# BigFix Integrated Vulnerability Remediation (IVR) v.5

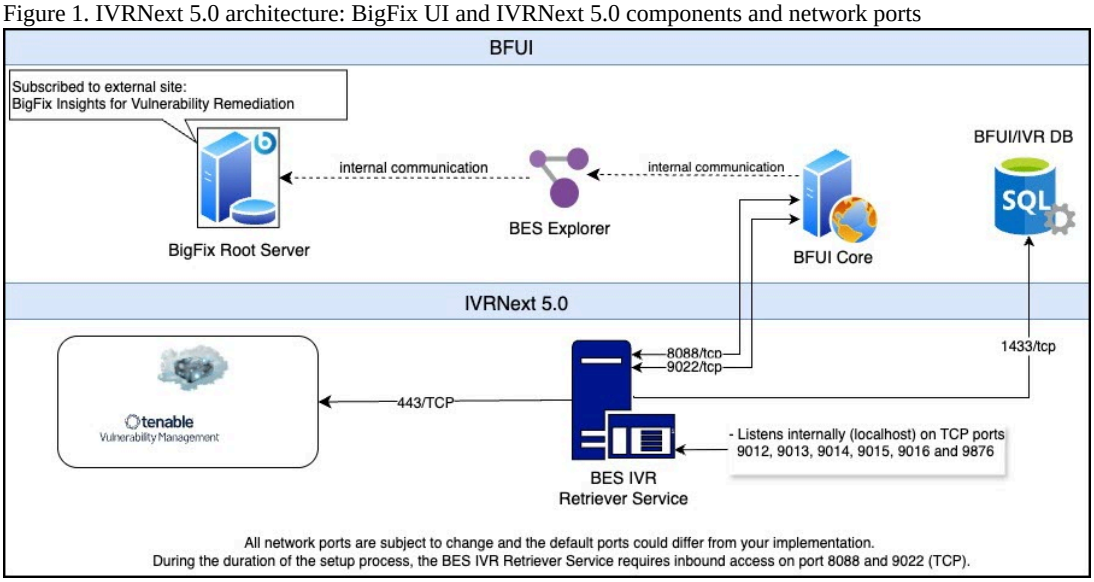
# Contents

**Chapter 1. Product overview** ..... **3**
**Chapter 2. System requirements** ..... **5**
**Chapter 3. IVR v.5 Fixlets and Tasks** ..... **8**
**Chapter 4. IVR v.5 setup process** ..... **14**
**Chapter 5. IVR on-prem Start Process** ..... **22**
**Chapter 6. Managing the IVR configuration** ..... **23**
**Chapter 7. IVR v.5 on BFUI** ..... **28**
**Chapter 8. Configuration settings for IVR on-prem** ..... **46**
**Chapter 9. IVR logs** ..... **47**
**Chapter 10. Troubleshooting** ..... **48**
**Chapter 11. Release notes** ..... **49**
**Chapter 12. Known limitations** ..... **50**
**Chapter 13. References** ..... **51**

# Chapter 1. Product overview

IVR v.5 connects vulnerability detection to remediation. It retrieves vulnerability findings from your scanner, matches them with BigFix Fixlets and devices, and lets you deploy the fix from the same screen where you review the finding. You do all of this in the BigFix UI.

Figure 1. IVRNext 5.0 architecture: BigFix UI and IVRNext 5.0 components and network ports




### How IVR v.5 works

IVR v.5 has two layers: the BigFix UI layer, which you already run, and the IVRNext 5.0 layer, which the Download Task adds.

| Component | Layer | Role in IVR |
|---|---|---|
| BigFix Root Server | BigFix UI | Subscribed to the BigFix Insights for Vulnerability Remediation external site. It provides the Fixlet content and device data, and runs the remediation actions. |
| BES Explorer | BigFix UI | Connects the BigFix UI to the BigFix Root Server. |
| BFUI Core | BigFix UI | Hosts the **Integrated Vulnerability Remediation** application, the configuration wizard, and remediation. It communicates with the BigFix Root Server through BES Explorer. |
| BFUI DB | BigFix UI | The SQL Server database of the BigFix UI. IVR stores its data in an IVR schema in this database. |
| BES IVR Retriever Service | IVRNext 5.0 | Retrieves vulnerability findings from Tenable, correlates them with BigFix Fixlets and devices, and writes the results to the IVR schema. |
| Tenable Vulnerability Management | External | The vulnerability scanner that provides findings and assets. |

#### End-to-end workflow

1. **Install.** You enable the BigFix Insights for Vulnerability Remediation site and deploy the Download Task. The BES IVR Retriever Service is installed and starts automatically. See IVR v.5 Fixlets and Tasks *(on page 8)*.
2. **Register.** On the BigFix UI server, you run `BFUI.exe --configure-ivr` to register the IVR Retriever with the BigFix UI. You enter the IVR server address, the basic authentication and mTLS ports (defaults 8088 and 9022), and the IVR user credentials from the Download Task. See Task 1: Register IVR with the BigFix UI *(on page 14)*.
3. **Configure.** In **Administration** > **Application Configuration**, you enter the BFUI database, application, and Tenable data source settings. IVR creates its schema in the BFUI DB. See Task 2: Configure IVR in Application Configuration *(on page 15)*.
4. **Retrieve and correlate.** The IVR Retriever pulls findings from Tenable over port 443 and correlates them with BigFix content and devices. It stores the results in the BFUI DB over port 1433. This automation runs every 12 hours by default.
5. **Review.** In **Resolve** > **Integrated Vulnerability Remediation**, you review vulnerabilities by vulnerability or by device. See IVR v.5 on BFUI *(on page 28)*.
6. **Remediate.** You deploy the correlated Fixlets from the BigFix UI. The deployment reaches the BigFix Root Server through BES Explorer, and the Root Server runs it on the target devices.

IVR v.5 keeps the core capabilities of IVR v.4:

- **Vulnerability-to-remediation correlation.** IVR correlates scanner findings with BigFix content through a rule-based system. The system uses scanner plugin attributes as well as CVE IDs. The BigFix team maintains a continuously updated, pre-correlated map from scanner plugins to BigFix Fixlets.
- **Asset correlation.** IVR matches scanner assets with BigFix devices through unique scanner asset identifiers rather than IP addresses, MAC addresses, or host names. Correlation therefore stays accurate for virtual machines and devices with dynamic or multiple network connections.
- **Reduced infrastructure.** The IVR Retriever service runs independently of BigFix Insights, so you don't need the Insights database or ETL configuration.

## What's new in IVR v.5

| Area | IVR v.4 | IVR v.5 |
|---|---|---|
| User interface | BigFix WebUI IVR app, opened from the Apps menu | Integrated Vulnerability Remediation in the BigFix UI, opened from the left navigation pane under **Resolve** |
| Setup | `ivrNext.exe --setup` command and the IVR Configuration Manager page | `BFUI.exe --configure-ivr` registration command on the BigFix UI server, followed by the configuration wizard in **Administration** > **Application Configuration** |
| Database | A dedicated database or schema that you create during setup | An IVR schema created in the existing BigFix UI database |
| Server configuration | Entered on the setup page | Entered once in the `--configure-ivr` command, and shown read-only in the BigFix UI |
| Starting the service | Manual start after setup | Starts automatically after installation with the Download Task |
| Access control | WebUI permissions | BigFix UI roles in **Administration** > **Identity and Access** |
| Device view | WebUI Device Centric view | **Device view** tab, with grid search and links to **Device Explorer** |
| Automation status | Log entry "Automation completed" | **Last Automation Run** and **Next Expected Automation Run** shown on the dashboard |
| Configuration reset | `ivrNext.exe --reset` | Not applicable. Change the configuration in the BigFix UI. |

# Chapter 2. System requirements

Learn about the prerequisites, system requirements, network ports, and platform dependencies for the BigFix IVR v.5 Retriever service.

### Software requirements

| Category | Details |
|---|---|
| BigFix component requirements | BigFix UI (BFUI) installed and running, with access to its database. See System Requirements and Installation in the BigFix UI Administration Guide. |
| Prerequisites | Microsoft SQL Server 2025, used by the BigFix UI database. |
| Operating system | Microsoft Windows Server 2016, 2019, 2022, or 2025 |
| Supported BigFix versions | Windows-based BigFix Server, version 11.0.7.61 or later.<br><br>**Note:** The BigFix IVR Retriever service does not support BigFix Server environments that are not based on Windows. |
| BigFix license requirements | BigFix Remediate, BigFix Lifecycle, BigFix Compliance, BigFix Workspace or Workspace+, or BigFix Enterprise or Enterprise+ |
| Supported vulnerability management platforms | Tenable Vulnerability Management (formerly Tenable.io), selected as **Tenable VM** in the BigFix UI.<br><br>**Note:** IVR v.5 supports only Tenable Vulnerability Management.<br><br>**Note:** You need an administrator user role in Tenable to generate the API keys that IVR uses. |
| Network requirements | **BES IVR Retriever Service (IVR host):**<br><br>• Inbound from BFUI Core on port 8088 (basic authentication) and port 9022 (mTLS).<br>• Outbound to Tenable Vulnerability Management on port 443. You can route this connection through an HTTP or HTTPS proxy server.<br>• Outbound to the BFUI DB (SQL Server) on port 1433.<br>• Listens internally (localhost only) on ports 9012, 9013, 9014, 9015, 9016, and 9876. These ports don't need firewall rules, but no other application can use them.<br><br>**BigFix UI:** BFUI Core communicates with the BigFix Root Server through BES Explorer. The IVR Retriever doesn't connect to the BigFix Root Server directly. |

| Category | Details |
|---|---|
| | **Note:** All ports are TCP. Ports can change, and your defaults can differ from this implementation. |
| System limitations | IVR v.5 supports one scanner data source per IVR instance. |

## Hardware requirements

| Hardware | IVR Retriever (Tenable) |
|---|---|
| CPU | Minimum 2 cores (4 cores recommended) |
| RAM | In addition to the host operating system requirements: 2 GB per 20,000 endpoints |
| Disk space | With default settings: 4 GB per 20,000 endpoints |
| Execution time | The time that data synchronization and processing take depends on CPU speed, the number of findings, the number of assets, the number of patch sites loaded in your BigFix environment, API latency, and other workloads on the IVR computer. |

## Deployment prerequisites

All IVR deployment prerequisites are documented here. The BigFix UI documentation summarizes IVR and links to this guide: see Integrated Vulnerability Remediation in the BigFix UI User's Guide.

- **Backend:** a Windows computer for the BES IVR Retriever Service. It can be the BigFix UI server or a separate computer, and it must meet the Hardware requirements *(on page 6)* and the network requirements in Software requirements *(on page 5)*.
- **Database:** the BigFix UI database on Microsoft SQL Server 2025, and a database user with permission to create a schema in it. IVR creates its own schema in this database.
- **BigFix:** the BigFix Insights for Vulnerability Remediation site and the IVR Vulnerability Scanner Host ID analysis. See Before you begin *(on page 8)*.

When the prerequisites are in place, Install the BigFix IVR Retriever *(on page 9)* and complete the IVR v.5 setup process *(on page 14)*.

## Moving from IVR v.4

**Important:** If an earlier version of IVR is installed in your environment, uninstall it before you install IVR v.5.

To move to IVR v.5 from an earlier version, uninstall the earlier version first, and then install and set up IVR v.5 as a new installation.

**CAUTION:** Uninstalling the earlier version removes its IVR Retriever folder, service, and configuration. Back up the installation folder and record your data source settings before you start.

1. In the BigFix Console, open the **BigFix Insights for Vulnerability Remediation** site, and then go to **Fixlets and Tasks**.
2. Uninstall the earlier version:

- **IVR v.4:** Select the **Uninstall BigFix IVR Retriever v4** Fixlet, and then follow steps 2-5 of Uninstall the BigFix IVR Retriever *(on page 13)*.
- **IVR v.2 or v.3:** Select the **Uninstall BigFix Insights for Vulnerability Remediation** Task, and then click **Take Action**. After the service is removed, delete the IVR schema from SQL Server. For the SQL query, see Uninstall the BigFix IVR Retriever *(on page 13)*.

3. Confirm the removal as described in the uninstall results. See Uninstall the BigFix IVR Retriever *(on page 13)*.
4. Install IVR v.5. See Install the BigFix IVR Retriever *(on page 9)*.
5. Set up IVR v.5. See IVR v.5 setup process *(on page 14)*.

**Note:** IVR v.5 stores its data in a new schema in the BigFix UI database, and you configure it from scratch in the BigFix UI. The earlier version's configuration isn't reused.

### Where each step runs

| Step | Runs on | Account you need |
|---|---|---|
| Enable the site, and deploy the Download and Uninstall Tasks | Computer that runs the BigFix Console | BigFix operator who can manage external sites and take actions |
| BES IVR Retriever Service | Target computer that you select in the Download Task (the IVR host) | — |
| `BFUI.exe --configure-ivr` | BigFix UI server | Local Windows administrator, plus the BigFix UI instance admin |
| Grant IVR access, run the configuration wizard | Any browser that can reach the BigFix UI | BigFix UI administrator |

You can install the IVR Retriever on the BigFix UI server or on a separate computer. If you use a separate computer, open the inbound and outbound ports listed in Network requirements in the firewalls between the computers. In Task 1 *(on page 14)*, enter the IVR host IP address and include it in the IP SANs.

# Chapter 3. IVR v.5 Fixlets and Tasks

Learn about the Fixlets and Tasks that install and uninstall the BigFix IVR Retriever for IVR v.5.

The **BigFix Insights for Vulnerability Remediation** site provides two Tasks:

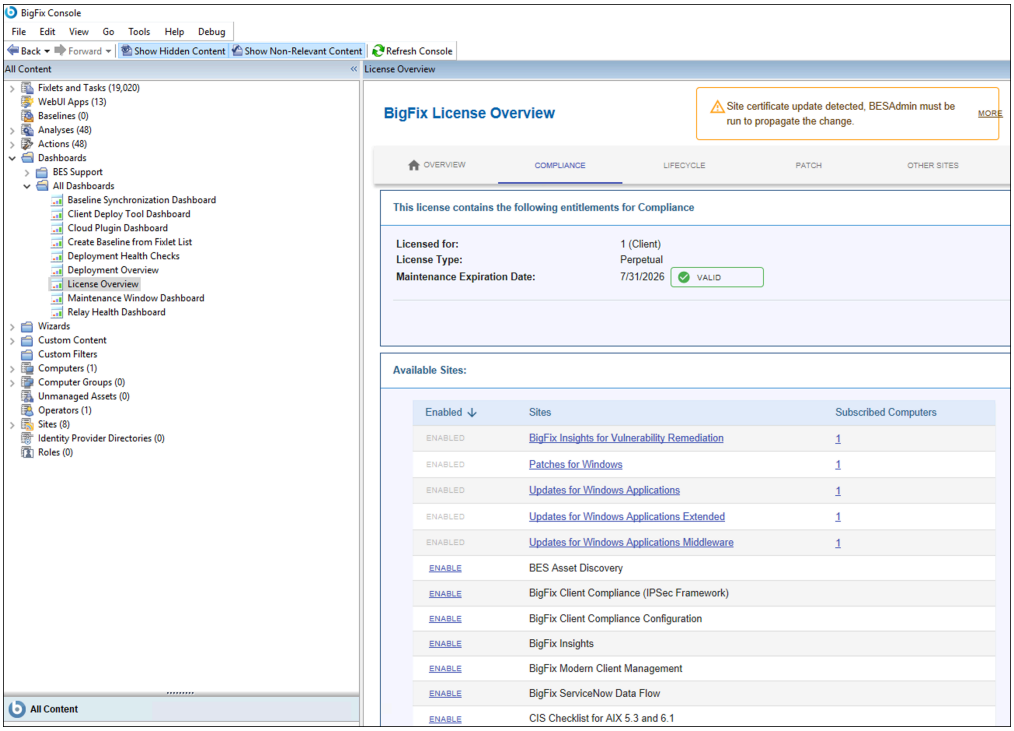
- **Download BigFix IVR Retriever v5.0.0.0**: installs the IVR Retriever service on the target computer.
- **Uninstall BigFix IVR Retriever v5**: removes the IVR Retriever service and its components from the target computer.

**Important:** Before you run either Task, close all Command Prompt windows, files, folders, and applications on the target computer. Open handles cause file-locking conflicts.

## Before you begin

1. Enable the **BigFix Integrated Vulnerability Remediation** site.
   In the BigFix Console, open the **BigFix License Overview** dashboard, and then, in the **Compliance/Lifecycle** panel, select **Enable** for the **BigFix Integrated Vulnerability Remediation** site. See License Overview dashboard.

   Figure 2. BigFix License Overview dashboard



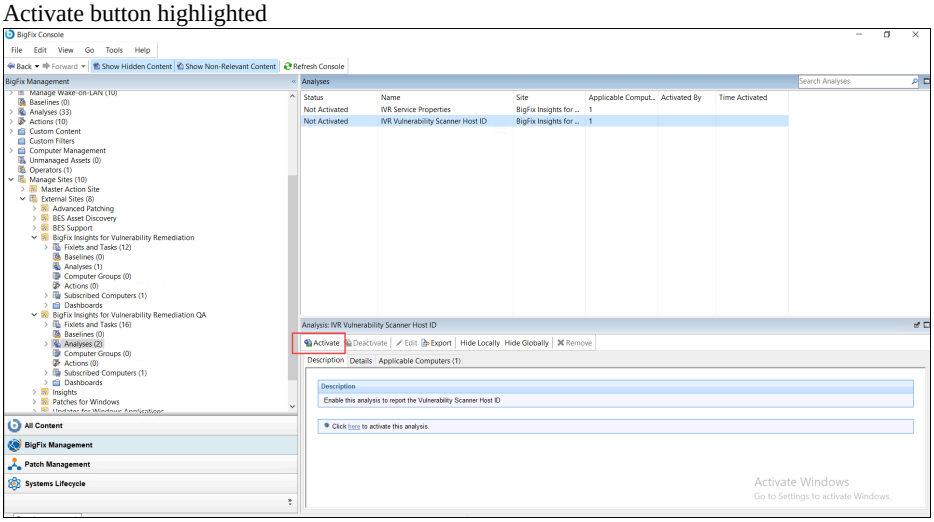

2. Subscribe computers to the site.
   We recommend that you subscribe **All computers**. See Restricting Computers (site **Computer Subscriptions** tab).
3. Confirm that the site is gathered.
   Under **Sites** > **External Sites**, check that the site version is greater than **0**. Until the version is greater than 0, IVR doesn't appear in the BigFix UI.
4. Activate the **IVR Vulnerability Scanner Host ID** analysis globally.
   IVR uses this analysis to collect the asset data that correlates scanner assets with BigFix devices. Until you activate it, IVR can't match Tenable findings to your devices.

a. In the BigFix Console, go to **Sites** > **External Sites** > **BigFix Insights for Vulnerability Remediation** > **Analyses**.

b. Select **IVR Vulnerability Scanner Host ID**. Its status shows **Not Activated** until you activate it.

c. Click **Activate**, and make sure that it is activated globally.

