment	
ENABLE	Patches for CentOS 5 Native Tools (Deprecated)	
ENABLE	Patches for CentOS 6 Plugin R2	
ENABLE	Patches for CentOS 7 Plugin R2	
ENABLE	Patches for CentOS 8	

 **Note:** Refer to the following [link](#) for more information about **License Overview dashboard**.

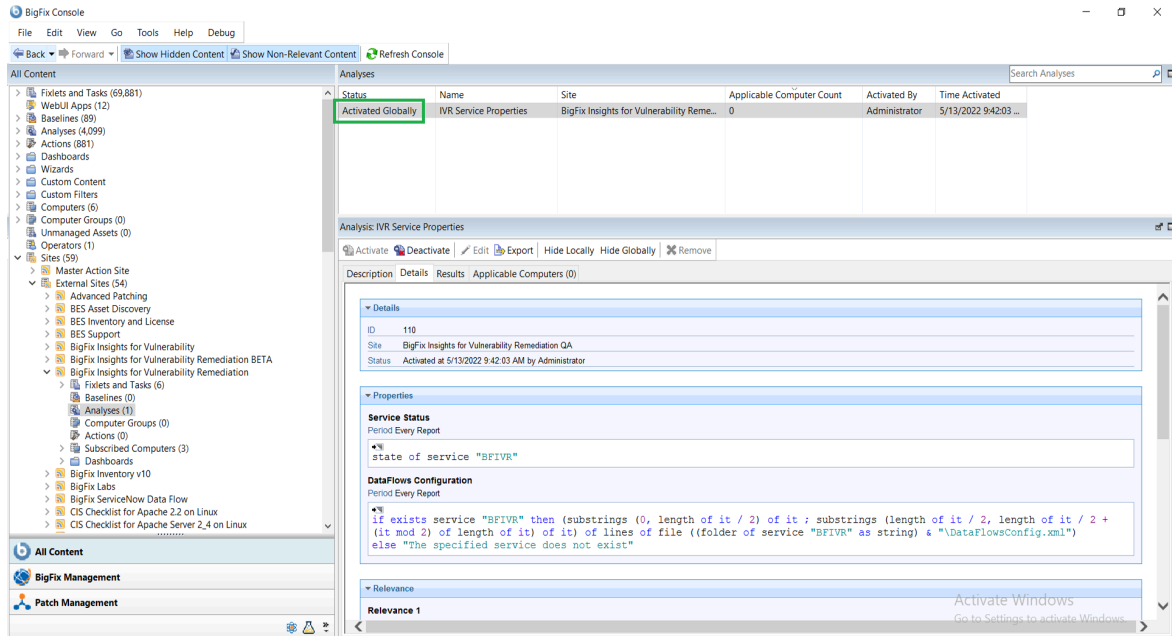
2. Subscribe computers to the site. It is recommended to subscribe to All computers. For more information on **Computer Subscriptions Tab** refer to the [link](#).




3. Activate the analysis.



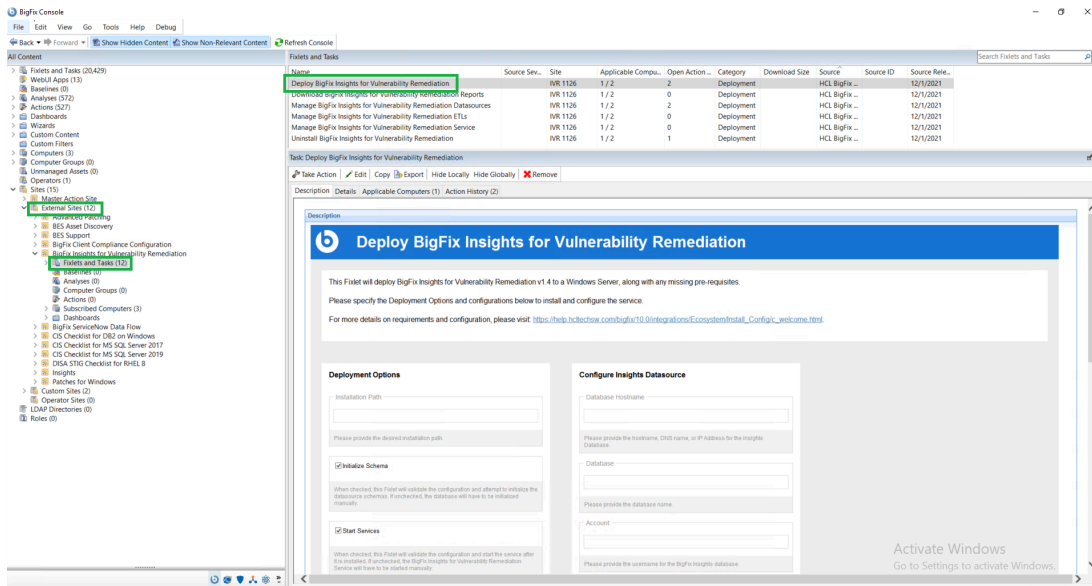
Status of the analysis should be **Activated Globally**.



 **Note:** Refer to the [link](#) to learn more about **Computer Subscriptions Tab**.

4. Deploy the solution to the target server.

- a. Click **Deploy Insights for Vulnerability Remediation** Fixlet in the **BigFix Insights for Vulnerability Remediation** external sites.



- b. Fill in the blanks in the description panel and **Take action** to deploy the IVR services.

Please provide:

- Deployment Options
- Installation path

- Configure Insights Database
 - Database Hostname - the hostname, DNS name, or IP address for the Insights Database
 - Database - database name
 - Account - the user name for the BigFix Insights Database
 - Password - the password for the user name specified above
- Configure IVR ETL
 - Import Vulnerability Data Into Insights - specify the desired ETL schedule for Vulnerability data
 - Import BigFix Asset Data Into Tenable.IO - specify the desired ETL schedule for Asset data*

ETL schedule for Vulnerability data uses Cron Time String Format. Refer to the link to find out more about the Scheduler.

The column named `datasource_device_id` in Bigfix Insight serves as the device identifier for IVR purposes. This identifier is labeled as `bigfix_asset_id` and forwarded to TenableIO.

*Tenable.IO offers an optional feature that allows BigFix IVR to transmit endpoint asset data to Tenable.IO. This can potentially give Tenable users access to information about assets that were previously unknown. By providing a more comprehensive and current view of the assets, Tenable.IO and BigFix can help in identifying and mitigating potential security risks, identifying under-utilized resources, and facilitating compliance efforts. For more information about assets in Tenable.IO refer to the following page: <https://docs.tenable.com/tenableio/Content/Platform/Explore/>

The screenshot displays the BigFix console interface. At the top, there is a table titled 'Fixlets and Tasks' with columns: ID, Name, Source Sev..., Site, Applicable Compu..., Open Action..., Category, Download Size, Source, and Source ID. Two rows are visible: ID 3871 for 'Deploy BigFix Insights for Vulnerability Remediation' and ID 3876 for 'Download BigFix Insights for Vulnerability Remediation Reports'. Below the table, a task is selected: 'Task: Deploy BigFix Insights for Vulnerability Remediation'. The main area shows two configuration panels. The left panel, 'Configure IVR ETL', has two sections. The first, 'Import Vulnerability Data Into Insights', includes a checkbox (checked), a text input for 'Vulnerability import Schedule', and a note: 'ETL from the Vulnerability Management system to BigFix Insights will be enabled.' The second section, 'Import BigFix Asset Data Into Tenable IO', also has a checked checkbox, a text input for 'Asset import Schedule', and a note: 'ETL for Asset data from BigFix Insights to Tenable IO will be enabled.' The right panel, 'Configure Vulnerability Management Datasource', includes a dropdown for 'VM Platform' set to 'TenableIO', a text input for 'Connection String', and two sections for 'Access Key' and 'Secret Key', each with a text input and a note: 'Please provide the [key] for the Vulnerability Management Platform.'

[ExploreAssets.htm.](#)

Activate Windows

- Configure Vulnerability Management Datasource

- VM Platform - specify the VM Platform
- Connection String - the URL to the Vulnerability Management Platform
- Access Key - access key for the Vulnerability Management Platform
- Secret Key - secret key for the user name specified above

Task Deploy BigFix Insights for Vulnerability Remediation

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (2)

Deployment Options

Installation Path

Please provide the desired installation path.

Initialize Schema

When checked, this Fidet will validate the configuration and attempt to initialize the database schemas. If unchecked, the database will have to be initialized manually.

Start Services

When checked, this Fidet will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for Vulnerability Remediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname

Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database

Please provide the database name.

Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the user names specified above.

Configure IVR ETL

Import Vulnerability Data Into Insights

When checked, the ETL from the Vulnerability Management system to BigFix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

Import BigFix Asset Data into Tenable IO

When checked, the ETL for Asset data from BigFix Insights to Tenable IO will be

Configure Vulnerability Management Datasource

VM Platform

TenableIO

Please specify the Vulnerability Management Platform

Connection String

Please provide the URI to the Vulnerability Management Platform

Access Key

To provide proxy details click on **Advanced Settings**. This option is not mandatory.

Advanced Settings

Proxy Settings for Insights Datasource

Proxy Host

Please provide the proxy/host for Insights Datasource.

Proxy User

Please provide the proxy/username.

