



Configuring Security Mitigation Settings for Security Bulletin HPSBPI03569

Protecting Solution Installation Settings

Table of contents

Overview	2
Using the Embedded Web Server (EWS)	2
Set the local administrator password.....	2
Disable “Allow firmware updates sent as print jobs (port 9100)”	4
Using HP Web Jetadmin to configure multiple devices	6
Discovering devices in Web Jetadmin	6
Creating and Adding Devices to a Web Jetadmin Group	11
Creating a Web Jetadmin template for Security Migration Settings	13
Applying the Web Jetadmin template for Security Migration Settings	16

Overview

This document provides instructions for mitigation steps you can take to prevent exposure to the remote code execution vulnerability (CVE-2017-2750). These instructions apply to HP Enterprise printers and multi-function printers running FutureSmart version 3 and FutureSmart version 4. Configure the following two settings:

- Set the Local Administrator password for the Embedded Web Server (EWS). A password must be configured before access to the Solution Installer is permitted.
- Disable the “Allow firmware updates sent as print jobs (Port 9100)” setting in the EWS. This prevents solution packages from being uploaded through the firmware update method.

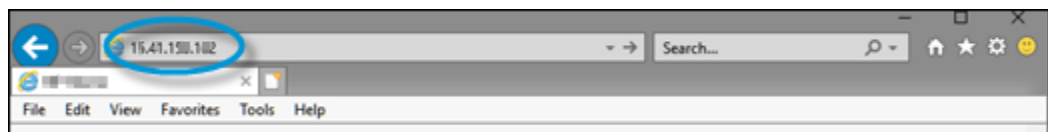
Using the Embedded Web Server (EWS)

Set the local administrator password

To allow access to the Solution Installer, follow the steps below to set the local administrator password for the Embedded Web Server (EWS).

1. Open a web browser and enter the printer IP Address or host name in the browser address field. If you do not know what the IP Address or host name is, ask your administrator.

Figure 1: Entering the IP Address



NOTE:

If a certificate warning appears, proceed to the printer EWS. A certificate warning is normal if the printer is using a self-signed certificate.

2. Select the **Security** tab. By default, **General Security** will be selected in the left panel.

Figure 2: Selecting the Security tab in the EWS

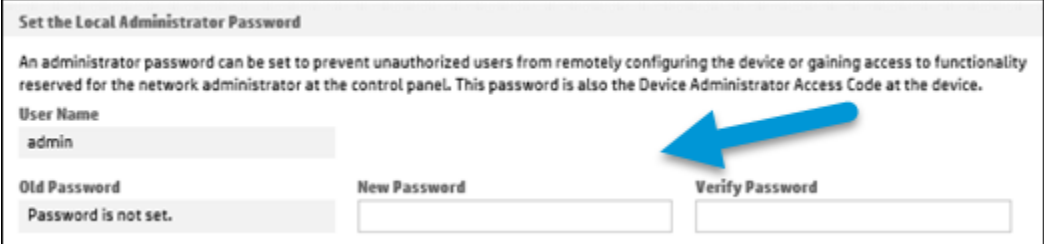


NOTE:

If a password is required, click the Sign In button, sign in, and then skip the next two steps.

3. In the **Set the Local Administrator Password** section of **General Security**, set the local administrator password in the **New Password** and **Verify Password** fields.

Figure 3: Setting the password



Set the Local Administrator Password

An administrator password can be set to prevent unauthorized users from remotely configuring the device or gaining access to functionality reserved for the network administrator at the control panel. This password is also the Device Administrator Access Code at the device.

User Name
admin

Old Password
Password is not set.