Figure 3. BigFix Console Analyses list for the BigFix Insights for Vulnerability Remediation site, with the IVR Vulnerability Scanner Host ID analysis selected, status Not Activated, and the Activate button highlighted



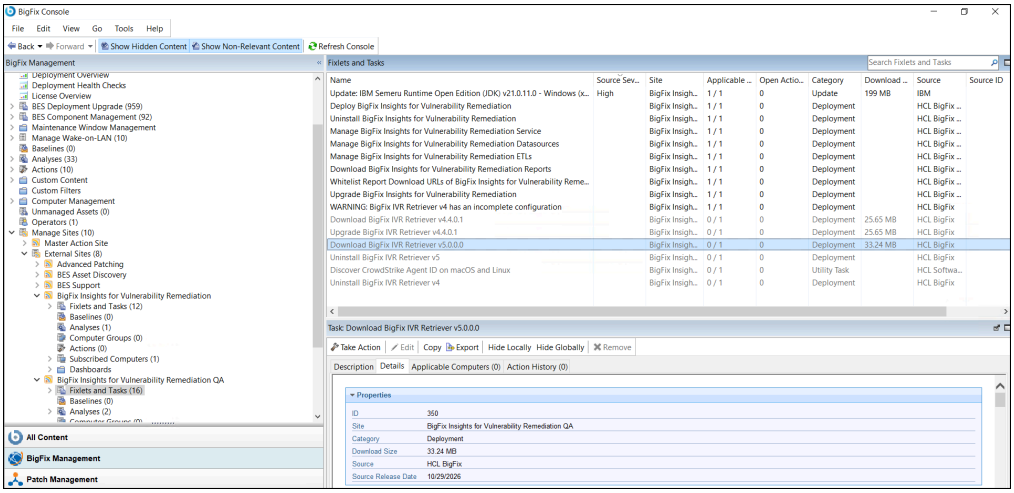

5. Confirm that the target computer (the IVR host) runs the BigFix Client, is subscribed to the site, and meets the system requirements *(on page 5)*.

# Install the BigFix IVR Retriever

This task describes how to install the BigFix IVR Retriever on the computer that will host IVR by using the **Download BigFix IVR Retriever v5.0.0.0** Task.

1. In the BigFix Console, go to **BigFix Insights for Vulnerability Remediation** > **Fixlets and Tasks**, and then select **Download BigFix IVR Retriever v5.0.0.0**.

   Figure 4. BigFix Console showing the BigFix Insights for Vulnerability Remediation site, Fixlets and Tasks list, with Download BigFix IVR Retriever v5.0.0.0 selected



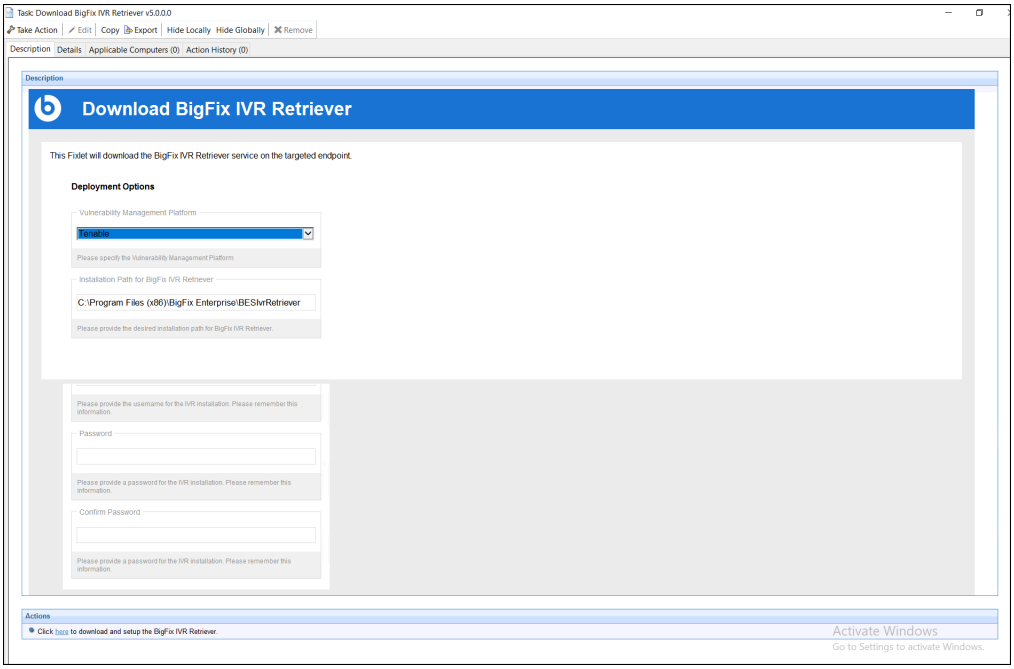

2. On the **Description** tab, under **Deployment Options**, set the following fields.

| Field | Description |
|---|---|
| Vulnerability Management Platform | Select **Tenable**. IVR v.5 supports Tenable only. |
| Installation Path for BigFix IVR Retriever | The folder where the IVR Retriever is installed. The default is `C:\Program Files (x86)\BigFix Enterprise\BESIvrRetriever`. |

3. Under **Configure IVR User Credentials**, enter a **Username**, a **Password**, and the same password again in **Confirm Password**.

**Important:** Record the IVR user credentials in your password vault. You enter them as the **IVR Admin Username** and **IVR Admin Password** when you register IVR with the BigFix UI.

Figure 5. Download BigFix IVR Retriever v5.0.0.0 Description tab showing Deployment Options and Configure IVR User Credentials

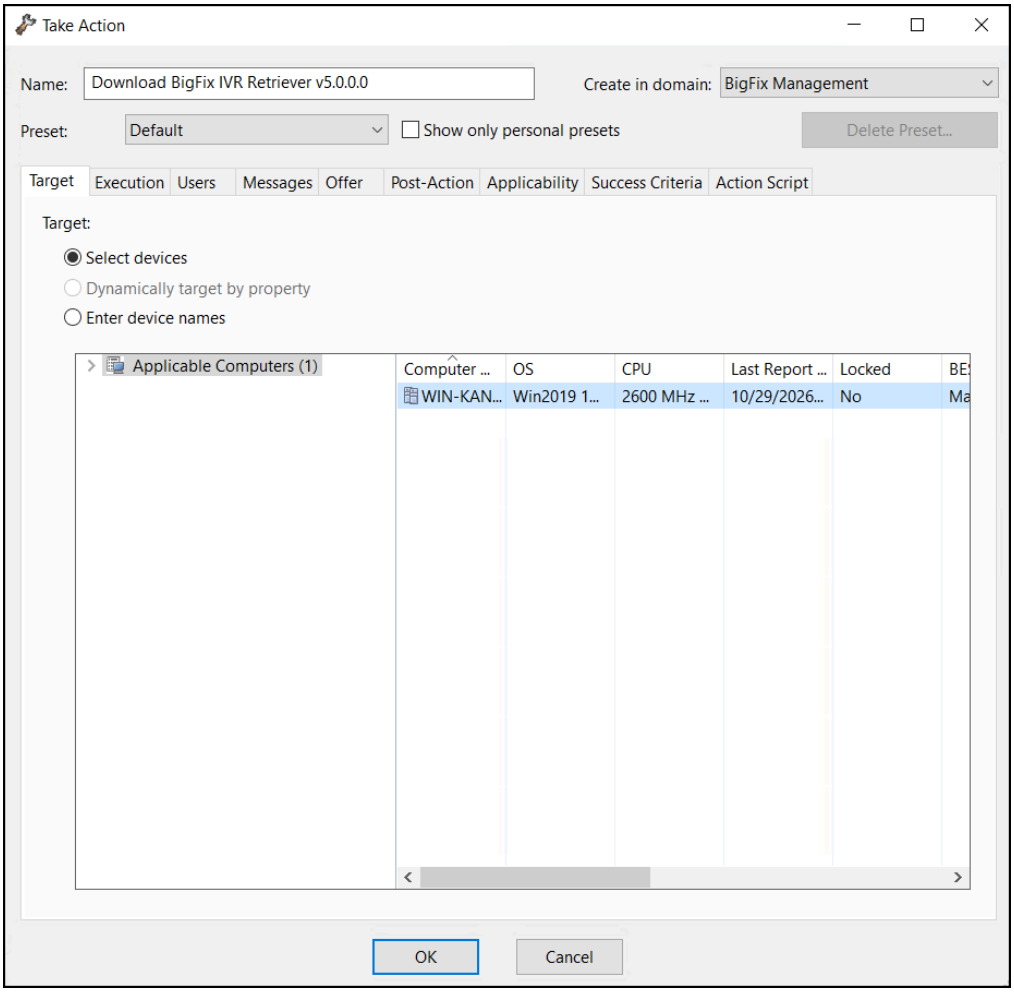



4. Click **Take Action**.

**Note:** It can take 2-3 minutes for the target computer to appear in the **Applicable Computers** list.

5. On the **Target** tab of the **Take Action** dialog box, select the computer where you want to install IVR, and then click **OK**.

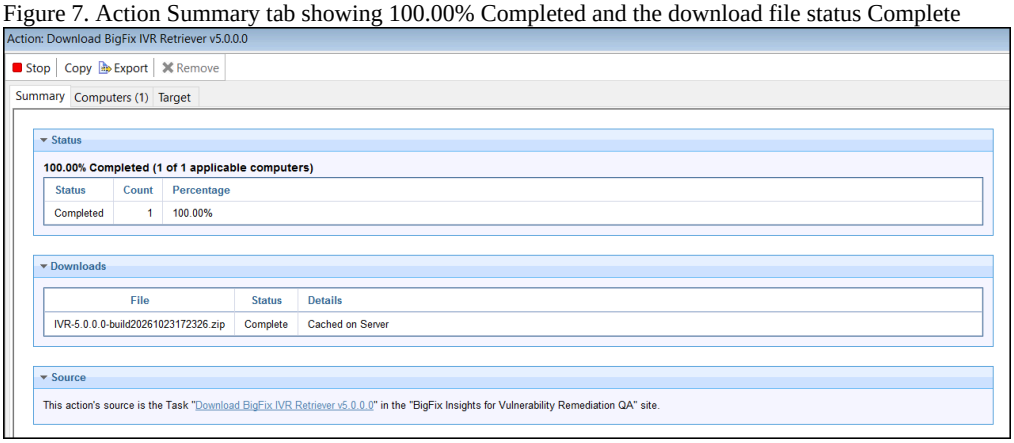
Figure 6. Take Action dialog box, Target tab, with one applicable computer selected




6. Wait for the action status to change to **Completed**.

- On the action **Summary** tab, the status shows **100.00% Completed**, and the download status shows **Complete**.

Figure 7. Action Summary tab showing 100.00% Completed and the download file status Complete



- The `BESIvrRetriever` folder exists in the installation path that you set.
- The **BES IVR Retriever Service** appears in Windows Services with status **Running**, and starts automatically. You don't need to start it manually.

Register IVR with the BigFix UI, and then configure it. See IVR v.5 setup process *(on page 14)*.

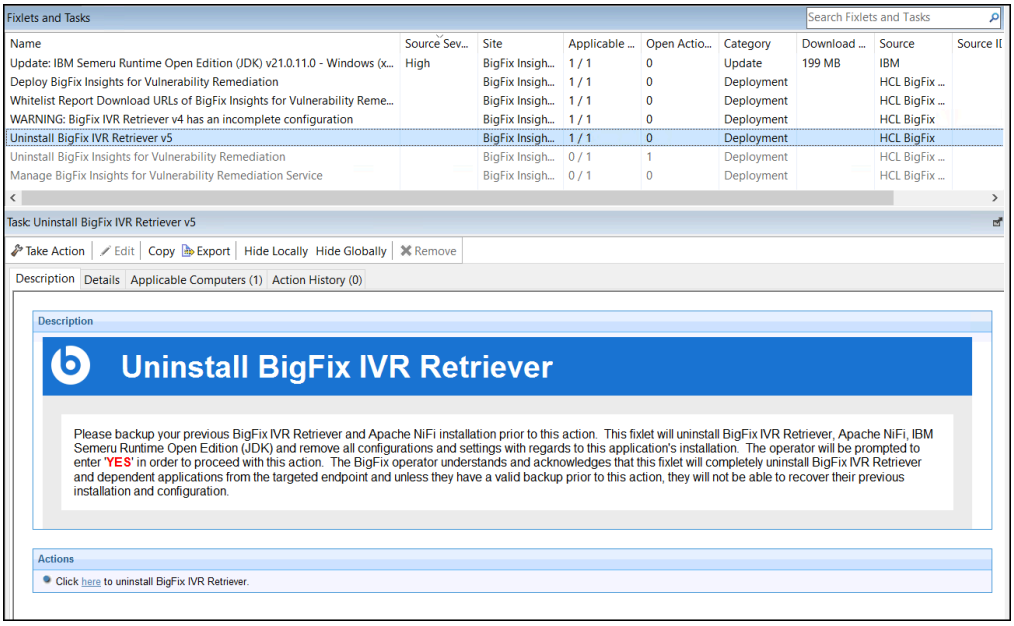
# Uninstall the BigFix IVR Retriever

The **Uninstall BigFix IVR Retriever v5** task removes the BigFix IVR Retriever from the target computer. It also removes all of its configurations and settings.

**CAUTION:** Uninstallation can't be undone. Back up your BigFix IVR Retriever installation and its configuration before you start. Without a valid backup, you can't recover the previous installation or configuration.

1. In the BigFix Console, go to **BigFix Insights for Vulnerability Remediation** > **Fixlets and Tasks**, and then select **Uninstall BigFix IVR Retriever v5**.

   Figure 8. Uninstall BigFix IVR Retriever v5 Descripxtion tab showing the backup warning and the Actions box




2. Review the **Description**, and then click **Take Action**, or click **here** in the **Actions** box.
3. Select the computer where IVR is installed, and then click **OK**.
4. When you are prompted, type **YES**, and then click **OK**.
5. Wait for the action status to change to **Completed**.

- The `BESIvrRetriever` folder is removed from the installation path.
- The **BES IVR Retriever Service** is removed from Windows Services.

# Chapter 4. IVR v.5 setup process

This section explains how to set up IVR v.5 after the IVR Retriever is installed. You register IVR with the BigFix UI by running one command on the BigFix UI server, and then complete the configuration in the BigFix UI. Complete the tasks in order.

**Before you begin**

- The **BES IVR Retriever Service** is installed and running. See Install the BigFix IVR Retriever *(on page 9)*.
- You know the BigFix UI **instance admin** credentials and the IVR user credentials that you set in the Download Task. The **instance admin** is the application instance credential created during BigFix UI installation. See Configure Administrative Credentials.
- You have a BigFix UI administrator account that is mapped to a BigFix operator under **Manage BigFix access**. Use this account, not the instance admin, for Task 2 and Task 3. Administrators can access Application Configuration *(on page )* and all BigFix UI applications. To create one, see Creating a new user. You map the user to a BigFix operator on the **Role** step.
- You have the following values ready:

| Value | Where it comes from | Where you use it |
|---|---|---|
| BigFix UI instance admin | Created when the BigFix UI was installed | Task 1 *(on page 14)* (--configure-ivr) |
| IVR user (username and password) | You set it in the Download Task | Task 1 *(on page 14)*, as **IVR Admin Username** and **IVR Admin Password** |
| SQL Server user and password | Your database administrator | Task 2 *(on page 15)*, **Database Configuration** |
| BigFix UI database host, port, and name | Your BigFix UI installation (see Configure Database Settings) | Task 2 *(on page 15)*, **Database Configuration** |
| Tenable Cloud URL, access key, secret key | Your Tenable administrator account, API Keys section | Task 2 *(on page 15)*, **Scanner Datasource** configuration |

**Note:** Store the database password and Tenable keys in a secure location. Don't paste them into email, tickets, or documentation.

## Task 1: Register IVR with the BigFix UI

Registering connects the BigFix UI to the IVR Retriever. Run this command once, after the Download Task completes and before you configure IVR in Application Configuration.

1. On the BigFix UI server, open Command Prompt as an administrator.
2. Go to the BigFix UI command folder.

```
cd "C:\Program Files (x86)\BigFix Enterprise\BES UI\cmd\bfui"
```

3. Run the registration command.

```
BFUI.exe --configure-ivr
```

4. Enter the values when prompted.

| Prompt | What to enter |
|---|---|
| Enter instance admin username / password | The BigFix UI instance admin credentials. |
| Enter IVR Server IP Address | The IP address of the IVR host. Use `127.0.0.1` when the IVR Retriever runs on the BigFix UI server. |

| Prompt | What to enter |
|---|---|
| Enter IVR Server Basic Authentication Port | The basic authentication port of the IVR Retriever, for example, `8088`. |
| Enter IVR Server mTLS Port | The mTLS port of the IVR Retriever, for example, `9022`. |
| Enter IVR Admin Username / Password | The IVR user credentials that you set in the Download Task. |
| Enter comma separated list of IP SANs for IVR certificate | The addresses that the IVR certificate must cover, for example, `localhost` when the IVR Retriever runs on the BigFix UI server. For a separate IVR host, include its IP address. |

5. Check that the output ends with **IVR configuration completed successfully**. For other BFUI.exe options, see Installation in the BigFix UI Administration Guide.