Proxy Password

Please provide the proxy/password.

Proxy Settings for VM

Proxy Host

Please provide the proxy/host URI for VM

Proxy User

Please provide the proxy/username.

Proxy Password

Please provide the proxy/password.



Note: Please note the following pre-requisites:

- Microsoft Visual Studio C++ Redistributable 2012: <https://www.microsoft.com/en-in/download/details.aspx?id=30679>
- Microsoft ODBC Driver 17 for SQL Server: <https://www.microsoft.com/en-us/download/details.aspx?id=56567>
 - <https://www.microsoft.com/en-us/download/details.aspx?id=56567>

The Fixlet will attempt to deploy the pre-requisites automatically.

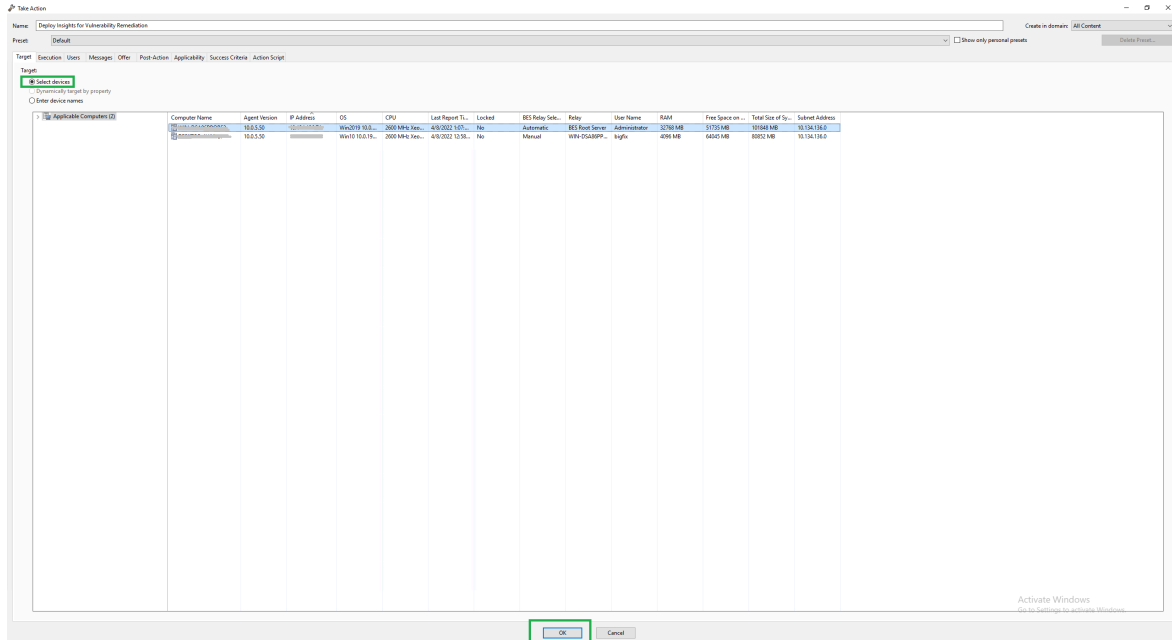


Warning: Do not deploy the **BigFix Insights for Vulnerability Service** to more than 1 machine.



Warning: Do not have more than 2 dataflows per IVR Service.

5. Select target devices under Target tab and click **OK**.



Wait for the deployment to complete. Status should show 100% completed.

Status		
100.00% Completed (1 of 1 applicable computers)		
Status	Count	Percentage
Completed	1	100.00%

- If **Start services** option was selected in the Description panel **BigFix Insights for Vulnerability Remediation** service should be present and in **Running** state in the Services. Otherwise, the **BigFix Insights for Vulnerability Remediation** service must be started manually. This indicates deployment is completed. Deployment can be checked on the log file: install.log.

Refer to the following [link](#) to learn more about other IVR Tasks.

Deployment and configuration for Tenable.sc

This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution.

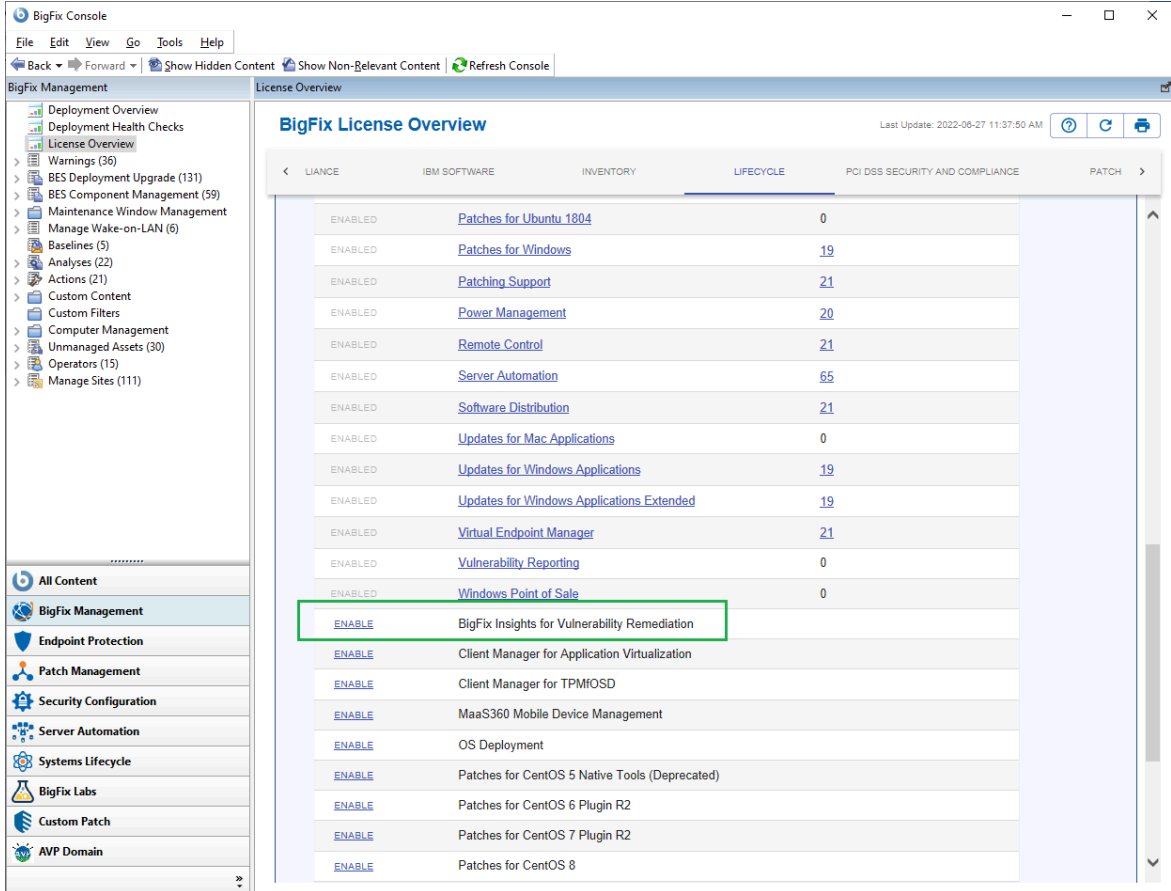
To install and configure BigFix Insights for Vulnerability Remediation service, perform below steps:



Note: To use the latest release build, the old version must be uninstalled.

1. Enable a content site.

Navigate to BigFix License Overview Dashboard. In **Compliance/Lifecycle** panel, click **Enable BigFix Insights for Vulnerability Remediation Fixlet** to gather the required content.



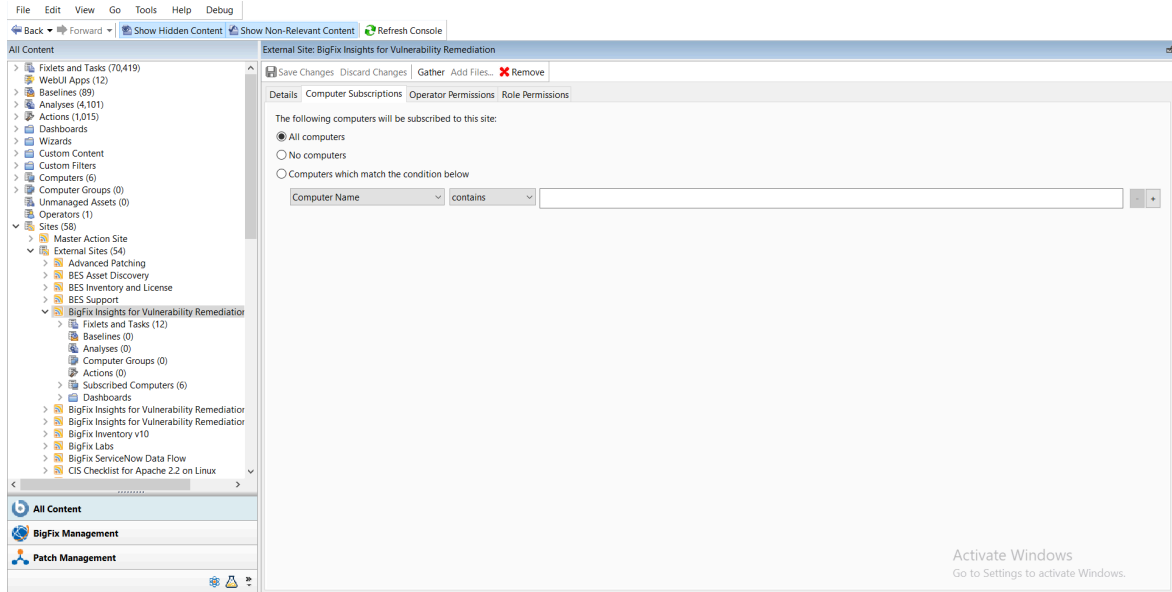
The screenshot shows the BigFix License Overview dashboard. The left sidebar contains a navigation menu with categories like Deployment Overview, License Overview, Warnings, BES Deployment Upgrade, BES Component Management, Maintenance Window Management, Manage Wake-on-LAN, Baselines, Analyses, Actions, Custom Content, Custom Filters, Computer Management, Unmanaged Assets, Operators, and Manage Sites. The main content area is titled 'BigFix License Overview' and shows a table of content sites. The 'LIFECYCLE' tab is active, and the 'BigFix Insights for Vulnerability Remediation' site is highlighted with a green box, indicating it is enabled.

ENABLED	Content Site Name	Count
ENABLED	Patches for Ubuntu 1804	0
ENABLED	Patches for Windows	19
ENABLED	Patching Support	21
ENABLED	Power Management	20
ENABLED	Remote Control	21
ENABLED	Server Automation	65
ENABLED	Software Distribution	21
ENABLED	Updates for Mac Applications	0
ENABLED	Updates for Windows Applications	19
ENABLED	Updates for Windows Applications Extended	19
ENABLED	Virtual Endpoint Manager	21
ENABLED	Vulnerability Reporting	0
ENABLED	Windows Point of Sale	0
ENABLE	BigFix Insights for Vulnerability Remediation	
ENABLE	Client Manager for Application Virtualization	
ENABLE	Client Manager for TPM/OSD	
ENABLE	MaaS360 Mobile Device Management	
ENABLE	OS Deployment	
ENABLE	Patches for CentOS 5 Native Tools (Deprecated)	
ENABLE	Patches for CentOS 6 Plugin R2	
ENABLE	Patches for CentOS 7 Plugin R2	
ENABLE	Patches for CentOS 8	

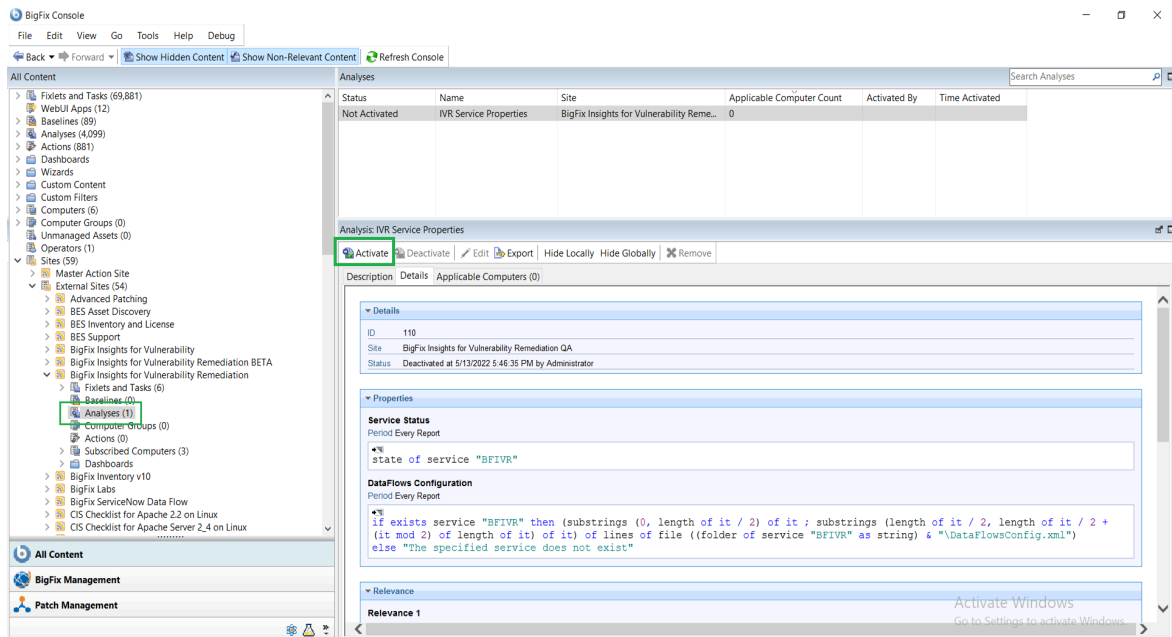


Note: Refer to the following [link](#) for more information about **License Overview** dashboard.

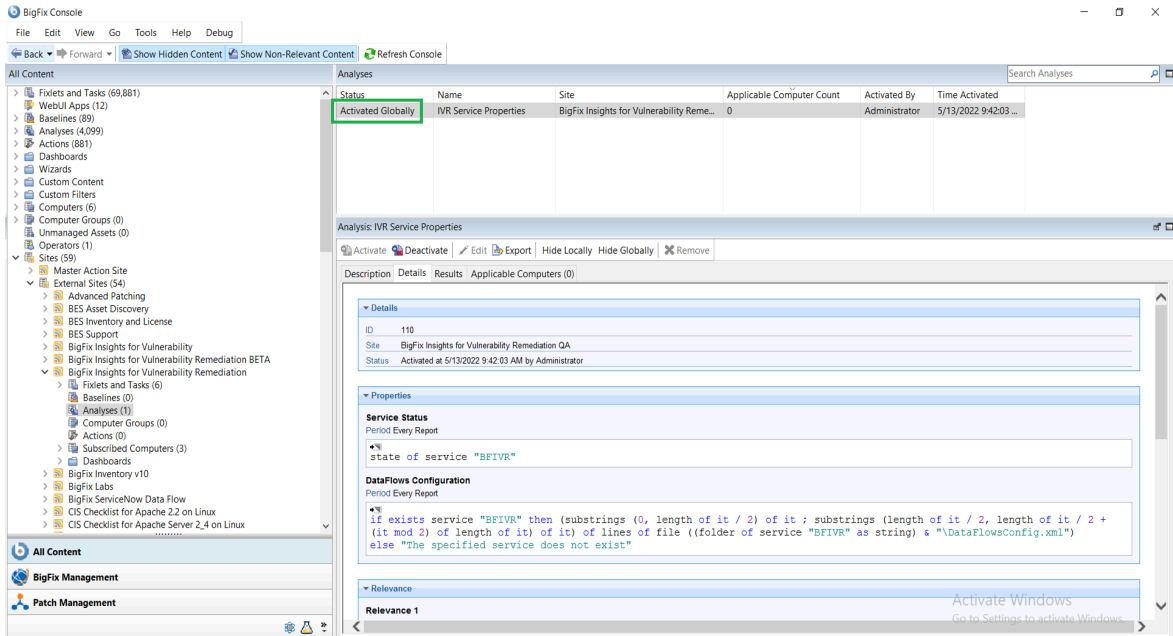
2. Subscribe computers to the site. It is recommended to subscribe to All computers. For more information on **Computer Subscriptions Tab** refer to the [link](#).




3. Activate the analysis.



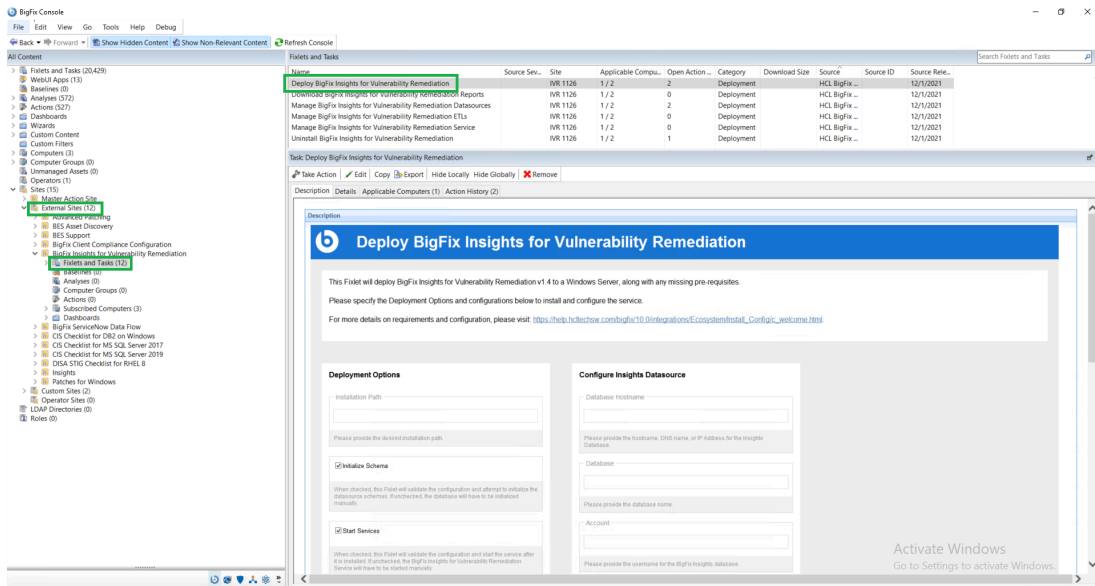
Status of the analysis should be **Activated Globally**.