**Note:** The command output can include a warning that no recovery bundle exists for the BigFix UI encryption key. This warning concerns the BigFix UI platform, not IVR.

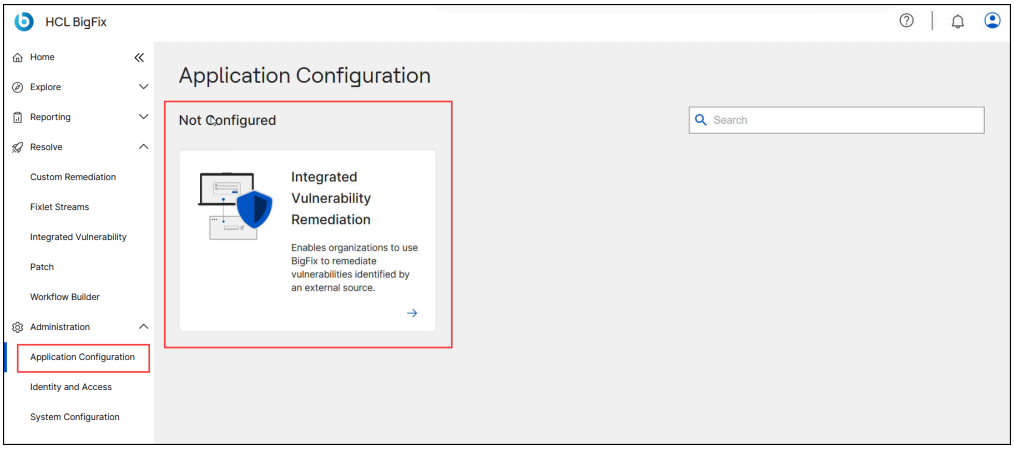
# Task 2: Configure IVR in Application Configuration

The IVR configuration wizard collects the database, application, and scanner data source settings. When you click **Finish**, IVR starts its background automation.

**CAUTION:** The wizard creates a new IVR schema in the existing BigFix UI database. Back up the BigFix UI database before you start.

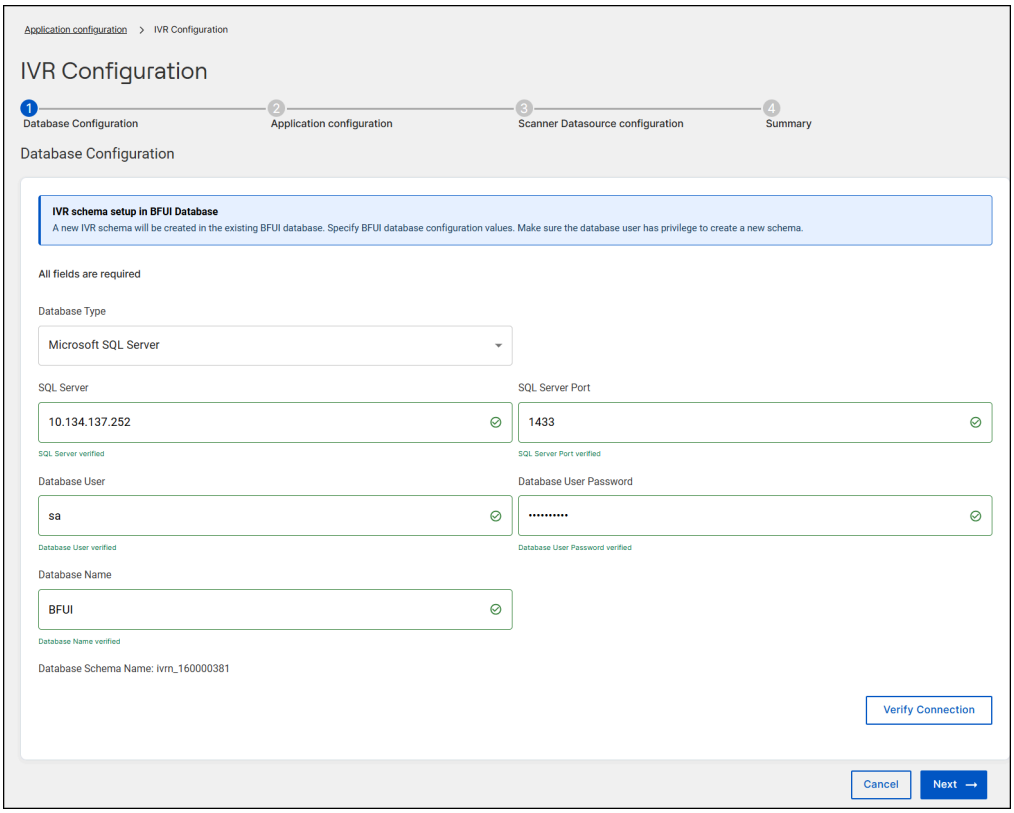
1. Log in to the BigFix UI as an administrator. See Access and security.
2. In the left navigation pane, select **Administration** > **Application Configuration**.

Figure 9. Administration > Application Configuration in the BigFix UI left navigation pane




3. Select the **Integrated Vulnerability Remediation** tile.
   The **IVR Configuration** wizard opens with four steps: **Database Configuration**, **Application configuration**, **Scanner Datasource configuration**, and **Summary**.
4. On the **Database Configuration** step, enter the BigFix UI database values. All fields are required.

Figure 10. Database Configuration step of the IVR Configuration wizard




**Note:** The **IVR schema setup in BFUI Database** banner reminds you that IVR creates a new schema in the existing BigFix UI database, so the database user must have permission to create a schema.

| Field | Description |
|---|---|
| Database Type | Select **Microsoft SQL Server**. |
| SQL Server | The host name or IP address of the SQL Server that hosts the BigFix UI database. |
| SQL Server Port | The SQL Server port, for example, `1433`. |
| Database User | A database user with permission to create a schema. |
| Database User Password | The password of the database user. |
| Database Name | The name of the existing BigFix UI database. Use the database that you set when you installed the BigFix UI. See Configure Database Settings. |

Below the fields, the wizard shows the **Database Schema Name** that IVR generates, for example, `ivrn_<number>`. You can't change it.

If you connect with a DSN instead, enter an ADO.NET connection string. Only Microsoft SQL Server DSN strings are supported, and the database must already exist. For example:

```
server=10.127.137.71;database=<DATABASE>;user=<USER>;password=<PASSWORD>;port=1433

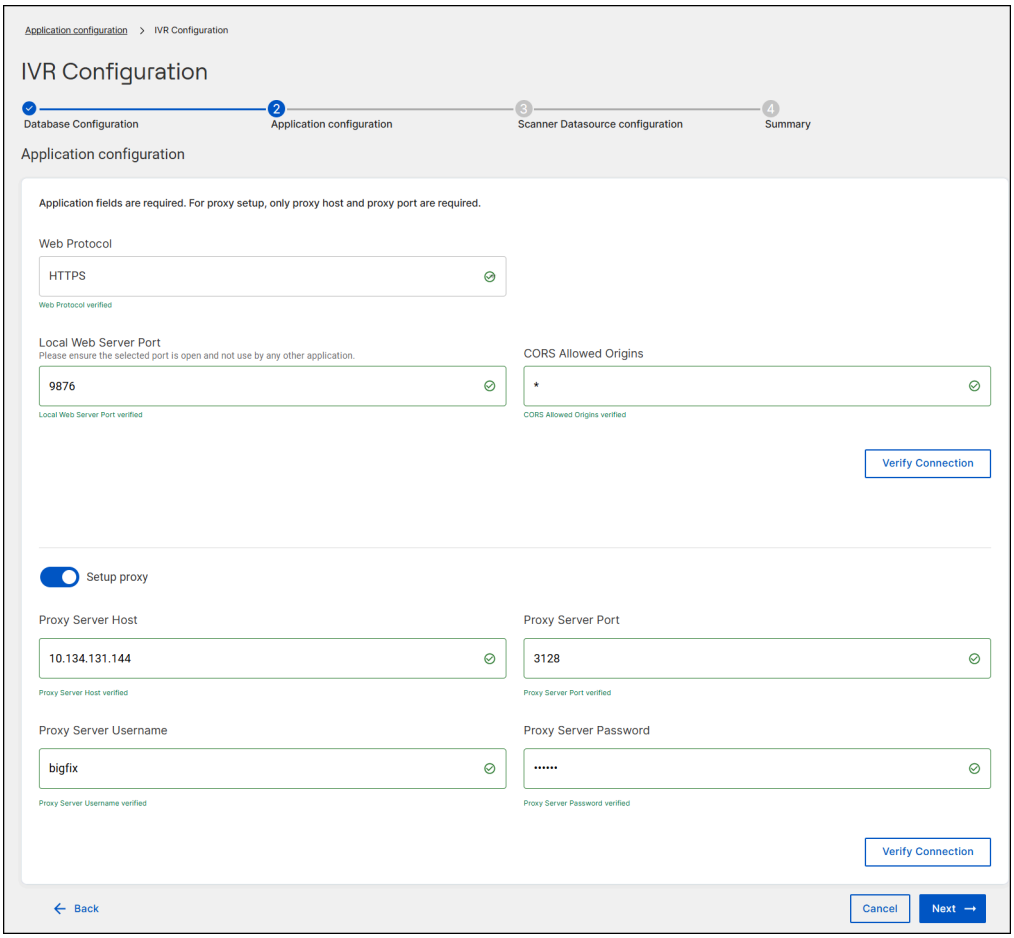
Server=10.131.121.61;Database=<DATABASE>;Integrated Security=True;Trusted_Connection=True
```

The second example uses Windows Authentication. In that case, the account that runs the service must have the `db_owner` user mapping on the database.

Select **Verify Connection**. A verified message appears under each field, for example, **SQL Server verified**. When every field is verified, select **Next**.

5. On the **Application configuration** step, enter the application settings. The application fields are required. For a proxy, only the proxy host and proxy port are required.

Figure 11. Application configuration step of the IVR Configuration wizard, with a proxy set up




| Field | Description |
|---|---|
| Web Protocol | Select **HTTPS**. |
| Local Web Server Port | The port that the IVR application listens on, for example, `9876`. Make sure that the port is open and no other application uses it. |
| CORS Allowed Origins | The origins allowed to make cross-origin requests. An asterisk (`*`) allows all origins. In production, consider limiting this to your BigFix UI origin, for example, `https://` |

| Field | Description |
|---|---|
| | `<BFUI_HOST>`. For general CORS guidance in the BigFix UI, see CORS allowed origins configuration. |

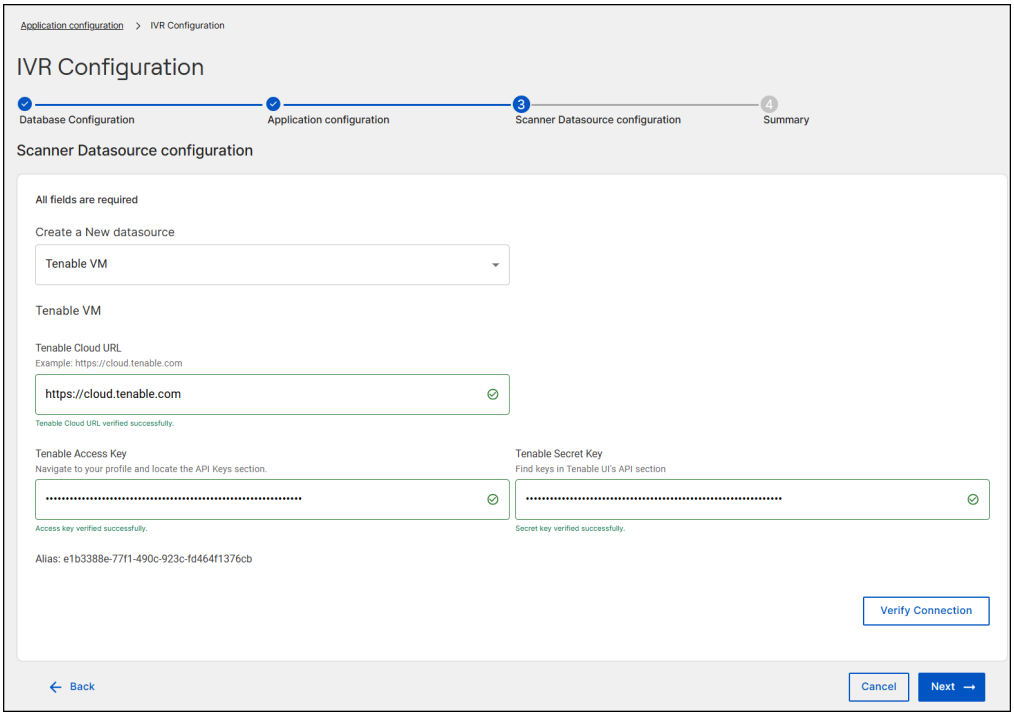
Select **Verify Connection** below the application fields. A verified message appears under each field.

If your network routes outbound scanner traffic through a proxy, turn on **Setup proxy**, and then enter the **Proxy Server Host** and **Proxy Server Port**. If the proxy requires authentication, also enter the **Proxy Server Username** and **Proxy Server Password**. Then click the **Verify Connection** button below the proxy fields. When all fields are verified, click **Next**.

**Important:** If you change any IVR configuration setting later, such as the application settings, the proxy, the database configuration, or the data source, restart the **BES IVR Retriever Service** so that the changes take effect. For the procedure, see To change a configuration *(on page 23)* section in Managing the IVR configuration *(on page 23)*.

6. On the **Scanner Datasource configuration** step, create the data source. All fields are required.

Figure 12. Scanner Datasource configuration step of the IVR Configuration wizard

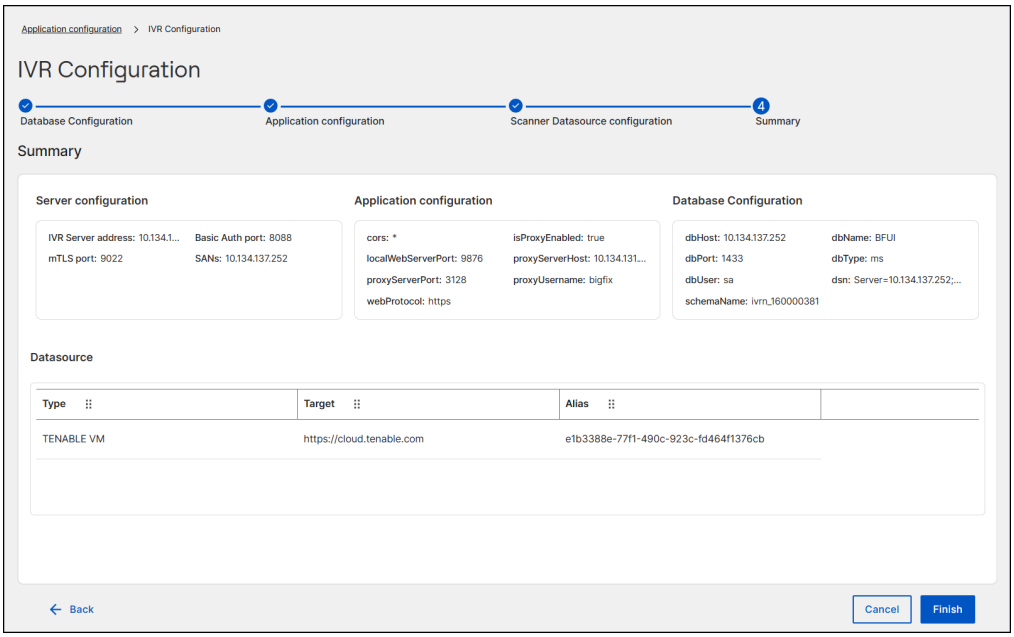



| Field | Description |
|---|---|
| Create a New datasource | Select **Tenable VM** (Tenable Vulnerability Management, the same platform that you selected as **Tenable** in the Download Task). |
| Tenable Cloud URL | Your Tenable URL, for example, https://cloud.tenable-.com. |
| Tenable Access Key | The access key from the **API Keys** section of your Tenable profile. |
| Tenable Secret Key | The secret key from the same section. |

Select **Verify Connection**. When all fields are verified, IVR shows the data source **Alias**, a generated identifier that you can't edit. Select **Next**.

7. On the **Summary** step, review your settings, and then select **Finish**. To change a value, select **Back**.

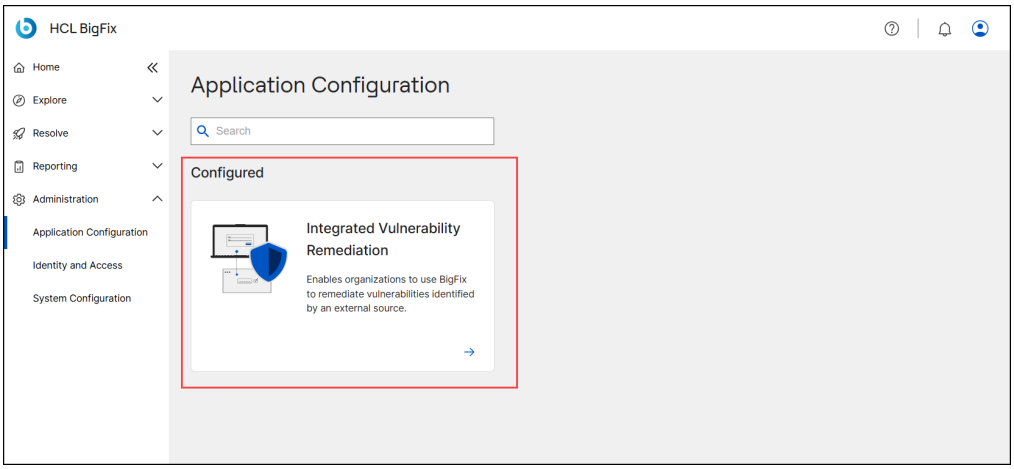
Figure 13. Summary step of the IVR Configuration wizard




The BigFix UI returns you to the **Application Configuration** page and starts the IVR background automation processes, including BES asset automation and BES Fixlet automation.