 **Note:** Refer to the [link](#) to learn more about **Computer Subscriptions Tab**.

4. Deploy the solution to the target server.

a. Click **Deploy Insights for Vulnerability Remediation** Fixlet in the **BigFix Insights for Vulnerability Remediation** external site.



b. Fill in the blanks in the description panel and **Take action** to deploy the IVR services.

Please provide:

- Deployment Options
- Installation path

- Configure Insights Database
 - Database Hostname - the hostname, DNS name, or IP address for the Insights Database
 - Database - database name
 - Account - the user name for the BigFix Insights Database
 - Password - the password for the user name specified above
- Configure IVR ETL
 - Vulnerability Import Schedule - specify the desired ETL schedule for Vulnerability data. ETL schedule for Vulnerability data uses Cron Time String Format. Refer to the link to find out more about the Scheduler.
- Configure Vulnerability Management Datasource
 - specify the VM Platform
 - Connection String - the URL to the Vulnerability Management Platform
 - Account - the user name for the Vulnerability Management Platform
 - Password - the password for the user name specified above

Task Deploy BigFix Insights for Vulnerability Remediation

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (2)

Deployment Options

Installation Path

Please provide the desired installation path.

Initialize Schema

When checked, this Policy will validate the configuration and attempt to initialize the database schemas. If unchecked, the database will have to be initialized manually.

Start Services

When checked, this Policy will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for Vulnerability Remediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname

Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database

Please provide the database name.

Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the user name specified above.

Configure IVR ETL

Import Vulnerability Data into Insights

When checked, the ETL from the Vulnerability Management system to Big Fix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

Configure Vulnerability Management Datasource

VM Platform

tenableSC

Please specify the Vulnerability Management Platform

Connection String

Please provide the URI to the Vulnerability Management Platform

Account

To provide proxy details click on **Advanced Settings**. This option is not mandatory.

The screenshot shows a dialog box titled "Advanced Settings". It is divided into two main sections: "Proxy Settings for Insights Datasource" on the left and "Proxy Settings for VM" on the right. Each section contains three input fields: "Proxy Host", "Proxy User", and "Proxy Password". Below each input field is a small text prompt: "Please provide the proxy/host for Insights Datasource.", "Please provide the proxy/host URI for VM", "Please provide the proxyusername.", and "Please provide the proxypassword." respectively.



Note: Please note the following pre-requisites:

- Microsoft Visual Studio C++ Redistributable 2012: <https://www.microsoft.com/en-in/download/details.aspx?id=30679>
- Microsoft ODBC Driver 17 for SQL Server: <https://www.microsoft.com/en-us/download/details.aspx?id=56567>
 - <https://www.microsoft.com/en-us/download/details.aspx?id=56567>

The Fixlet will attempt to deploy the pre-requisites automatically.

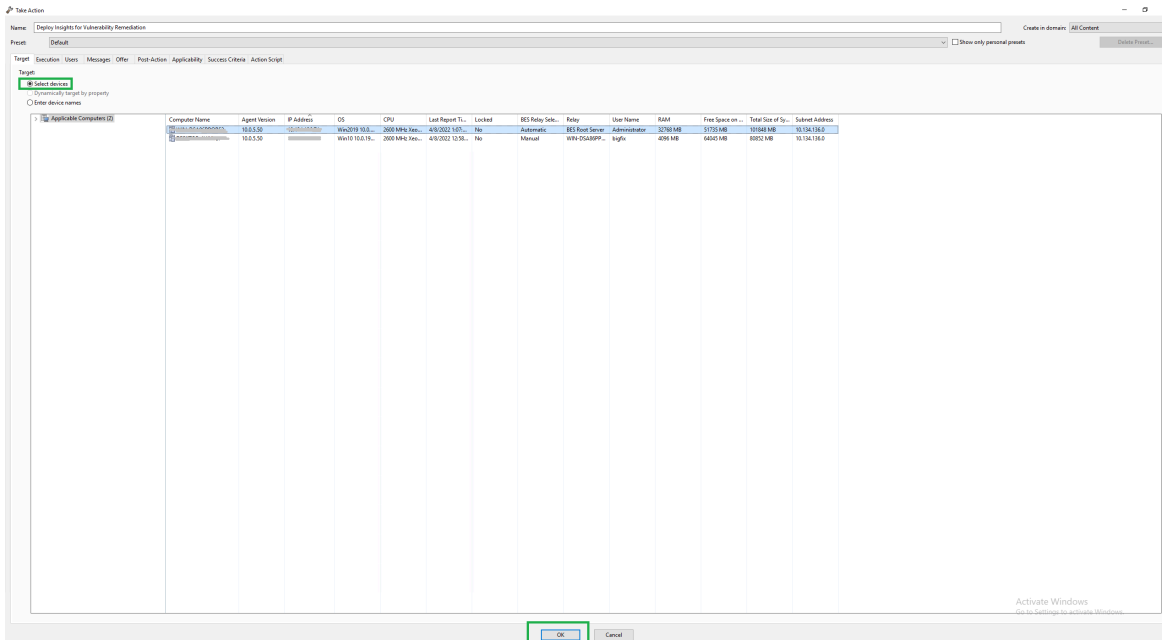


Warning: Do not deploy the BigFix Insights for Vulnerability Remediation Service to more than 1 machine.



Warning: Do not have more than 1 dataflow per IVR Service.

5. Select target devices and click **OK**.



Wait for the deployment to complete. Status should show 100% completed.

▼ Status		
100.00% Completed (1 of 1 applicable computers)		
Status	Count	Percentage
Completed	1	100.00%

- If **Start services** option was selected in the Description panel **BigFix Insights for Vulnerability Remediation** service should be present and in **Running** state in the Services. Otherwise, the **BigFix Insights for Vulnerability Remediation** service must be started manually. This indicates deployment is completed. can be checked on the log file: install.log.

Refer to the following [link](#) to learn more about other IVR Tasks.

Deployment and configuration for Qualys

This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution.

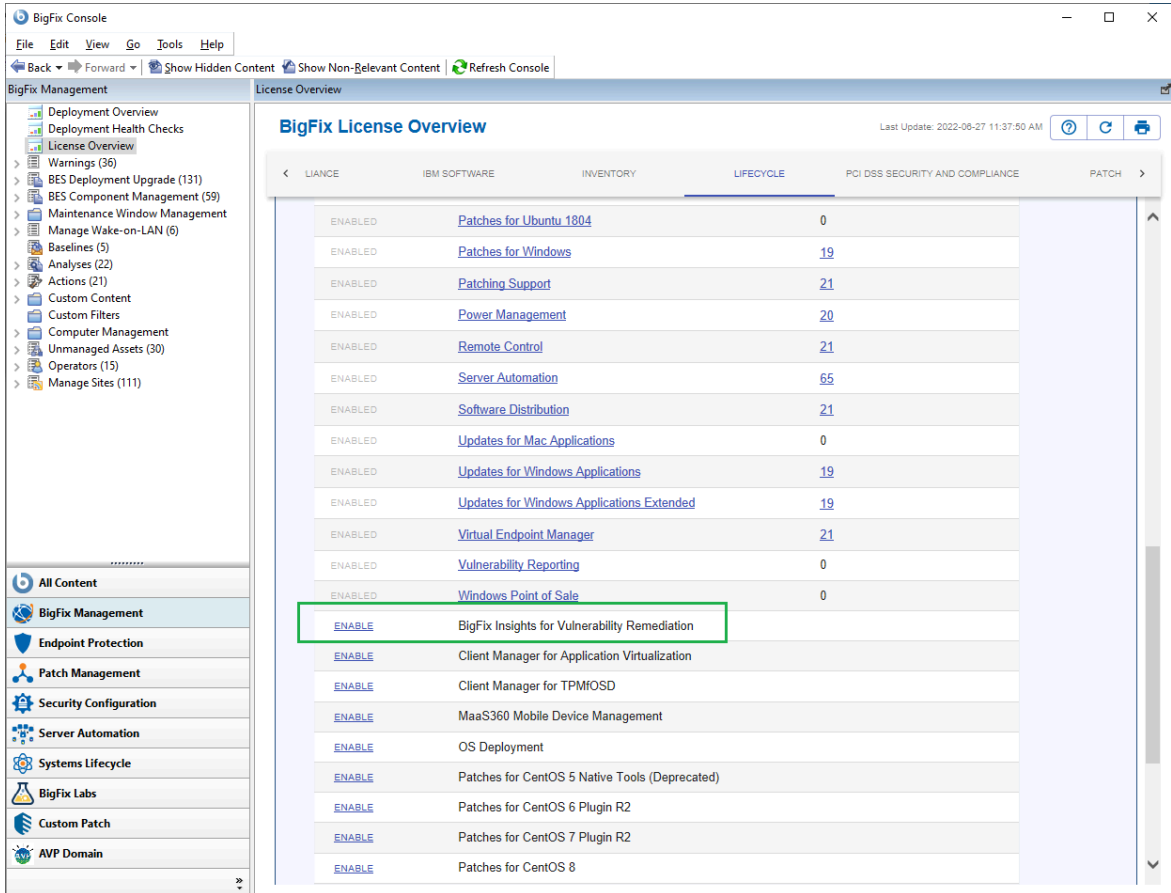
To install and configure BigFix Insights for Vulnerability Remediation service, perform below steps:



Note: To use the latest release build, the old version must be uninstalled.

1. Enable a content site.

Navigate to BigFix License Overview Dashboard. In **Compliance/Lifecycle** panel, click **Enable BigFix Insights for Vulnerability Remediation Fixlet** to gather the required content.



The screenshot shows the BigFix Console interface. The left sidebar contains a navigation menu with categories like Deployment Overview, License Overview, Warnings, BES Deployment Upgrade, BES Component Management, Maintenance Window Management, Manage Wake-on-LAN, Baselines, Analyses, Actions, Custom Content, Custom Filters, Computer Management, Unmanaged Assets, Operators, and Manage Sites. Below this is a 'All Content' section with various management tabs such as BigFix Management, Endpoint Protection, Patch Management, Security Configuration, Server Automation, Systems Lifecycle, BigFix Labs, Custom Patch, and AVP Domain.

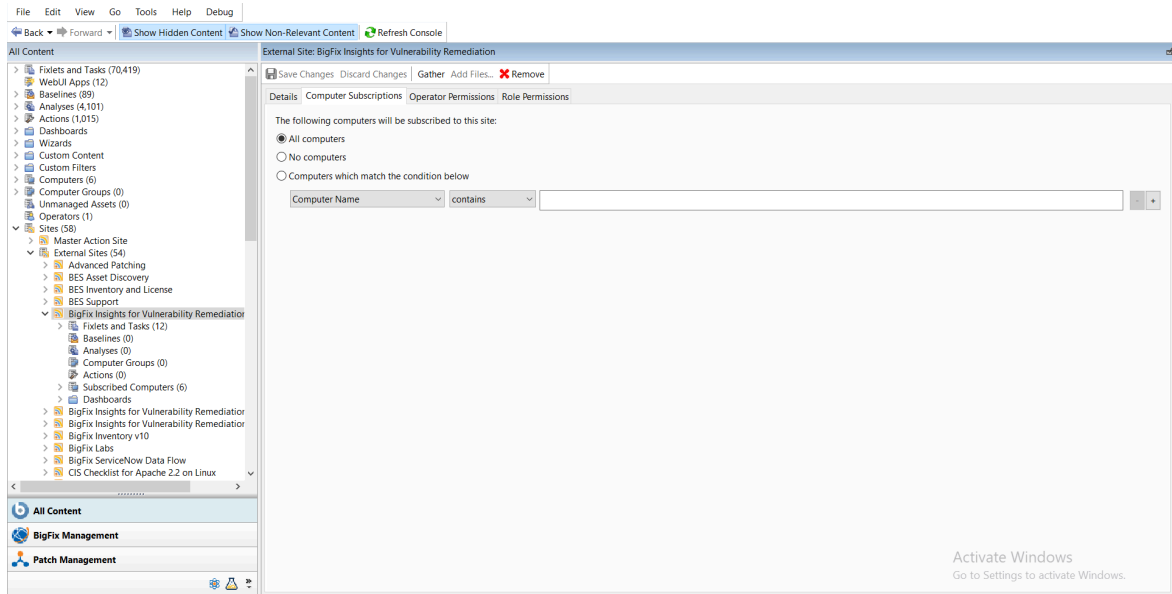
The main area displays the 'BigFix License Overview' dashboard. At the top, there are tabs for LIANCE, IBM SOFTWARE, INVENTORY, LIFECYCLE (selected), PCI DSS SECURITY AND COMPLIANCE, and PATCH. Below the tabs is a table of content sites. The table has columns for status (ENABLED), name, and a numerical value. The row for 'BigFix Insights for Vulnerability Remediation' is highlighted with a green border.

Status	Content Site Name	Value
ENABLED	Patches for Ubuntu 1804	0
ENABLED	Patches for Windows	19
ENABLED	Patching Support	21
ENABLED	Power Management	20
ENABLED	Remote Control	21
ENABLED	Server Automation	65
ENABLED	Software Distribution	21
ENABLED	Updates for Mac Applications	0
ENABLED	Updates for Windows Applications	19
ENABLED	Updates for Windows Applications Extended	19
ENABLED	Virtual Endpoint Manager	21
ENABLED	Vulnerability Reporting	0
ENABLED	Windows Point of Sale	0
ENABLE	BigFix Insights for Vulnerability Remediation	
ENABLE	Client Manager for Application Virtualization	
ENABLE	Client Manager for TPM/OSD	
ENABLE	MaaS360 Mobile Device Management	
ENABLE	OS Deployment	
ENABLE	Patches for CentOS 5 Native Tools (Deprecated)	
ENABLE	Patches for CentOS 6 Plugin R2	
ENABLE	Patches for CentOS 7 Plugin R2	
ENABLE	Patches for CentOS 8	

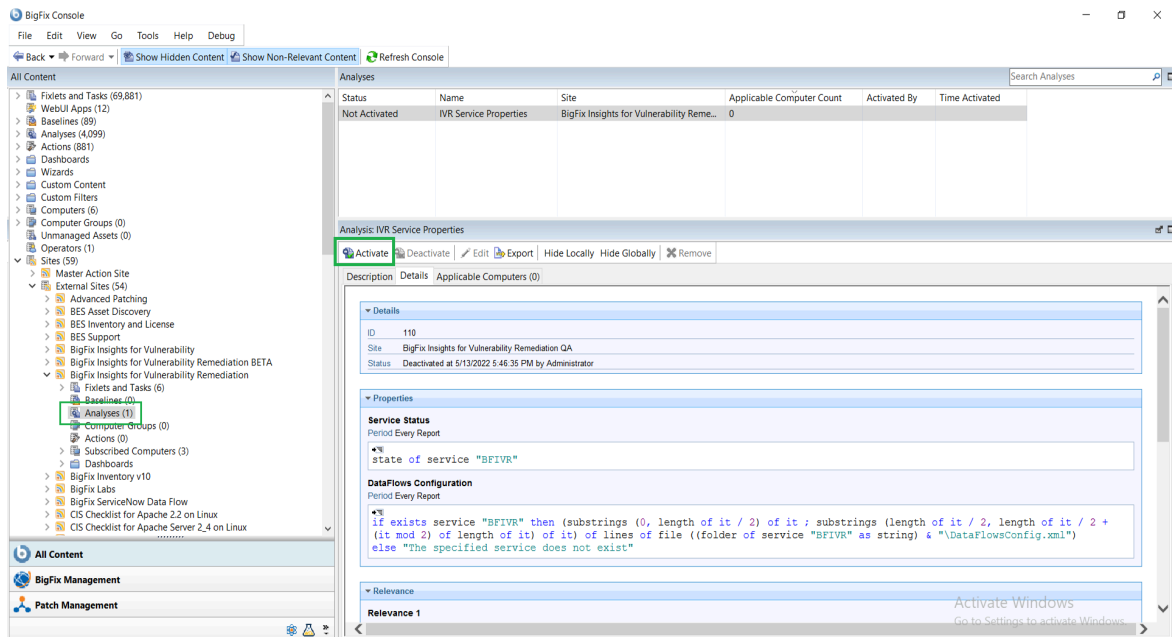


Note: Refer to the following [link](#) for more information about **License Overview dashboard**.

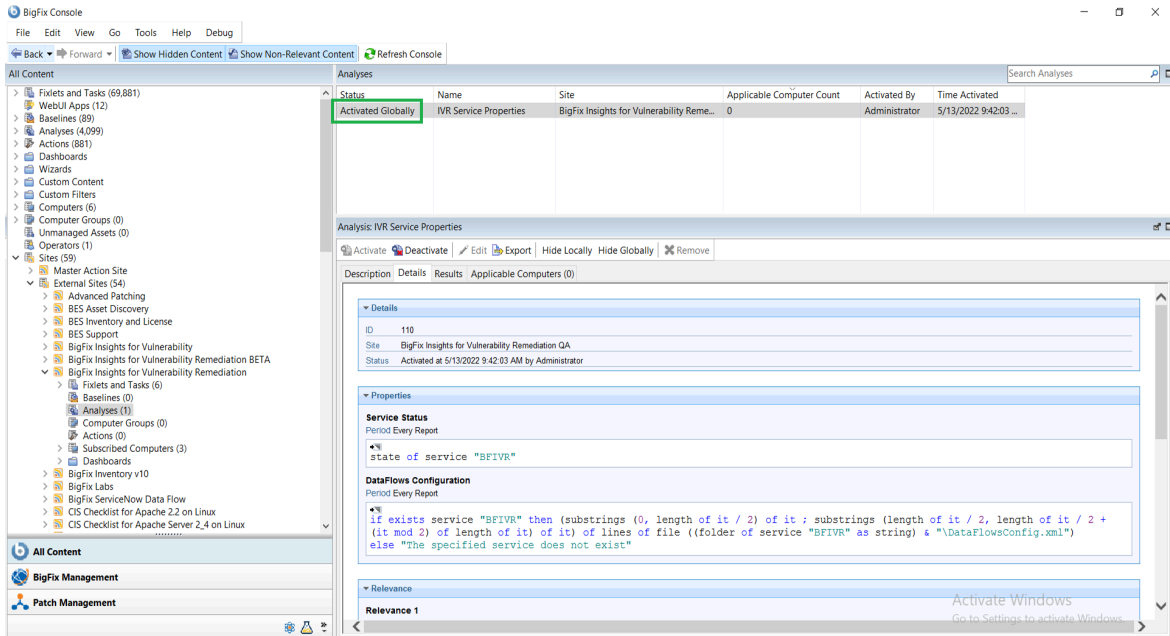
2. Subscribe computers to the site. It is recommended to subscribe to All computers. For more information on **Computer Subscriptions Tab** refer to the [link](#).