- **In progress:** While the processes run, IVR pages show **IVR automation is in progress. Please wait until it completes.** Don't start the wizard again during this time.
- **Success:** When all processes complete, the IVR tile moves to the **Configured** section.

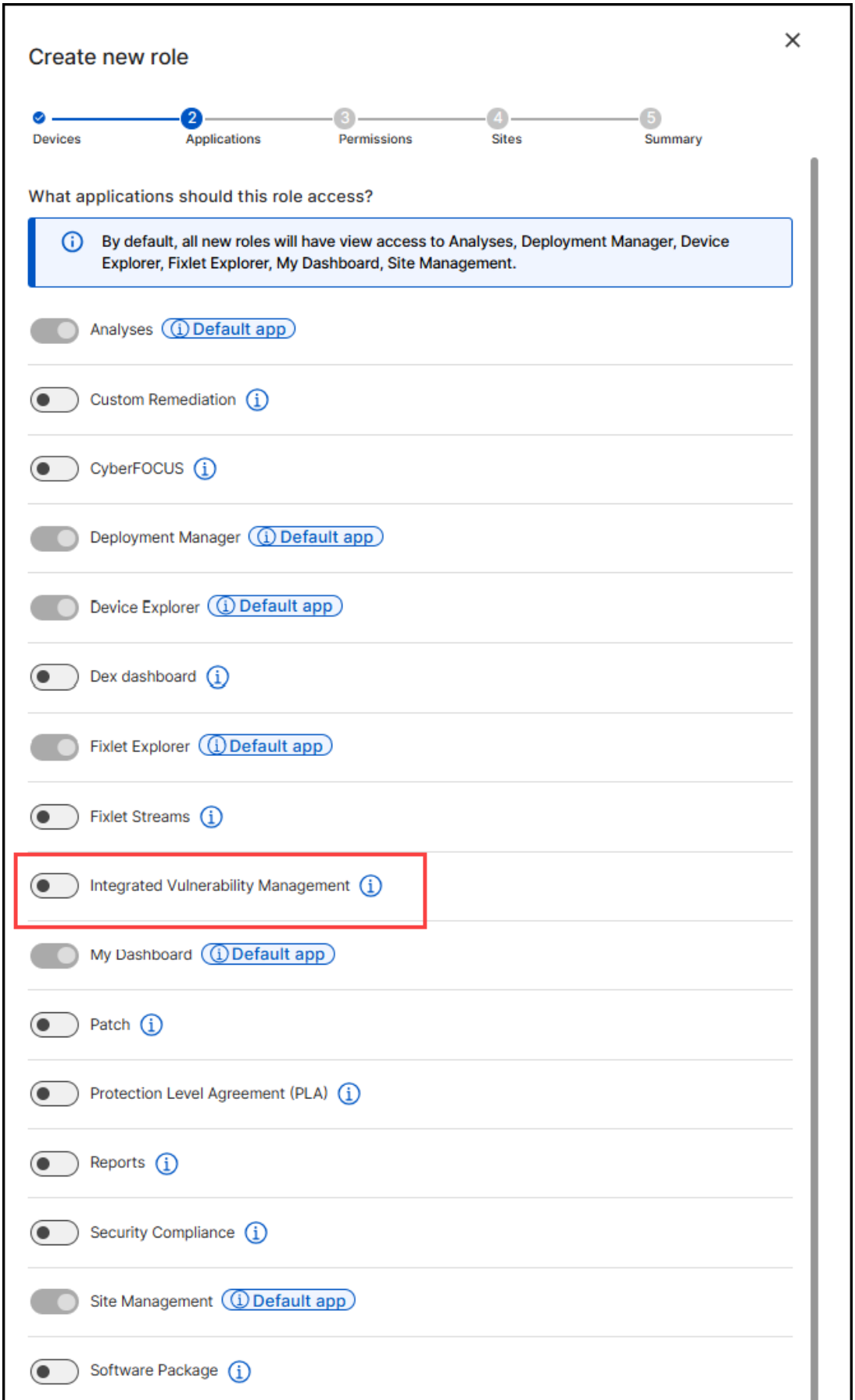
Figure 14. Application Configuration page displays IVR as Configured




- **Failure:** If a process fails, the tile stays in **Not Configured**, and a message reports that the background process stopped unexpectedly. Check the BigFix UI and IVR logs (IVR logs *(on page 47)*), fix the reported problem, and then open the wizard again and click **Finish**.

# Task 3: Grant IVR access to other users (optional)

Figure 15. Create role wizard, application selection step, Turn on Integrated Vulnerability Remediation



Do this task after IVR is configured. Otherwise, users with the new role see **IVR is not configured** when they open IVR. Administrators can access all BigFix UI applications. Other users see **Integrated Vulnerability Remediation** only if their role includes the IVR application.

1. Log in to the BigFix UI as an administrator, click **Administration** > **Identity and Access**, and then select the **User & Role Management** card. See User & Role Management.
2. On the **Roles** tab, select **Create role**.

   The **Create new role** wizard opens with five steps: **Devices**, **Applications**, **Permissions**, **Sites**, and **Summary**.
3. On the **Devices** step, set the devices for the role, and then select **Next**.
4. On the **Applications** step, turn on **Integrated Vulnerability Management**. It appears in the list only when the BigFix Insights for Vulnerability Remediation site is enabled.
5. Complete the **Permissions**, **Sites**, and **Summary** steps to create the role. See Managing Roles.
6. Assign the role to the users who need IVR. These users see IVR under **Resolve** the next time they log in. See Assigning roles to users.



**Note:** Users can't turn applications on or off for themselves. Access is controlled by the role.

# Verify the setup

1. On the IVR host, open `services.msc` and confirm that **BES IVR Retriever Service** is **Running** with startup type **Automatic**.
2. On the IVR host, confirm that the basic authentication and mTLS ports that you entered in Task 1 are listening. For example:

   ```
   netstat -ano | findstr ":8088 :9022"
   ```
3. On **Administration** > **Application Configuration**, confirm that the IVR tile shows **Configured**.
4. Click **Resolve** > **Integrated Vulnerability Remediation**.
   The **IVR-Scanner Import** page opens with an **Updated** time stamp.
5. After the first automation run completes, check that vulnerabilities appear in the **Vulnerability view**, that devices appear in the **Device view**, and that **Last Automation Run** shows a time.
   If the **Device view** is empty, check that the **IVR Vulnerability Scanner Host ID** analysis is activated globally (see Before you begin, step 4 *(on page 8)* in IVR v.5 Fixlets and Tasks *(on page 8)*) and returns results for your devices.
6. In **Explore** > **Devices**, open a device and confirm that the **Vulnerabilites** tab is present. See Device Details Page.

# Chapter 5. IVR on-prem Start Process

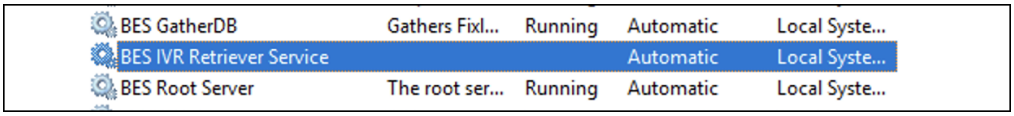
This section explains how to start the IVR Retriever service.

When you install IVR with the Download Task, the **BES IVR Retriever Service** is installed as a Windows service and starts automatically. You don't need to start it after installation.

Start the service manually if the computer restarts and the service doesn't start, or if someone stops it. To restart the service after a configuration change, see Managing the IVR configuration *(on page 23)*. To start the service, use one of these methods:

- **Windows Services:** Open `services.msc`, find **BES IVR Retriever Service**, and then click **Start**.

  Figure 16. Windows Services window showing BES IVR Retriever Service with Startup Type Automatic

- **Command line:** Open Command Prompt as an administrator, and then run:

```
cd "C:\Program Files (x86)\BigFix Enterprise\BESIvrRetriever\cmd\ivrNext"
ivrNext.exe --start
```

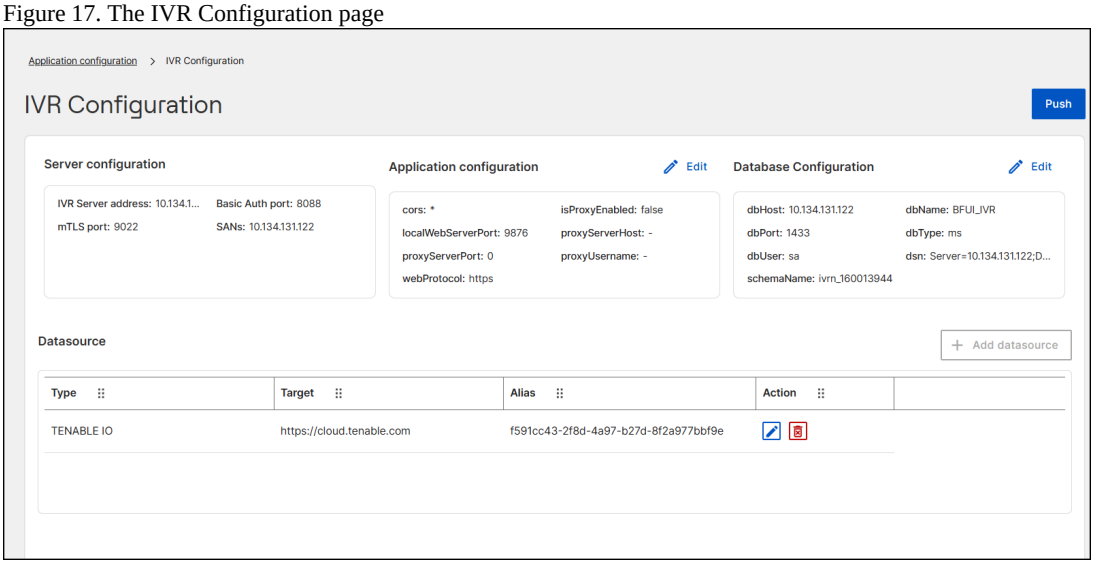
**Note:** The paths in this guide assume the default installation path. If you changed it in the Download Task, replace `C:\Program Files (x86)\BigFix Enterprise\BESIvrRetriever` with your path.

# Chapter 6. Managing the IVR configuration

Learn about updating the IVR configuration settings.

After IVR is configured, click the Integrated Vulnerability Remediation tile in **Administration** > **Application Configuration** *(on page )* to review or change its settings. The **IVR Configuration** page opens.

Figure 17. The IVR Configuration page




| Area | What you can do |
|---|---|
| Server configuration | View the IVR server address, Basic Auth port, mTLS port, and SANs. These values are set by the `--configure-ivr` command. You can't edit them here. |
| Application configuration | The web protocol, local web server port, CORS allowed origins, and proxy settings. |
| Database Configuration | The connection to the BigFix UI database. |
| Datasource | The Tenable data source, with its **Type**, **Target**, and **Alias**. Use the icons in the **Action** column to edit or delete it. |
| Push | Applies your configuration changes to the IVR service. |

### To change a configuration

1. On the card or data source that you want to change, click **Edit** (or the edit icon in the **Action** column).
2. Change the values in the dialog box, click **Verify Connection**, and then click **Update**. The **Database Configuration**, **Application configuration**, and **Update datasource** dialog boxes have the same fields as the matching steps in Task 2: Configure IVR in Application Configuration *(on page 15)*.

Figure 18. Edit Database Configuration dialog

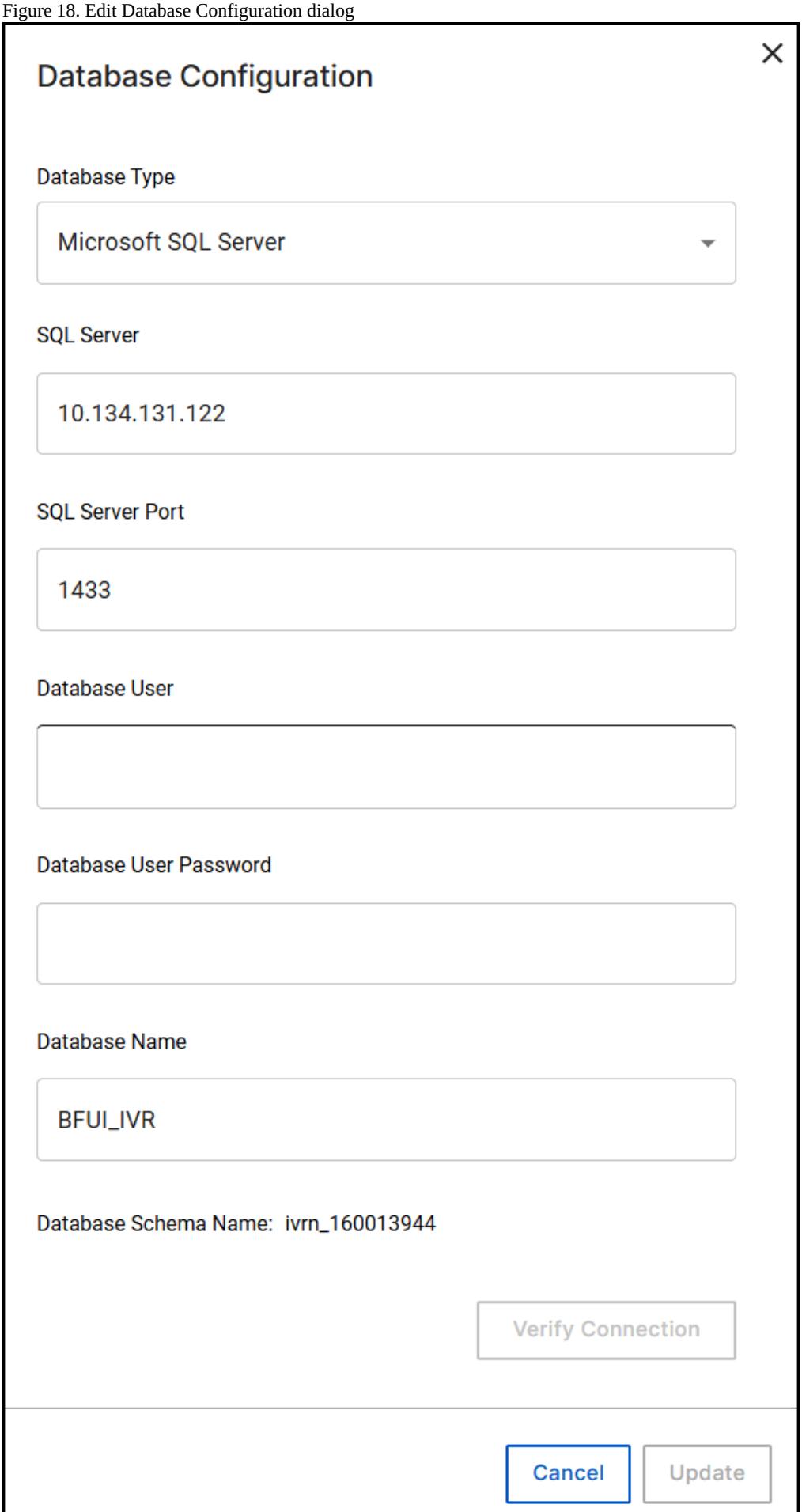


Figure 19. Edit Application configuration dialog

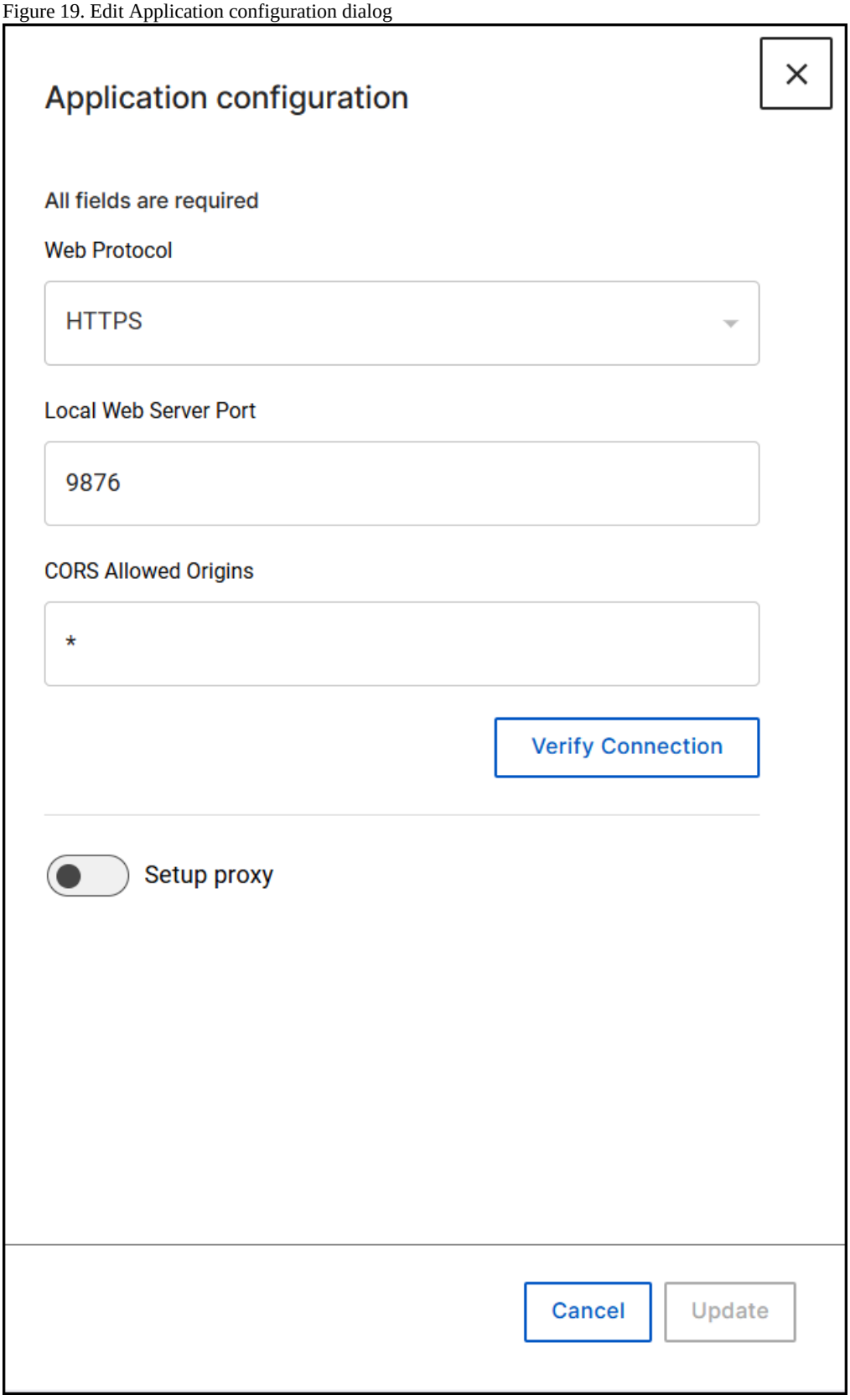
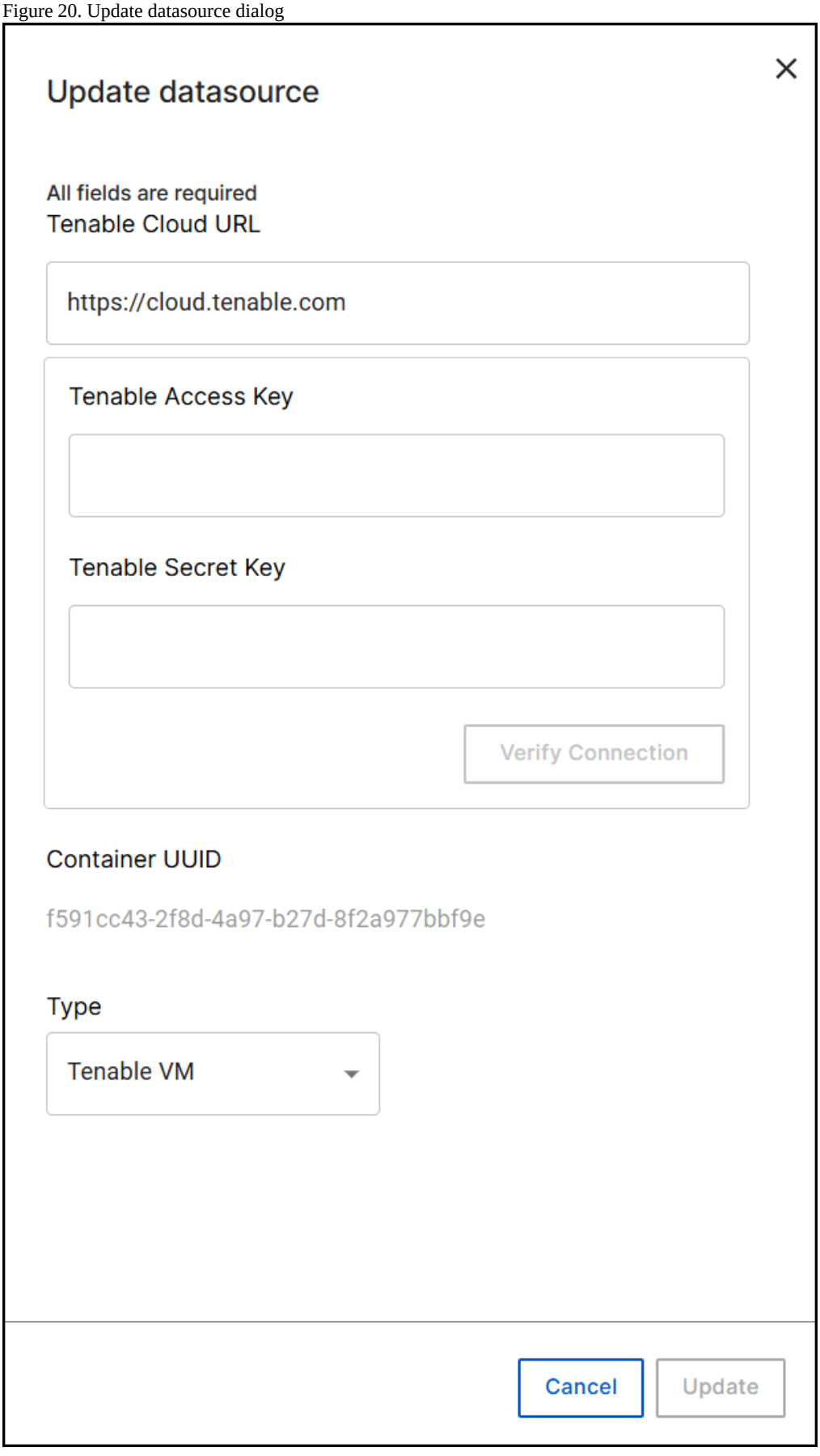


Figure 20. Update datasource dialog



3. Click **Push**.
4. Restart the IVR service so that the changes take effect: open `services.msc`, right-click **BES IVR Retriever Service**, and then click **Restart**. A restart is required after any change to the application configuration, the database configuration, the data source, or the proxy.

**Note:** To use different Tenable credentials, edit the existing data source. For data source limits, see Known limitations *(on page 50)*.

**Note:** If you delete a data source and the BigFix UI can't update the service status, a message asks you to check the logs. Re-create the data source, and then click **Push** to continue using IVR.

# Chapter 7. IVR v.5 on BFUI

This section explains how to use IVR in the BigFix UI: open the application, read the dashboard, work with vulnerability data, and remediate vulnerabilities. It applies to every user whose role includes IVR, not only administrators.

With IVR in the BigFix UI, you can:

- View vulnerability trends in charts on the Overview tab.
- Review vulnerabilities in the Vulnerability view and the affected devices in the Device view.
- Search, filter, and export your vulnerability data.
- Save a report of your current view and load it again later.
- Remediate vulnerabilities by deploying Fixlets to devices, starting from either the vulnerabilities or the devices.

## Open IVR

In the left navigation pane, expand **Resolve**, and then click **Integrated Vulnerability Remediation**. See Resolve in the BigFix UI User's Guide.

The **Integrated Vulnerability Remediation** option appears only when both of the following are true:

- Your administrator has enabled the BigFix Integrated Vulnerability Remediation site.
- Your role includes the IVR application. See Task 3: Grant IVR access to other users (optional) *(on page 20)*.

If you don't see the option, contact your BigFix administrator. Administrators: see Troubleshooting *(on page 48)*.

**Note:** If your role includes IVR but IVR isn't configured yet, the page shows **IVR is not configured** with this message: "Set it up under Administration > Application Configuration > IVR Configuration. If you don't have access, contact your administrator." Ask your administrator to complete the IVR v.5 setup process *(on page 14)*.

## The IVR dashboard

The IVR dashboard is the **IVR-Scanner Import** page. It shows an **Updated** time stamp for the most recent data refresh and has three tabs: **Overview**, **Vulnerability view**, and **Device view**.

At the top of the **Vulnerability view** and **Device view** tabs, two indicators show the status of the IVR automation:

- **Last Automation Run** shows when the most recent run finished.
- **Next Expected Automation Run** shows when the next run is expected to start. IVR refreshes scanner data every 12 hours by default.

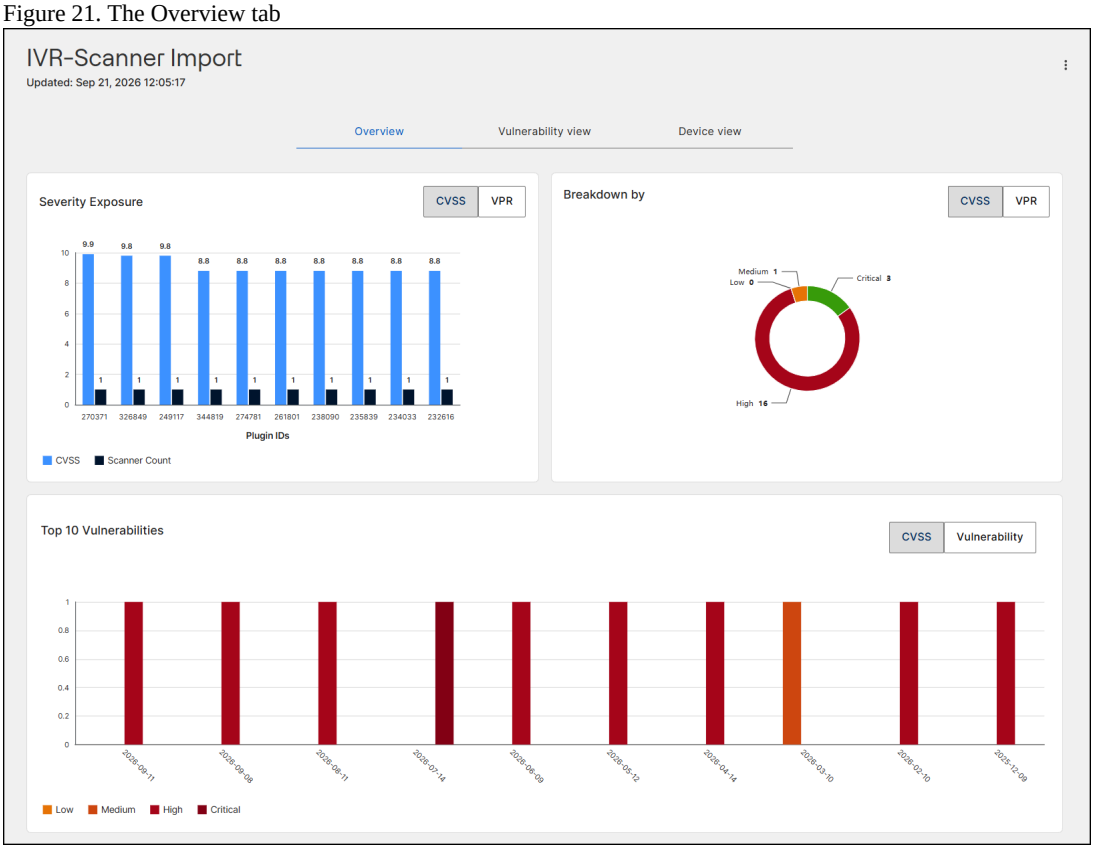
### Header controls

- Ellipsis icon (three vertical dots): opens a menu that includes **Export**. See Export data *(on page 32)*.
- Filter icon: opens the **Filter data** widget. See Filter vulnerabilities *(on page 32)*.
- Manage reports: saves or loads a report. See Save and load reports *(on page 32)*.

**Note:** The **Filter** icon and the **Manage reports** button are available on the **Vulnerability view** and **Device view** tabs. They are hidden on the **Overview** tab.

### Overview tab

Figure 21. The Overview tab

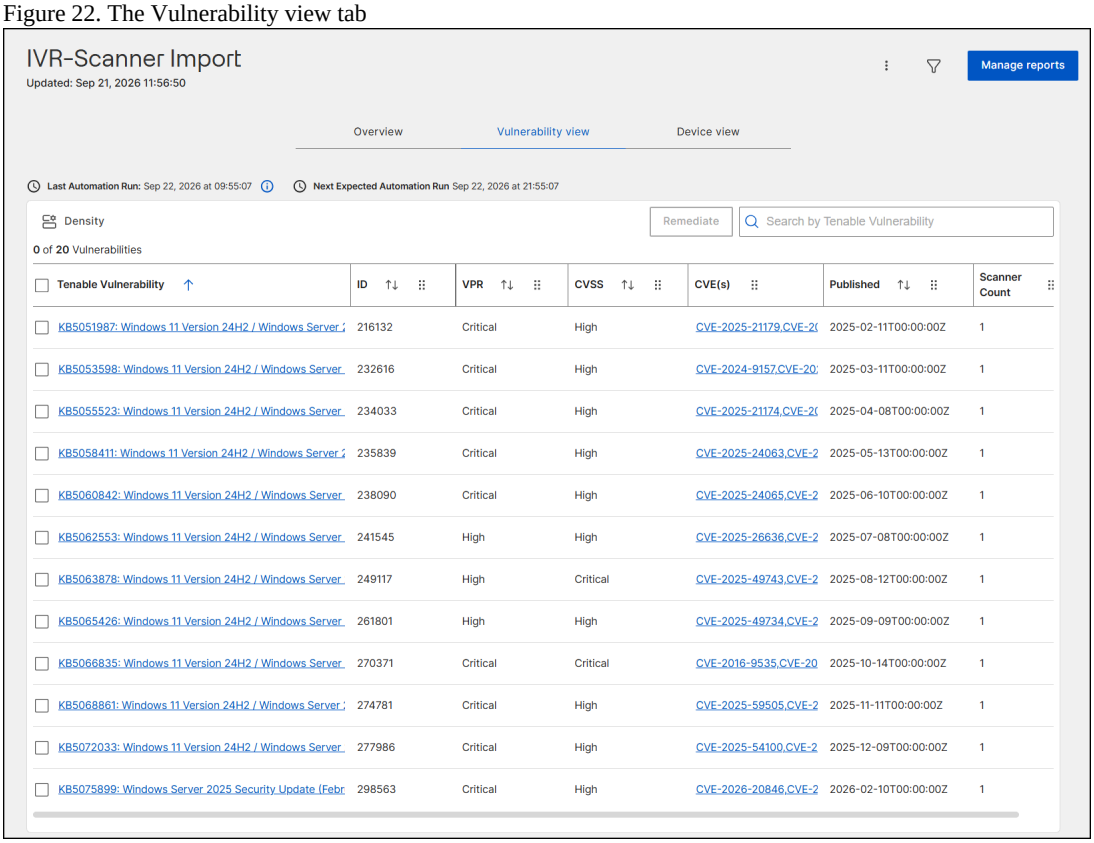



The **Overview** tab shows charts that help you decide which vulnerabilities to remediate first:

- **Severity Exposure**: a bar chart that plots, for each plugin ID, the vulnerability score and the scanner count side by side. Click **CVSS** or **VPR** to change the scoring model.
- **Breakdown by**: a donut chart that shows how vulnerabilities are distributed by severity (Critical, High, Medium, and Low). Click **CVSS** or **VPR** to change the scoring model.
- **Top 10 Vulnerabilities**: a timeline bar chart of the ten highest-ranked risks, plotted against their publication dates and color-coded by severity from Low to Critical. Click **CVSS** or **Vulnerability** to change the view.

**Vulnerability view tab**

Figure 22. The Vulnerability view tab




The **Vulnerability view** tab lists the active vulnerabilities in a grid. A counter above the grid shows how many vulnerabilities are selected (for example, "0 of 20 Vulnerabilities"). Use **Density** to change the row spacing, click the sort arrows in a column heading to sort the grid, and type in **Search by Tenable Vulnerability** to search the vulnerability names.

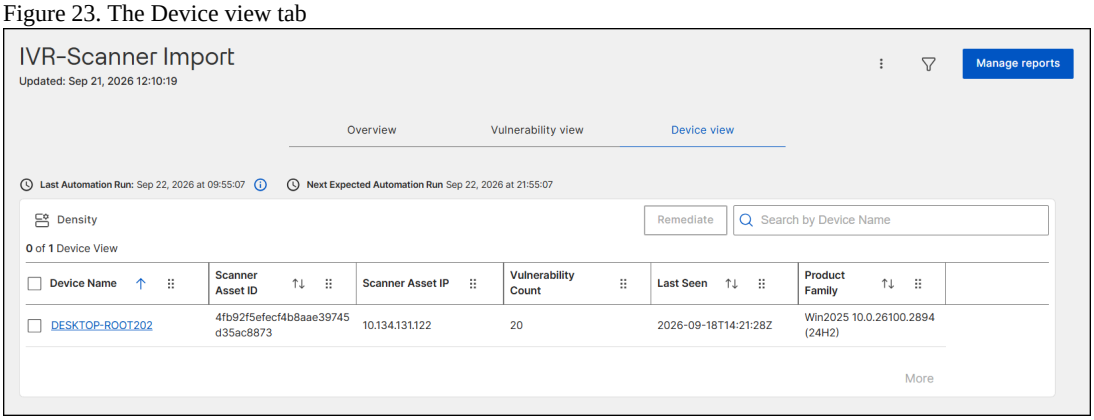
| Column | Description |
|---|---|
| Selection check box | Select one or more rows to act on them, for example, to remediate. The check box in the heading row selects all rows. |
| Tenable Vulnerability | The vulnerability name as identified by the scanner. Click it to open the vulnerability details page, which has the **Vulnerability Information**, **Contents**, **Devices**, and **Deployment** tabs. |
| ID | The unique numeric ID (plugin ID) of the vulnerability. |
| VPR | The Vulnerability Priority Rating, a dynamic rating (for example, Low, Medium, High, or Critical) that helps you prioritize remediation. |
| CVSS | The Common Vulnerability Scoring System severity (for example, High or Critical). |
| CVE(s) | The Common Vulnerabilities and Exposures identifiers. Each identifier is a link to its public entry. |
| Published | The date and time when the vulnerability was publicly disclosed. |
| Scanner Count | The number of devices on which the scanner detected the vulnerability. |

**Note:** Scanner Count shows the devices that the scanner detected. The Contents tab of the vulnerability details page shows the devices that are relevant to each Fixlet. The two numbers can differ.