3. Activate the analysis.



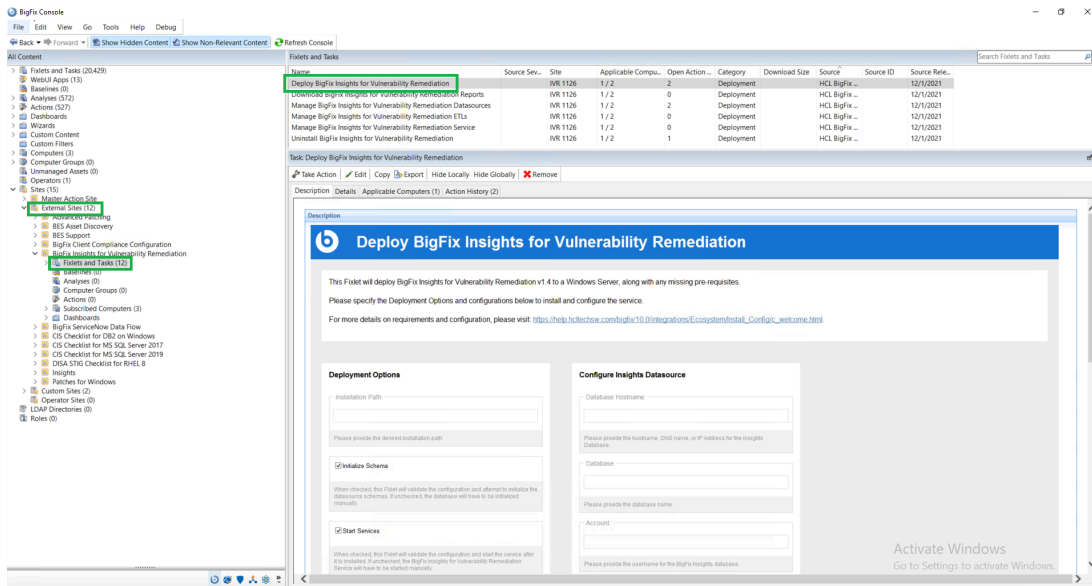
Status of the analysis should be **Activated Globally**.



 **Note:** Refer to the [link](#) to learn more about **Computer Subscriptions Tab**.

4. Deploy the solution to the target server.

a. Click **Deploy Insights for Vulnerability Remediation Fixlet** in the **BigFix Insights for Vulnerability Remediation** external site.



b. Fill in the blanks in the description panel and **Take action** to deploy the IVR services.

Please provide:

- Deployment Options:
 - Installation path

- Configure Insights Database
 - Database Hostname - the hostname, DNS name, or IP address for the Insights Database
 - Database - database name
 - Account - the user name for the BigFix Insights Database
 - Password - the password for the user name specified above
- Configure IVR ETL
 - Vulnerability Import Schedule - ETL schedule for Vulnerability data uses Cron Time String Format. Refer to the link to find out more about the Scheduler
- Configure Vulnerability Management Datasource:
 - specify the VM Platform
 - Connection String - the URL to the Vulnerability Management Platform
 - Account - the user name for the Vulnerability Management Platform
 - Password - the password for the user name specified above

Task Deploy BigFix Insights for Vulnerability Remediation

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (2)

Deployment Options

Installation Path

Please provide the desired installation path.

Initialize Schema

When checked, this Policy will validate the configuration and attempt to initialize the database schema. If unchecked, the database will have to be initialized manually.

Start Services

When checked, this Policy will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for Vulnerability Remediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname

Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database

Please provide the database name.

Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the username specified above.

Configure IVR ETL

Import Vulnerability Data Into Insights

When checked, the ETL from the Vulnerability Management system to BigFix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

Configure Vulnerability Management Datasource

VM Platform

QualysAPI

Please specify the Vulnerability Management Platform

Connection String

Please provide the URI to the Vulnerability Management Platform

Account

To provide proxy details click on **Advanced Settings**. This option is not mandatory.

The screenshot shows a dialog box titled "Advanced Settings" with two columns of proxy configuration options. The left column is titled "Proxy Settings for Insights Datasource" and the right column is titled "Proxy Settings for VM". Each column contains three input fields: "Proxy Host", "Proxy User", and "Proxy Password". Below each input field is a small grey box with a placeholder text: "Please provide the proxy/host for Insights Datasource.", "Please provide the proxy/host URI for VM", "Please provide the proxyusername.", and "Please provide the proxy password." respectively.



Note: Please note the following pre-requisites:

- Microsoft Visual Studio C++ Redistributable 2012: <https://www.microsoft.com/en-in/download/details.aspx?id=30679>
- Microsoft ODBC Driver 17 for SQL Server: <https://www.microsoft.com/en-us/download/details.aspx?id=56567>
 - <https://www.microsoft.com/en-us/download/details.aspx?id=56567>

The Fixlet will attempt to deploy the pre-requisites automatically.

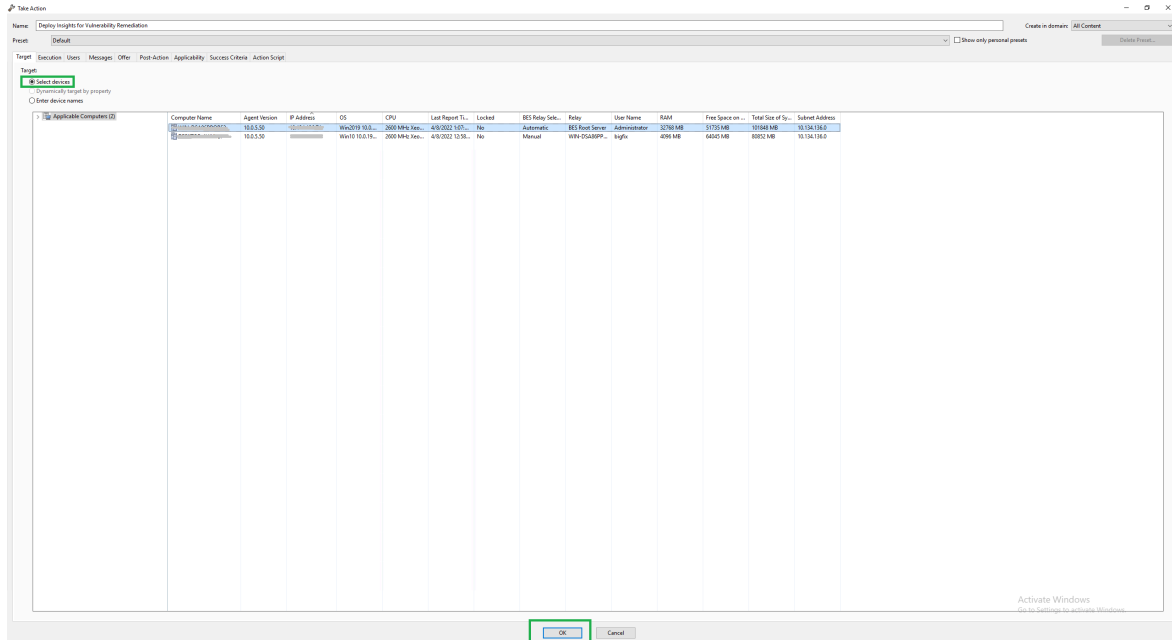


Warning: Do not deploy the BigFix Insights for Vulnerability Remediation Service to more than 1 machine.



Warning: Do not have more than 1 dataflow per IVR Service.

5. Select target devices and click **OK**. Wait for the deployment to complete.



Status should show 100% completed.

▼ Status		
100.00% Completed (1 of 1 applicable computers)		
Status	Count	Percentage
Completed	1	100.00%

- If **Start services** option was selected in the Description panel **BigFix Insights for Vulnerability Remediation** service should be present and in **Running** state in the Services. Otherwise, the **BigFix Insights for Vulnerability Remediation** service must be started manually. This indicates deployment is completed. can be checked on the log file: install.log.

Refer to the following [link](#) to learn more about other IVR Tasks.

Chapter 4. IVR Fixlets and Tasks

Learn more about available Fixlets and Tasks for BigFix Insights for Vulnerability Remediation.

[Deploy Insights for Vulnerability Remediation](#)

[Download BigFix Insights for Vulnerability Remediation Reports](#)

[Manage BigFix Insights for Vulnerability Remediation Datasources](#)

[Manage BigFix Insights for Vulnerability Remediation ETLs](#)

[Manage BigFix Insights for Vulnerability Remediation Service](#)

[Uninstall BigFix Insights for Vulnerability Remediation](#)

[Upgrade BigFix Insights for Vulnerability Remediation](#)

[Whitelist Report Download URLs of BigFix Insights for Vulnerability Remediation](#)

Deploy Insights for Vulnerability Remediation

[Tenable.io](#)

[Tenable.sc](#)

[Qualys](#)

Download BigFix Insights for Vulnerability Remediation Reports

Use this task to deploy the reports for PowerBI or Tableau platform.