To fix vulnerabilities, select them and click **Remediate**. See Remediate vulnerabilities *(on page 37)*.

## Device view

Figure 23. The Device view tab



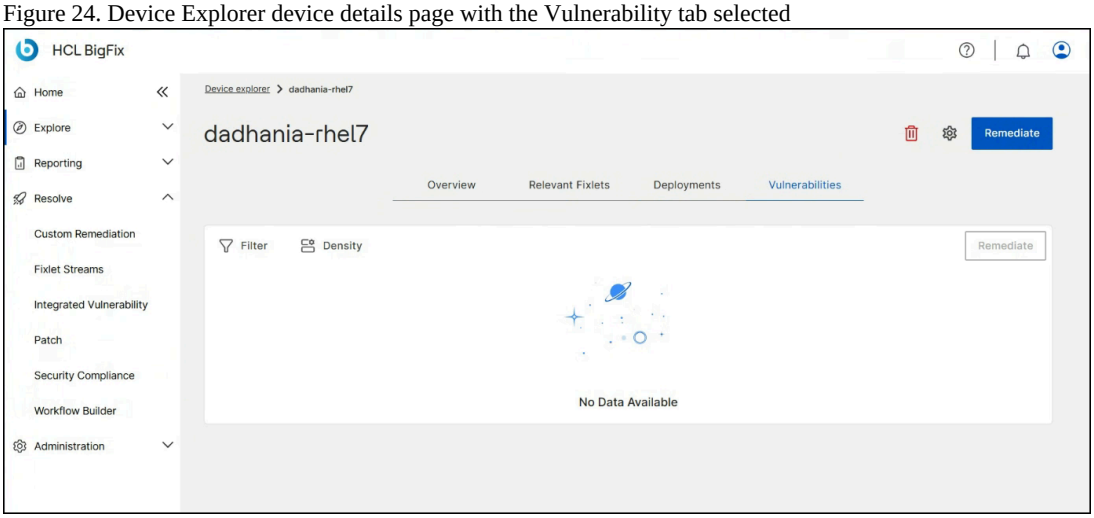

The **Device view** tab gives you a device-level dashboard. It lists only the devices that are relevant to IVR, not every device in **Explore**. Use this tab when you want to start from the devices instead of from the vulnerabilities.

Type in **Search by Device Name** to search the grid. The grid contains the following columns:

| Column | Description |
|---|---|
| Device Name | The name of the device. Click the name to open the device in Device Explorer. |
| Scanner Asset ID | The ID that the scanner assigned to the device. |
| Scanner Asset IP | The IP address that the scanner recorded for the device. |
| Vulnerability Count | The number of vulnerabilities found on the device. |
| Last Seen | The date and time when the scanner last saw the device. |
| Product Family | The operating system or product family of the device. |

**View a device's vulnerabilities in Device Explorer**

Figure 24. Device Explorer device details page with the Vulnerability tab selected



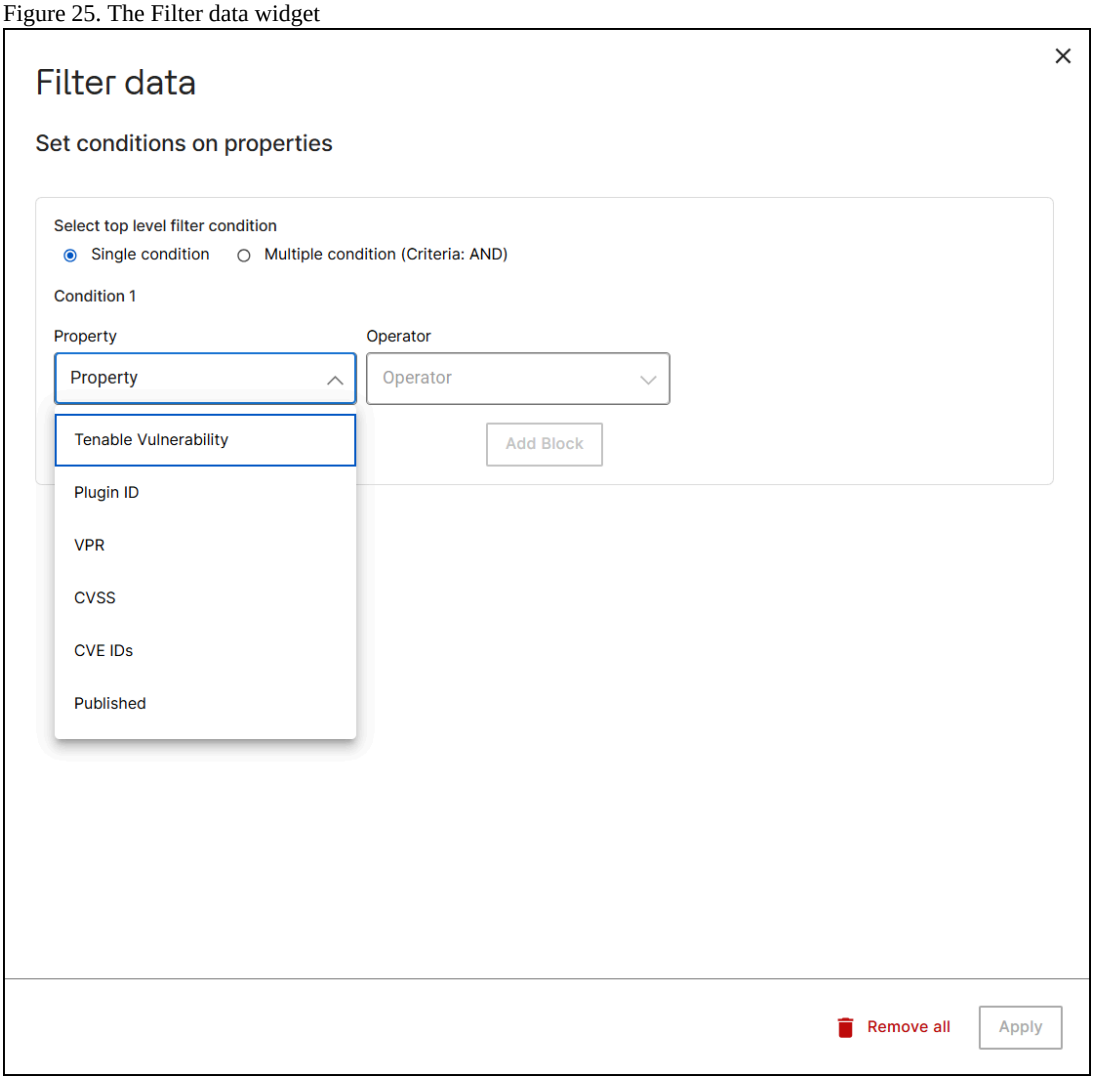

Click a device name to open it in **Device Explorer**. The **Vulnerabilities** tab lists the vulnerabilities that were found on that device. Use this path when you want to review a single device.

**Note:** The **Vulnerabilities** tab appears in Device Explorer only when the BigFix Integrated Vulnerability Remediation site is enabled. This applies to every device that you open in Device Explorer, including devices that you open from **Explore** > **Devices**.

## Work with dashboard data

### Filter vulnerabilities

Figure 25. The Filter data widget



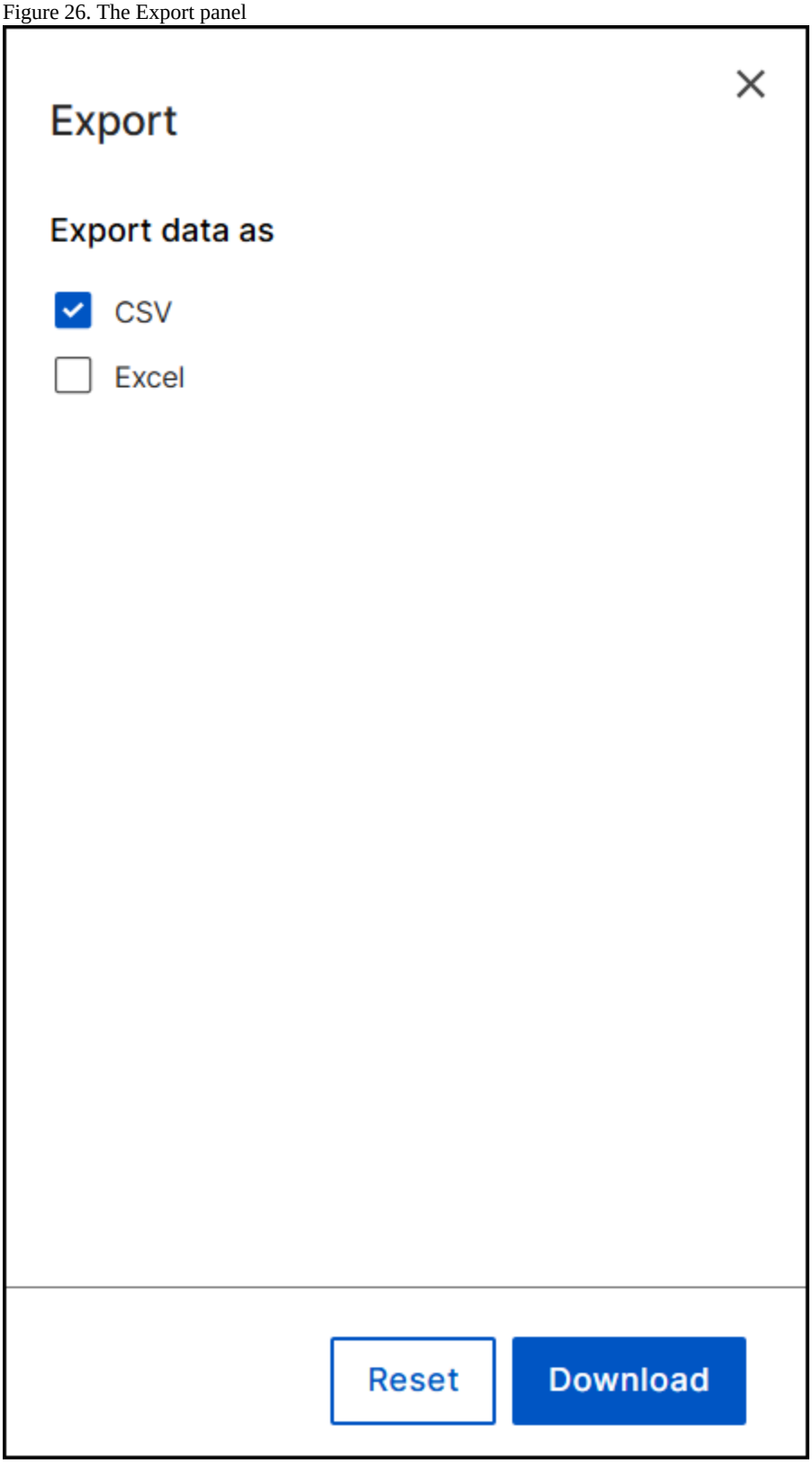

Use filters to find specific vulnerabilities in a large data set.

1. On the **Vulnerability view** tab, click the **Filter** icon. The **Filter data** widget opens.
2. Select **Single condition** or **Multiple condition (Criteria: AND)**.
3. Select a **Property** (**Tenable Vulnerability**, **Plugin ID**, **VPR**, **CVSS**, **CVE IDs**, or **Published**), an **Operator**, and a value.
4. Click **Apply**.

While a filter is active, indicators appear above the grid so that you can see which filters are applied and clear them. To clear all conditions in the widget, click **Remove all**.

**Export data**

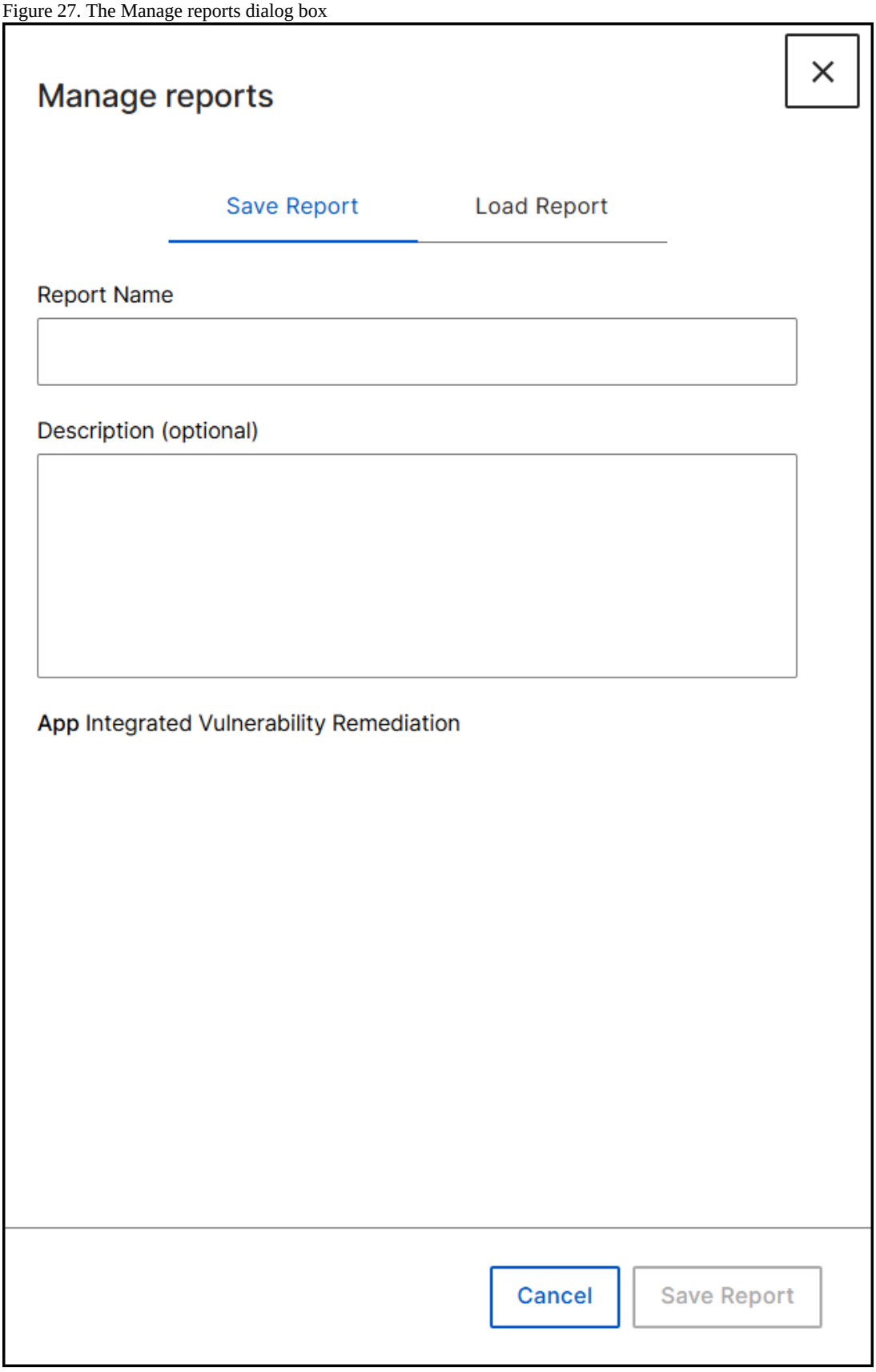
Figure 26. The Export panel



1. Click the **Ellipsis** icon (three vertical dots) in the header controls.
2. Click **Export**.
3. In the **Export** panel, select **CSV** or **Excel**.
4. Click **Download**. To clear your selection, click **Reset**.

**Save and load reports**

Figure 27. The Manage reports dialog box



A report saves your current grid view so that you can load it again later.

1. Click **Manage reports** in the dashboard header.
2. On the **Save Report** tab, enter a **Report Name**. Optionally, enter a **Description**.
3. Click **Save Report**.

To load a saved report, click **Manage reports**, open the **Load Report** tab, and then select the report.

## Remediate vulnerabilities

Remediation deploys Fixlets to the devices that are affected by vulnerabilities. A wizard guides you through choosing the Fixlets, setting the actions, targeting the devices, setting the deployment behavior, and scheduling the deployment. The steps match the BigFix UI deployment wizard; see Deploying Fixlets. You can start the wizard in three ways:

| Start from | Use it when | Wizard steps |
|---|---|---|
| Vulnerability view | You want to fix specific vulnerabilities. | Fixlets, Actions, Devices, Behavior, Schedule, Summary |
| Vulnerability details page | You want to fix one vulnerability. | Same as the Vulnerability view |
| Device view | You want to fix the vulnerabilities on specific devices. | Devices, Fixlets, Actions, Behavior, Schedule, Summary |

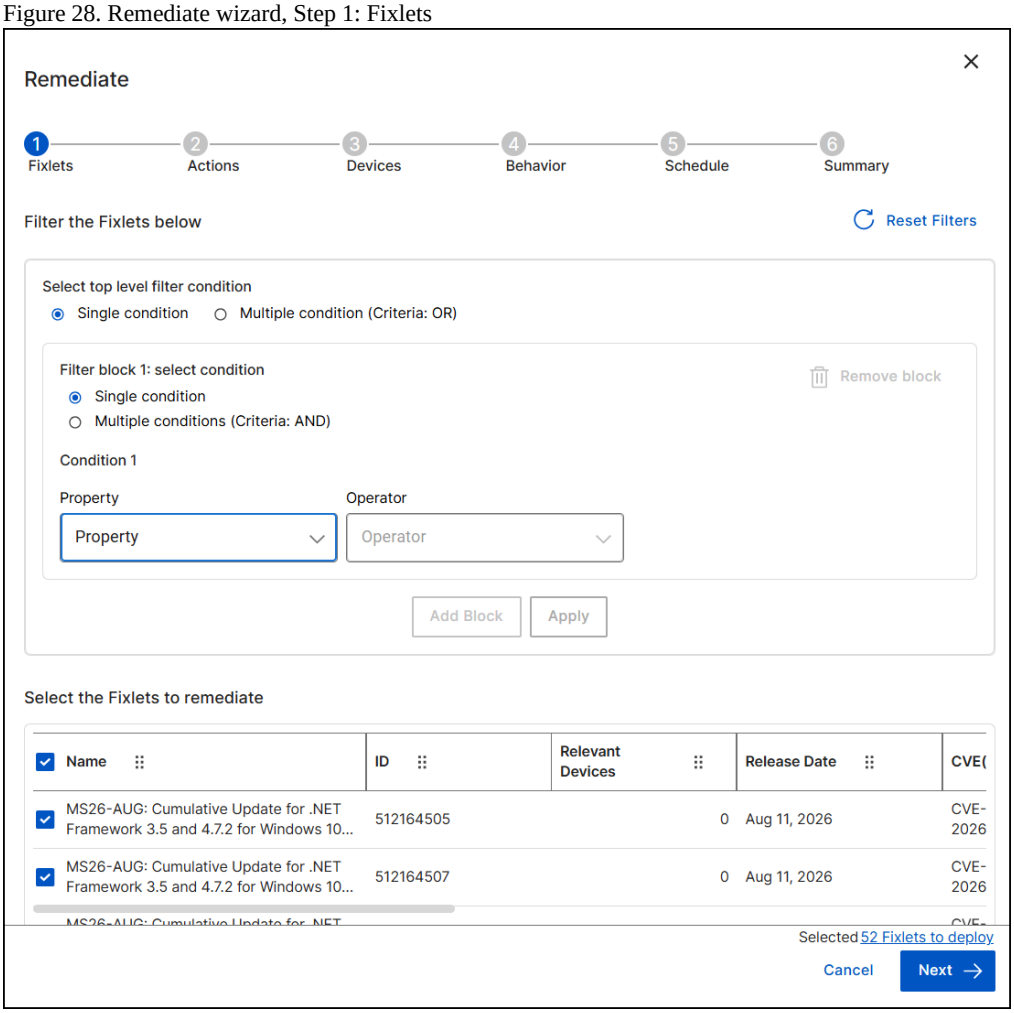
**CAUTION:** Deploying Fixlets changes software on the targeted devices. A deployment can require restarts, use network bandwidth to download files, and run inside or outside device maintenance windows, depending on your **Schedule** settings. Review the **Summary** step carefully before you click **Deploy**. Run your first remediation against a small test device group.

### Remediate from the Vulnerability view

1. Start the wizard in one of these ways:
   - On the **Vulnerability view** tab, select the check box for each vulnerability that you want to remediate, and then click **Remediate**.
   - Click a vulnerability name to open its details page, and then click **Remediate**.

   The **Remediate** wizard opens at the **Fixlets** step.
2. **Step 1: Fixlets.** Choose the Fixlets to deploy.

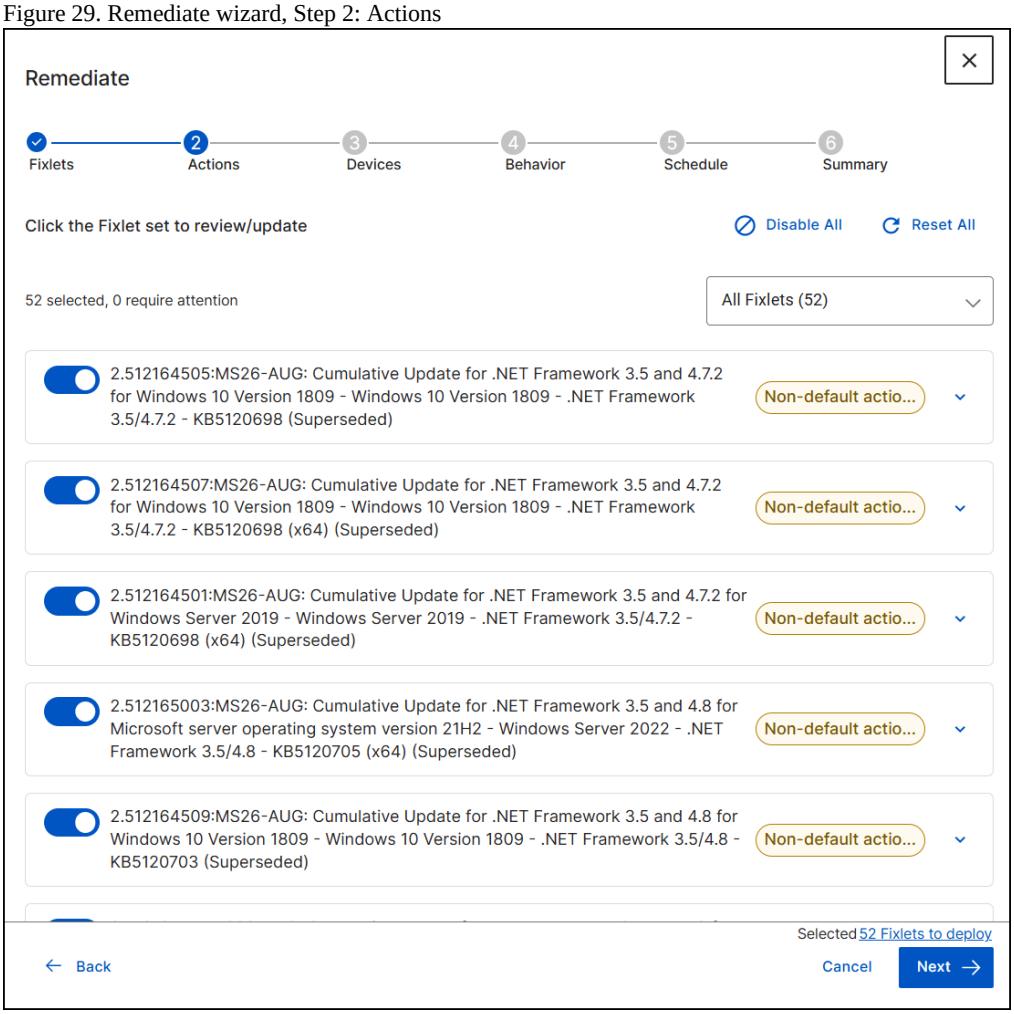
Figure 28. Remediate wizard, Step 1: Fixlets




a. Review the **Select the Fixlets to remediate** table. It shows the **Name**, **ID**, **Relevant Devices**, **Release Date**, and CVEs of each Fixlet.
b. Optional: To narrow the list, use **Filter the Fixlets below**. Under **Select top level filter condition**, select **Single condition** or **Multiple condition (Criteria: OR)**. Within each filter block, select **Single condition** or **Multiple conditions (Criteria: AND)**, choose a **Property** and an **Operator**, and then click **Apply**. To add another filter block, click **Add Block**. Conditions inside one block are combined with AND, and separate blocks are combined with OR. To start over, click **Reset Filters**.
c. Make sure that the check box is selected for every Fixlet that you want to deploy. The total appears at the bottom of the wizard, for example, "Selected 52 Fixlets to deploy".
d. Click **Next**.

3. **Step 2: Actions.** Review the action that each Fixlet runs.

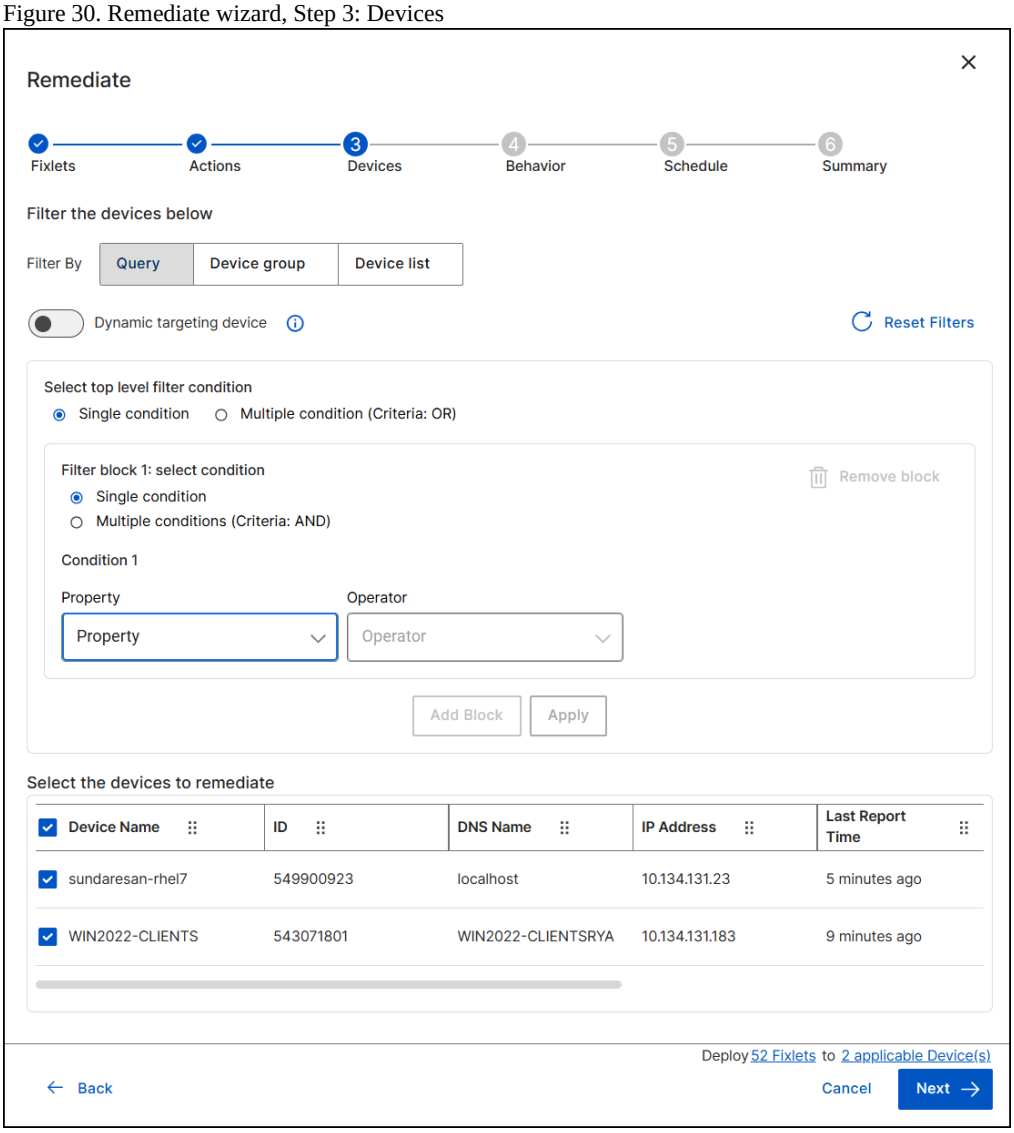
Figure 29. Remediate wizard, Step 2: Actions




a. Use the toggle next to a Fixlet to include it in or exclude it from the deployment.
b. Review the Fixlets that are marked **Non-default action**. The counter at the top of the page (for example, "52 selected, 0 require attention") shows how many Fixlets need your attention. Fixlets that require attention aren't deployed until you resolve them. To resolve one, expand it and select the action to run, as described in the next step.
c. To see the details of a Fixlet, expand it. The expanded view shows the available actions (for example, **Action1** to start the deployment) and the Fixlet attributes: **Category**, **CVE(s)**, **Download size**, **Release date**, **Severity**, **Source**, and **Source ID**.
d. Optional: Click **Disable All** to exclude all Fixlets, or click **Reset All** to restore the default selection. Use the **All Fixlets** list to change which Fixlets are shown.
e. Click **Next**.

4. **Step 3: Devices.** Choose the devices that receive the remediation. The wizard lists the devices that the selected Fixlets apply to.

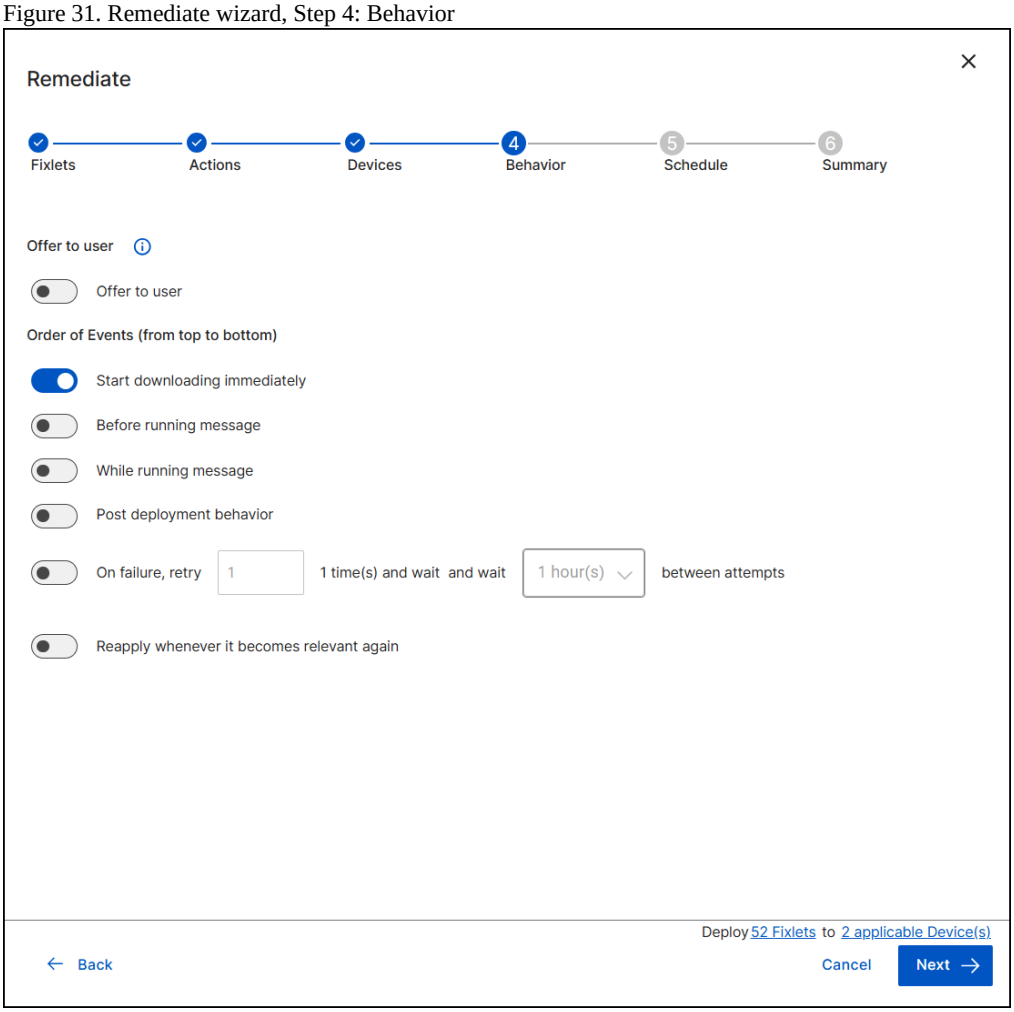
Figure 30. Remediate wizard, Step 3: Devices




a. Under **Filter By**, click **Query**, **Device group**, or **Device list** to narrow the targets. For device groups, see Device Groups. With **Query**, you build conditions from device properties.
b. Optional: Turn on **Dynamic targeting device** to also include devices that meet your criteria later.
c. In the **Select the devices to remediate** table, confirm the final list of devices. The table shows the **Device Name**, **ID**, **DNS Name**, **IP Address**, and **Last Report Time**. The bottom of the wizard summarizes the deployment, for example, "Deploy 52 Fixlets to 2 applicable Device(s)".
d. Click **Next**.

5. **Step 4: Behavior.** Set how the deployment runs. The wizard runs the events that you turn on in the order listed, from top to bottom. Turn on the events that you need:

Figure 31. Remediate wizard, Step 4: Behavior

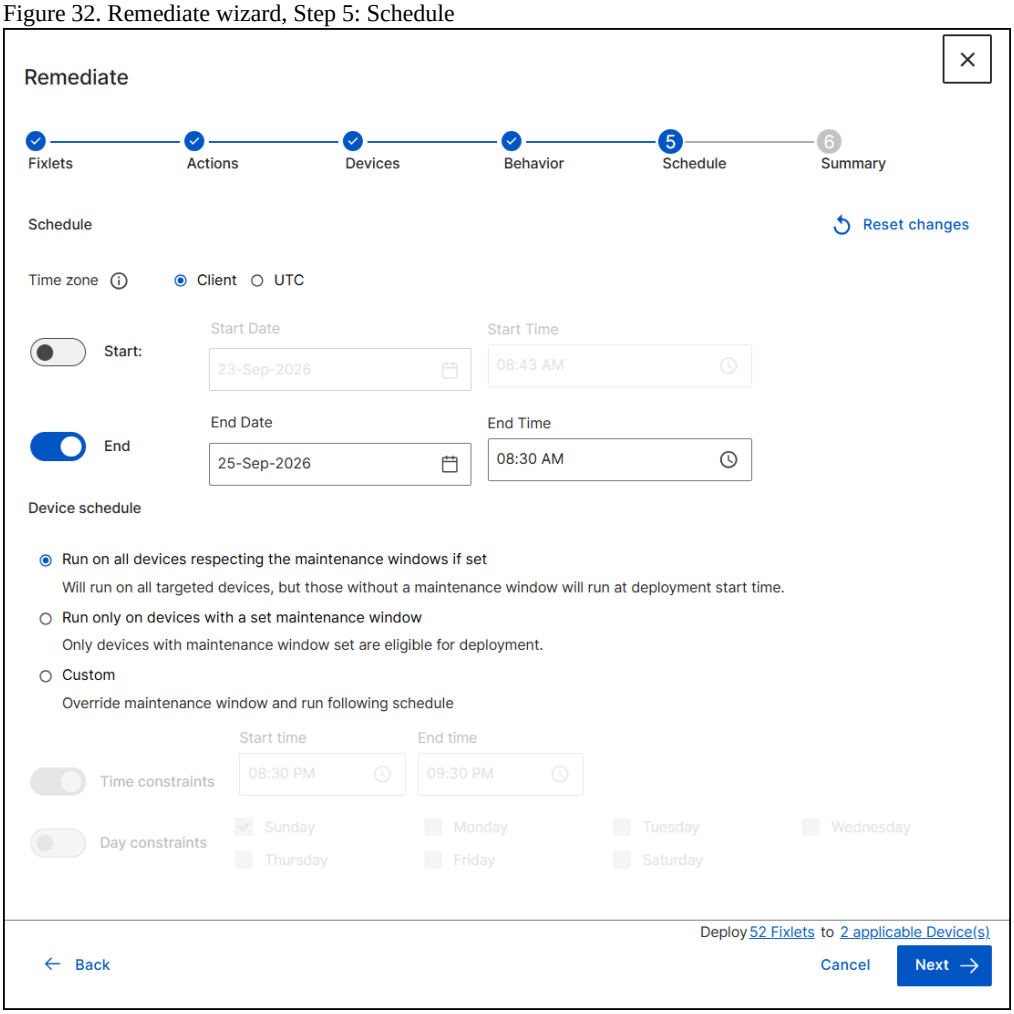



- **Offer to user**: offers the deployment to the users of the devices.
- **Start downloading immediately**: on by default. Downloads the deployment files right away, before the scheduled start.
- **Before running message**: displays a message on the targeted devices before the deployment runs.
- **While running message**: displays a message on the targeted devices while the deployment runs.
- **Post deployment behavior**: sets what happens after the deployment finishes. If you leave it off, the **Summary** shows "Do nothing after action completes".
- **On failure, retry**: retries a failed deployment. Enter the number of retries and the wait time between attempts.
- **Reapply whenever it becomes relevant again**: runs the action again if a device becomes relevant for the Fixlet again.