BigFix Insights for Vulnerability Remediation provides business intelligence reports to address three main use cases:

- **Vulnerabilities With Available Fixlets** - A list of vulnerabilities that have matching BigFix Fixlets available for remediation. The report will list the most recent Fixlet related to each vulnerability, and the CVE entries that are associated to the vulnerability.
- **Vulnerabilities Without Available Fixlets** - A list of vulnerabilities that do not have an available Fixlet for remediation.
- **Vulnerability Discrepancies** - A list of vulnerabilities where the scanning system identifies the issue, but BigFix does not see an applicable remediation.

Reporting fixlet uses dynamic downloading. To download the report, ensure that specific URL is added in the DownloadWhitelist.txt:

- Tenable.io
 - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Tenableio.tmp
 - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Tenableio.tmp

- Tenable.sc
 - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Tenable.tmp
 - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Tenable.tmp
- Qualys
 - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Qualys.tmp
 - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Qualys.tmp

The location of the file on the BigFix server is:

`C:\Program Files (x86)\BigFix Enterprise\BES Server\Mirror Server\Config`

If the file does not exist, create a new one with the same name. The file should contain file formats such as the following:

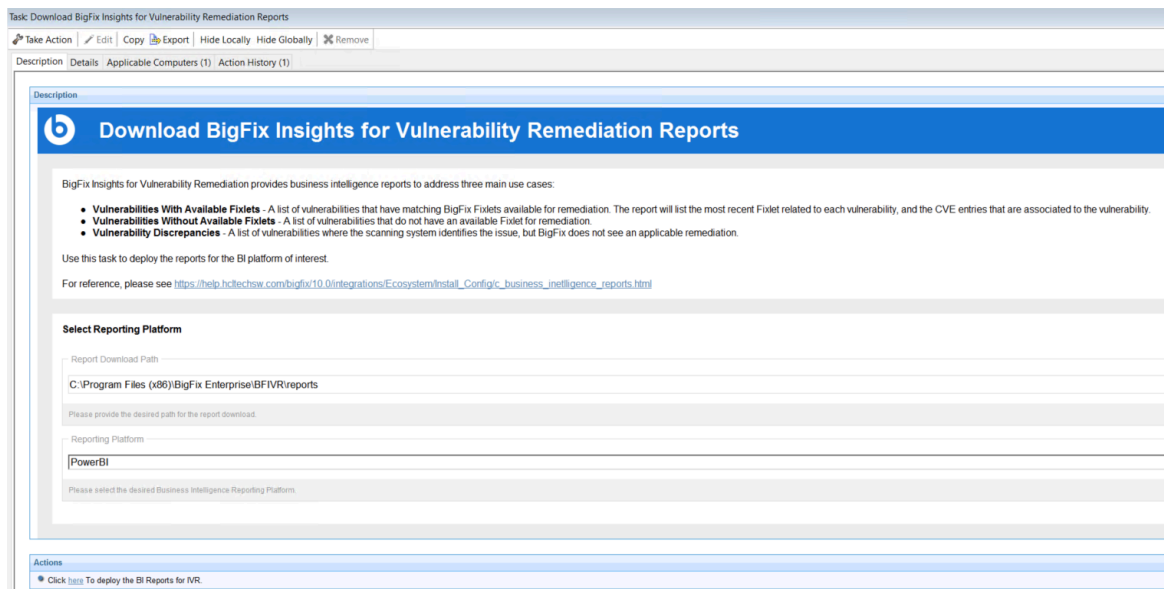
`http://127.0.0.1:52311/*.*`

`http://software.bigfix.com/*.*`

Refer to the following [link](#) to find out more about **Dynamic download White-lists**.



Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.



Manage BigFix Insights for Vulnerability Remediation Datasources

You can use this task to update the specified datasource or validate the IVR Service configuration. This task additionally provides option to specify proxy settings configuration for respective datasources.



Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.

Task: Manage BigFix Insights for Vulnerability Remediation Datasources

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

[Click here To update the specified datasource](#) y (3)
Click here To validate the IVR Service configuration.

Description

Manage BigFix Insights for Vulnerability Remediation Datasources

Use this Task to configure/re-configure the BigFix Insights for Vulnerability Remediation Datasources.

Select Datasource

<Create New Datasource>

Datasource Settings

Datasource Name
BigfixINSIGHT

Please select the datasource.

Connection String

Please specify the connection string.

Account

Please provide the user name for the datasource

Password

Please provide the password for the user specified above.

Proxy Settings

Proxy Host

Please specify the proxy host (if applicable).

Proxy User

Please specify the proxy user (if applicable).

Proxy Password

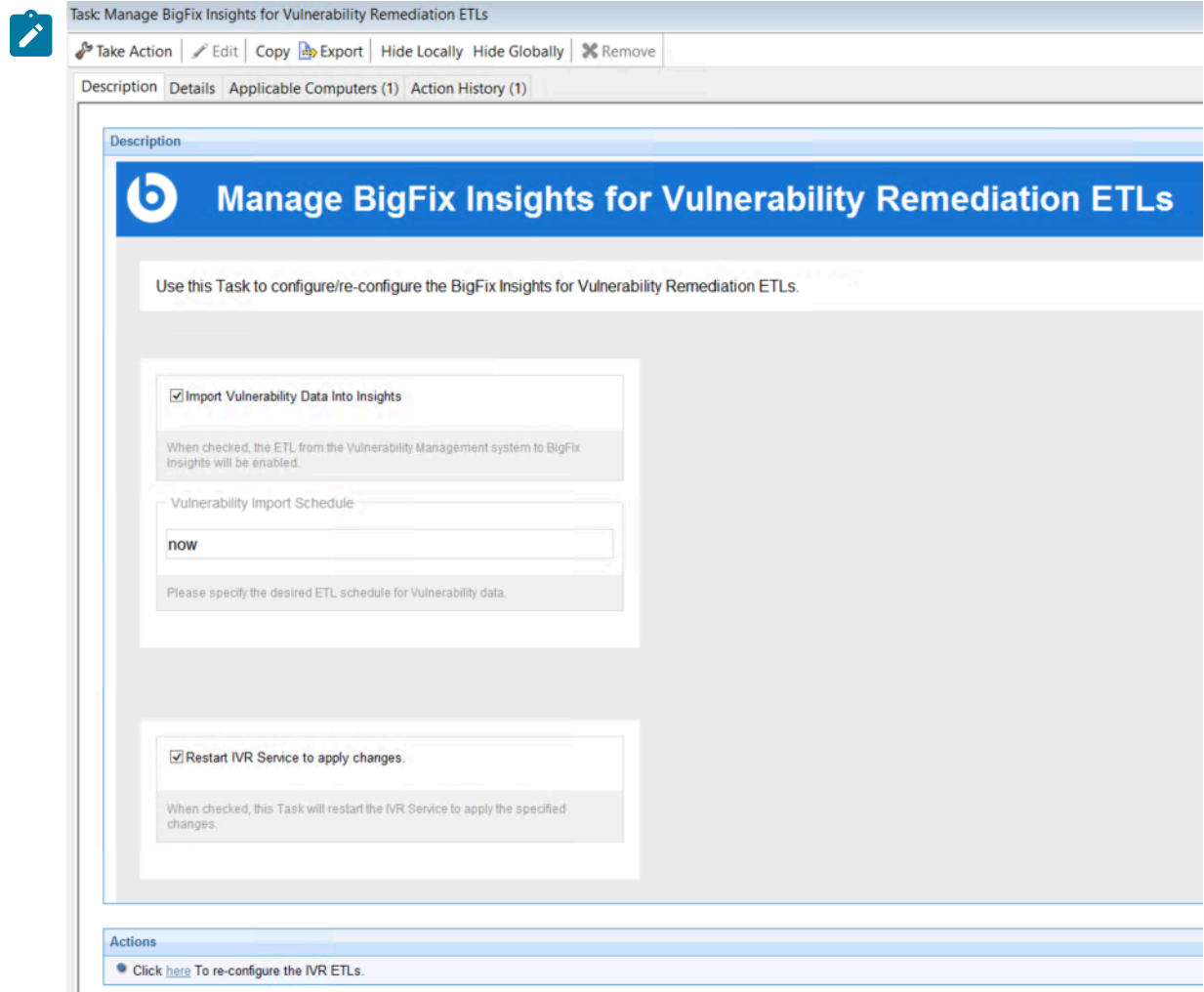
Please specify the proxy password (if applicable).

Manage BigFix Insights for Vulnerability Remediation ETLs

Use this task to configure/re-configure the BigFix Insights for Vulnerability Remediation ETLs. You can also use this fixlet to restart the IVR Service.



Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.



Task: Manage BigFix Insights for Vulnerability Remediation ETLs

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (1)

Manage BigFix Insights for Vulnerability Remediation ETLs

Use this Task to configure/re-configure the BigFix Insights for Vulnerability Remediation ETLs.

Import Vulnerability Data Into Insights

When checked, the ETL from the Vulnerability Management system to BigFix Insights will be enabled.