Click **Next**.

6. **Step 5: Schedule.** Set when the deployment runs.

Figure 32. Remediate wizard, Step 5: Schedule

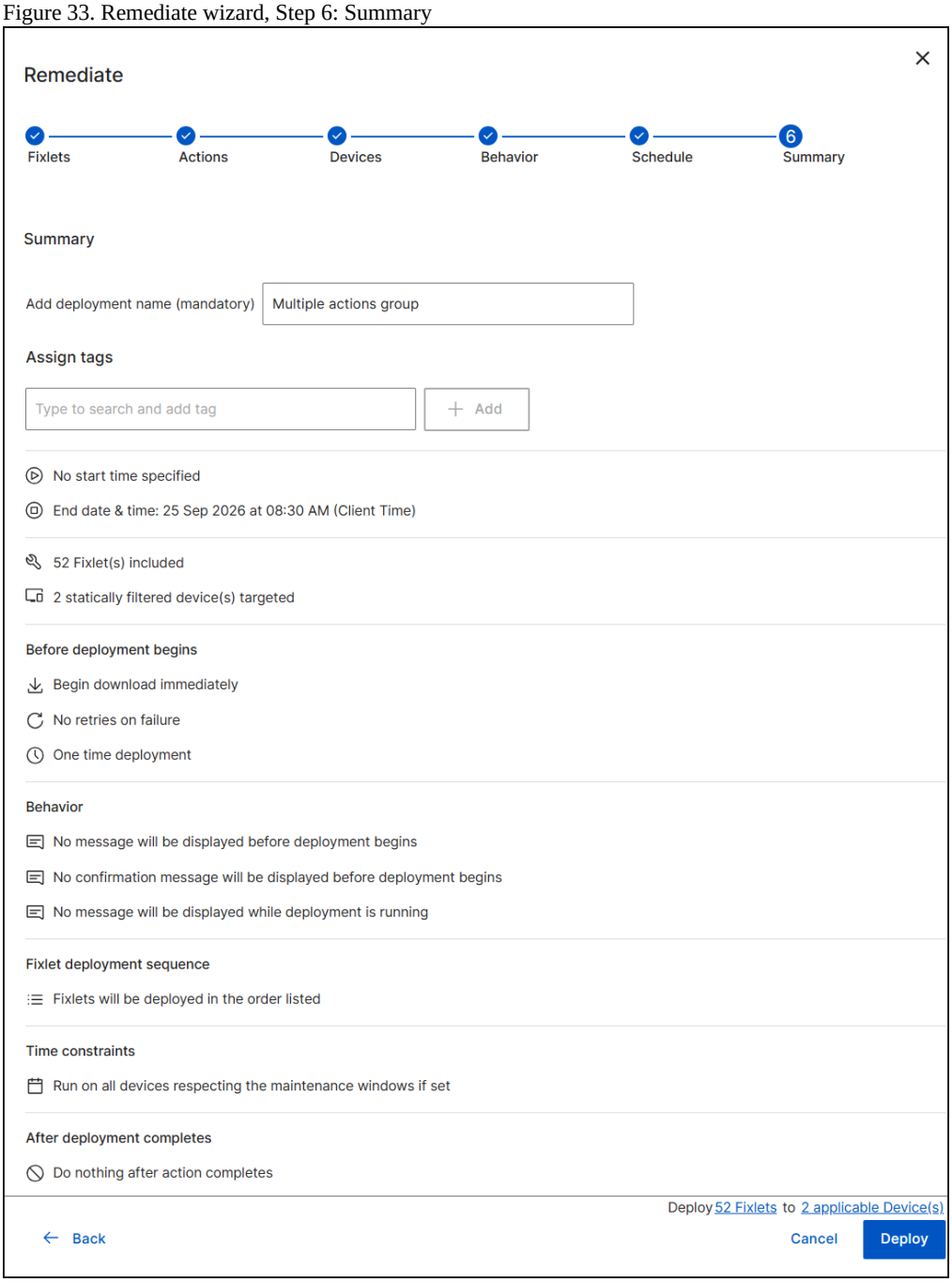



a. For **Time zone**, select **Client** to use each device's local time, or **UTC** to use Coordinated Universal Time.
b. Optional: Turn on **Start** and **End**, and then enter the date and time for each. If you leave **Start** off, the deployment has no specified start time.
c. Under **Device schedule**, select one option:
   - **Run on all devices respecting the maintenance windows if set**: the deployment runs on all targeted devices. Devices that have no maintenance window run at the deployment start time.
   - **Run only on devices with a set maintenance window**: only devices that have a maintenance window are eligible.
   - **Custom**: overrides maintenance windows and follows your schedule. Turn on **Time constraints** to set a start and end time, and **Day constraints** to select the days of the week.
d. Click **Next**.

   For maintenance windows, see Managing Device Maintenance Windows.

7. **Step 6: Summary.** Name the deployment, review your choices, and deploy.

Figure 33. Remediate wizard, Step 6: Summary



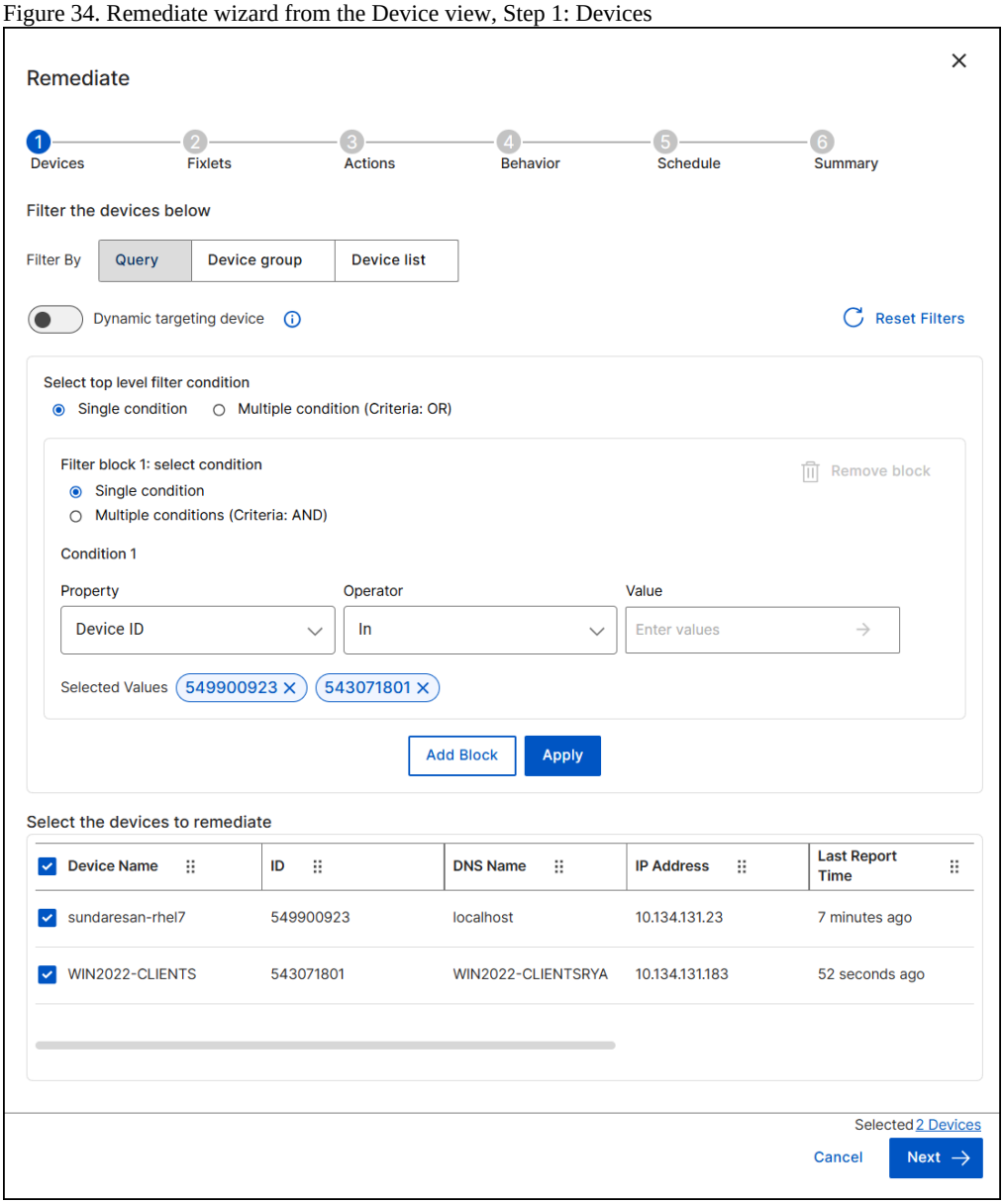

a. In **Add deployment name (mandatory)**, enter a unique name for the deployment.
b. Optional: Under **Assign tags**, type to search for a tag, and then click **Add**.
c. Review the summary: the schedule, the number of Fixlets and devices, the settings that apply before the deployment begins, the messages that display, the Fixlet deployment sequence, the time constraints, and what happens after the deployment completes.
d. Click **Deploy**.

**Result:** IVR submits the deployment.

**Remediate from the Device view**

1. Open the **Device view** tab.
2. Select the check box for each device that you want to remediate, and then click **Remediate**. The **Remediate** wizard opens at the **Devices** step.

Figure 34. Remediate wizard from the Device view, Step 1: Devices




3. **Devices:** This step looks like Step 3 of the Vulnerability view flow, with your selection already applied as a filter condition (for example, **Device ID In** the IDs of the devices that you selected). To change the targets, use **Query**, **Device group**, or **Device list**, or turn on **Dynamic targeting device**. Click **Next**.
4. **Fixlets:** select the Fixlets to deploy to the devices, and then click **Next**.
5. Complete the **Actions**, **Behavior**, **Schedule**, and **Summary** steps as described in Remediate from the Vulnerability view, and then click **Deploy**.

**Monitor the deployment**

To track the status of a deployment, use either of these:

- The **Deployment** tab of the vulnerability details page. It lists each deployment with its name, status (for example, Active, Completed, or Expired), start time, and the user who started it.
- **Deployment Manager**, which also shows the targeted devices and deployed Fixlets. See Deployments.

# Chapter 8. Configuration settings for IVR on-prem

The following settings in AppConfig.yaml control the IVR v.5 on-prem application. To change a setting, stop the BES IVR Retriever Service, edit the file, and then start the service.

**Note:** Change the web protocol, local web server port, CORS allowed origins, and proxy settings in the BigFix UI. See Managing the IVR configuration *(on page 23)*.

### `AppConfig.yaml`

| Setting name | Data type | Default value | Description |
|---|---|---|---|
| **Configs** | | | |
| ByPassCertificateVerification | Boolean | TRUE | Specifies whether to bypass certificate verification. Possible values: TRUE, FALSE. |
| CorsAllowedOrigins | String | '*' | The origins allowed for CORS. Managed from the BigFix UI (**Application configuration**). Don't edit it here. |
| LogCompression | Boolean | TRUE | Specifies whether to compress rotated log files. Compressed logs use the `.gz` format. Use a tool such as 7-Zip to open them. |
| LogMaxAgeDays | Int | 15 | The maximum age of log files, in days. |
| LogMaxBackups | Int | 100 | The maximum number of log backups to keep. |
| LogMaxSizeMb | Int | 10 | The maximum size of a log file, in megabytes. |
| Port | Int | 9011 | The port number for the application. |
| **EngConfigs** | | | |
| Port | Int | 9014 | The port number for the EngConfigs service. |
| WebServer | String | 127.0.0.1 | The server that hosts this service. |
| AutomationIntervalHours | Int | 12 | The interval, in hours, between automation runs. |

# Chapter 9. IVR logs

This section describes the IVR logs.

The logs are in `C:\Program Files (x86)\BigFix Enterprise\BESIvrRetriever\data\logs`.

### `AppConfig.log`

This log lists the application configuration and settings that IVR used at runtime during the last run, and is updated when you modify `AppConfig.yaml` while the application is running.

**Important:** IVR writes this log only when the application runs with the `--printconfig` flag. This requirement prevents unintentional disclosure of settings.

### `ivrn.log`

This is the main application log. Debug (verbose) logging is off by default. To turn it on, set `LogVerbose` to `true` in the Settings section of `AppConfig.yaml`.

When the file reaches its maximum size (set in `AppConfig.yaml`), the log rotates: IVR adds the date and time to the current `ivrn.log` file name and starts a new `ivrn.log`.

**Note:** When the BigFix UI reports a configuration or automation error, check the BigFix UI logs as well as the IVR logs.

# Chapter 10. Troubleshooting

Use this section to diagnose and resolve common problems with IVR v.5.

One or more of these symptoms occurs. Each symptom has a likely cause and a recommended action, listed in the following table.

Various causes, described in the table below.

| Symptom | Likely cause | What to do |
|---|---|---|
| IVR shows **IVR is not configured**. | The IVR configuration isn't complete. | Complete the IVR v.5 setup process *(on page 14)*, or ask your administrator to. |
| IVR doesn't appear under Resolve. | The IVR site isn't enabled, its version is 0, or the user's role doesn't include IVR. | See Before you begin *(on page 8)* for the site, and Task 3 *(on page 20)* for the role. |
| IVR isn't listed when you create a role. | The IVR site isn't enabled. | See Before you begin *(on page 8)*, steps 1-3. |
| `BFUI.exe --configure-ivr` fails at authentication. | Wrong instance admin or IVR admin credentials. | Run the command again with the BigFix UI instance admin credentials and the IVR credentials from the Download Task. |
| Verify Connection fails on Database Configuration. | Wrong SQL Server values, the port is blocked, or the user can't create a schema. | Check the values and firewall, and grant the user permission to create a schema. |
| Verify Connection fails on Application configuration. | The local web server port is in use or blocked, or the proxy settings are wrong. | Choose a free, open port, and check the proxy host and port. |
| Verify Connection fails on Scanner Datasource configuration. | Wrong Tenable URL or API keys, or outbound access to Tenable is blocked. | Regenerate the API keys with a Tenable administrator account, and check outbound access on port 443 or the proxy. |
| The IVR tile stays in Not Configured after Finish. | A background automation process failed. | See the failure result in Task 2 *(on page 15)*. |
| The dashboard shows no data. | The first automation run isn't complete. | Wait until Last Automation Run shows a time. |
| The Device view shows no devices. | The IVR Vulnerability Scanner Host ID analysis isn't activated. | See Before you begin *(on page 8)*, step 4. |
| Configuration changes, such as a new proxy, don't take effect. | The IVR service wasn't restarted. | See Managing the IVR configuration *(on page 23)*, step 4. |
| The Vulnerabilities tab is missing in Device Explorer. | The IVR site isn't enabled. | See Before you begin *(on page 8)*, steps 1-3. |

# Chapter 11. Release notes

This section lists the features and updates in each version of BigFix Integrated Vulnerability Remediation v.5.

### IVR 5.0.0.0

IVR 5.0.0.0 is the first release of IVR on the BigFix UI. It includes:

- **Integrated Vulnerability Remediation** in the BigFix UI, under **Resolve** in the left navigation pane.
- Setup with `BFUI.exe --configure-ivr` and the configuration wizard in **Administration** > **Application Configuration**.
- An IVR schema in the BigFix UI database.
- Access control through BigFix UI roles.
- The Device view, grid search, and the **Last Automation Run** and **Next Expected Automation Run** indicators.
- A **Vulnerabilities** tab in Device Explorer.

# Chapter 12. Known limitations

This section lists the known limitations in IVR v.5.

- IVR supports one scanner data source per instance, and Tenable Vulnerability Management is the only supported scanner.

# Chapter 13. References

Additional resources related to BigFix Integrated Vulnerability Remediation (IVR) v.5.

- Video: Install and configure IVR v.5 with Tenable Vulnerability Management
- BigFix UI Administration Guide
- BigFix UI User's Guide: Application Configuration
- BigFix UI User's Guide: Identity management
- BigFix UI User's Guide: User & Role Management and Managing Roles
- BigFix UI User's Guide: Device Details Page and Deployments
- BigFix UI User's Guide: Integrated Vulnerability Remediation (IVR summary page)