Vulnerability Import Schedule

now

Please specify the desired ETL schedule for Vulnerability data.

Restart IVR Service to apply changes.

When checked, this Task will restart the IVR Service to apply the specified changes.

Actions

Click [here](#) To re-configure the IVR ETLs.

Manage BigFix Insights for Vulnerability Remediation Service

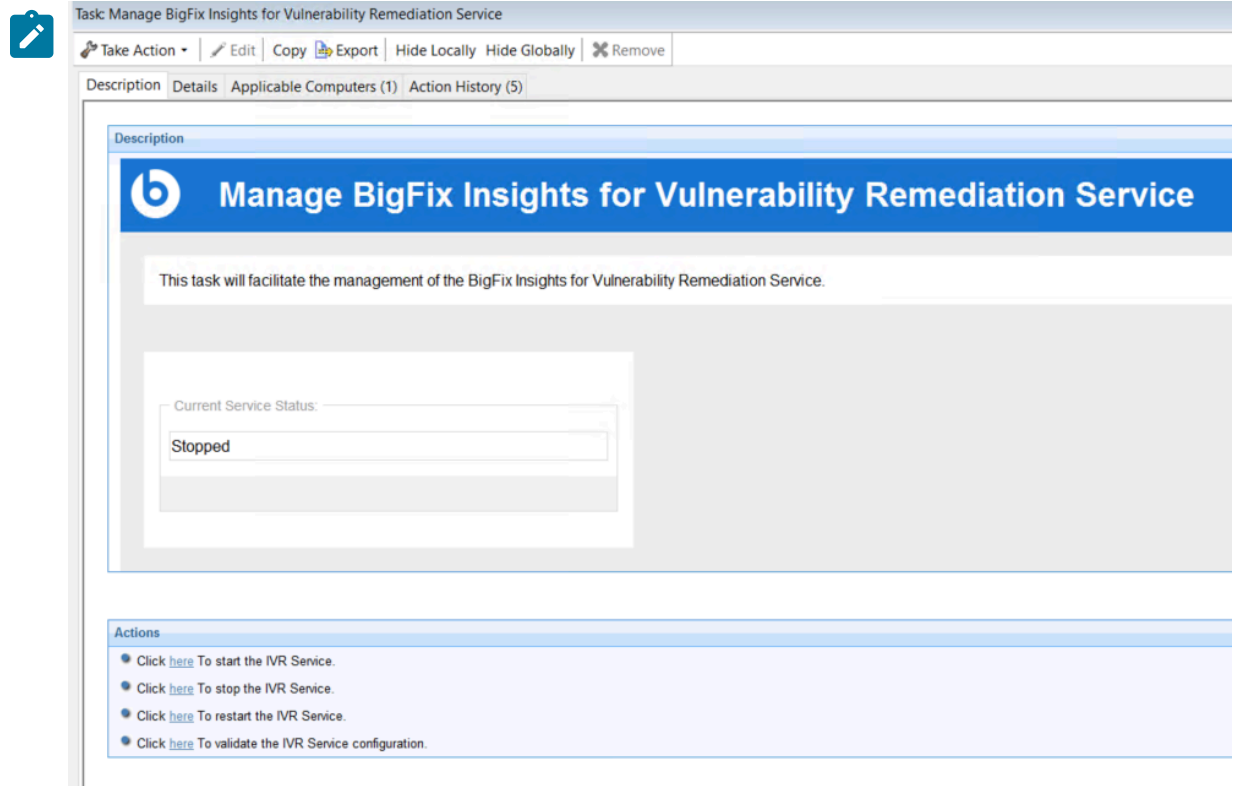
This task facilitates the management of the BigFix Insights for Vulnerability Remediation Service. You can use this task to Start, Stop, Restart or validate the configuration of the IVR Service.



Note: It is always recommended to stop the service before making any update on datasource or ETL fixlet to the already deployed service and then restart the service to apply the latest changes.



Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.



Task Manage BigFix Insights for Vulnerability Remediation Service

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (5)

Description

Manage BigFix Insights for Vulnerability Remediation Service

This task will facilitate the management of the BigFix Insights for Vulnerability Remediation Service.

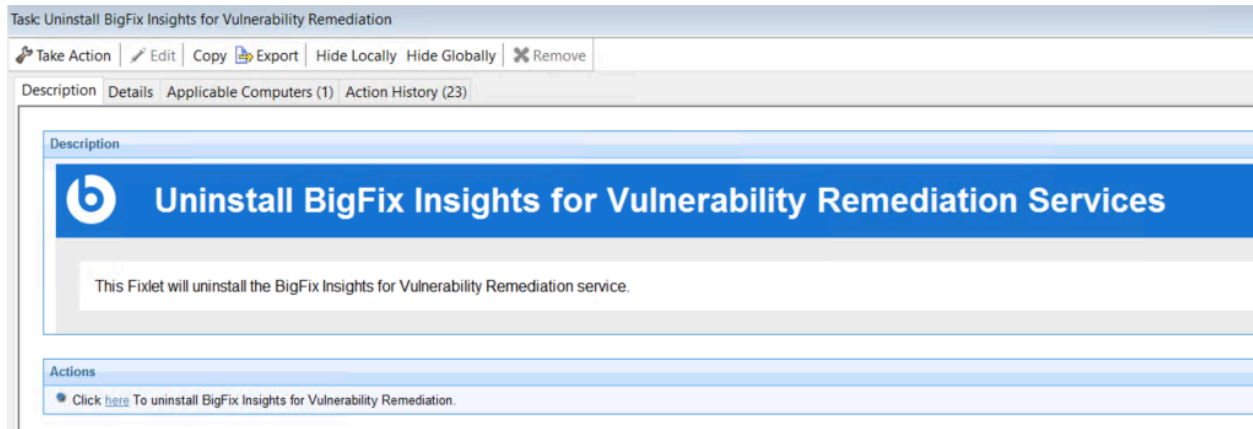
Current Service Status: Stopped

Actions

- Click [here](#) To start the IVR Service.
- Click [here](#) To stop the IVR Service.
- Click [here](#) To restart the IVR Service.
- Click [here](#) To validate the IVR Service configuration.

Uninstall BigFix Insights for Vulnerability Remediation

This Fixlet uninstalls the BigFix Insights for Vulnerability Remediation service.



Task Uninstall BigFix Insights for Vulnerability Remediation

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (23)

Description

Uninstall BigFix Insights for Vulnerability Remediation Services

This Fixlet will uninstall the BigFix Insights for Vulnerability Remediation service.

Actions

- Click [here](#) To uninstall BigFix Insights for Vulnerability Remediation.

Upgrade BigFix Insights for Vulnerability Remediation

The Fixlet will upgrade the BigFix Insights for Vulnerability Remediation service.

ID	Name	Source Sev...	Site	Applicable Compute...	Unlocked C...	Open Actio...	Category	Download ...	Source
4401	Manage BigFix Insights for Vulnerability Remediation Service		ivr	1 / 2	1 / 2	0	Deployment		HCL Bi
4400	Uninstall BigFix Insights for Vulnerability Remediation		ivr	1 / 2	1 / 2	0	Deployment		HCL Bi
4406	Upgrade BigFix Insights for Vulnerability Remediation		ivr	1 / 2	1 / 2	1	Deployment		HCL Bi
4405	Whitelist Report Download URLs of BigFix Insights for Vulnerability Remediation		ivr	1 / 2	1 / 2	0	Deployment		HCL Bi

Task Upgrade BigFix Insights for Vulnerability Remediation

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (1)

Upgrade BigFix Insights for Vulnerability Remediation

This Fixlet will Upgrade the BigFix Insights for Vulnerability Remediation service.

Provide Insights Credential for Schema Initialization

Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the user name specified above.



Note: Before you install the Fixlet, go to **Success Criteria** tab and select **all lines of the action script have completed**

Take Action

Name: Upgrade BigFix Insights for Vulnerability Remediation

Preset: Default

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

Consider this action successful when...

...the applicability relevance evaluates to false.

...all lines of the action script have completed successfully.

...the following relevance clause evaluates to false:

OK Cancel

successfully.

Whitelist Report Download URLs of BigFix Insights for Vulnerability Remediation

This Fixlet whitelists the dynamic download report URLs specific to each vendor of BigFix Insights for Vulnerability Remediation

The screenshot shows a configuration window for a task titled "Whitelist Report Download URLs of BigFix Insights for Vulnerability Remediation". The window has a title bar with the task name and a close button. Below the title bar is a menu bar with options: "Take Action", "Edit", "Copy", "Export", "Hide Locally", "Hide Globally", and "Remove". Underneath the menu bar is a tabbed interface with "Description", "Details", "Applicable Computers (0)", and "Action History (0)". The "Description" tab is active, showing a blue header with the BigFix logo and the task title. Below the header is a text box containing the description: "This Fixlet whitelists the dynamic download report URLs specific to each vendor of BigFix Insights for Vulnerability Remediation service." Below the description is an "Actions" section with three bullet points: "Click [here](#) to whitelist Qualys report URLs", "Click [here](#) to whitelist TenableSC report URLs.", and "Click [here](#) to whitelist TenableIO report URLs."

service.

Notices

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

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

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

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

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

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

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

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

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

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

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

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

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

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

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

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

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

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

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

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

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

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

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

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

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

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