New Password

Verify Password


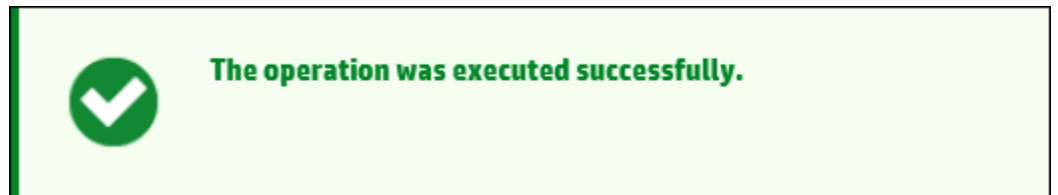
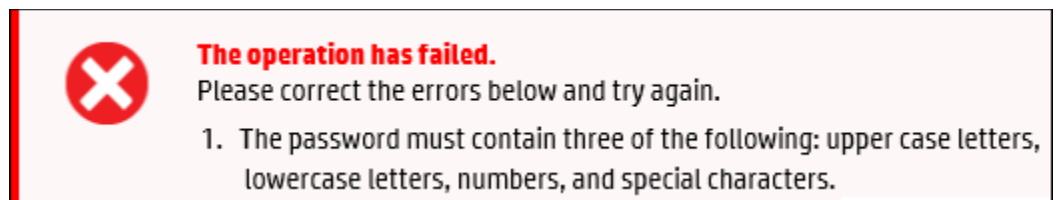
4. Click the **Apply**  button in the bottom right area of the EWS. If successful, a confirmation message appears at the top of the page.

Figure 4: The success message



Print devices running FuturesSmart 4 require a complex password with a minimum of eight characters, and must contain a combination of three of the following: uppercase letters, lowercase letters, numbers, and special characters. Otherwise, a failure message will appear.

Figure 5: The password reset failure message



5. To change password complexity requirements, click **Account Policy** in the left panel and update the fields under **Local Administrator Password**.

Figure 6: Changing password complexity requirements

The screenshot shows the 'Account Policy' dialog box with the 'Local Administrator Password' section selected. The 'Enable account lockout' checkbox is checked. Below it are three input fields: 'Maximum attempts' with the value '5' (range 3-30), 'Lockout interval' with the value '10' (range 5-1800 seconds), and 'Reset lockout counter interval' with the value '10' (range 0-1800 seconds). The 'Enable password complexity' checkbox is also checked. Below this, a note states: 'When checked, the password must contain three of the following: uppercase letters, lowercase letters, numbers, and special characters.' The 'Minimum password length' field is set to '0', and a blue arrow points to this field. A note below the field states: 'Zero (0) indicates that the minimum password length is disabled; no password is required.' At the bottom right, there are 'Apply' and 'Cancel' buttons.

Disable “Allow firmware updates sent as print jobs (port 9100)”

1. Open a web browser and enter the printer IP Address or host name in the browser address field. If you do not know what the IP Address or host name is, ask your administrator.

NOTE:

If a certificate warning appears, proceed to the printer EWS. A certificate warning is normal if the printer is using a self-signed certificate.

2. Select the **Security** tab. By default, **General Security** will be selected in the left panel.
3. In the **Firmware Upgrade Security** section of General Security, uncheck **Allow firmware updates sent as print jobs (port 9100)**. This also prevents sending print solution and device firmware over certain paths.

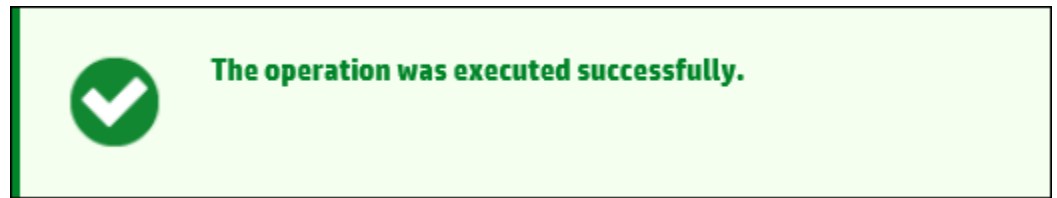
Figure 7: Disabling firmware upgrades sent as print jobs

The screenshot shows the 'Firmware Upgrade Security' section of the EWS. It contains a single checkbox labeled 'Allow firmware upgrades sent as print jobs (port 9100)', which is currently unchecked.

4. Click the **Apply** button in the bottom right area of the EWS.

If successful, a confirmation message appears at the top of the page.

Figure 8: The success message



Using HP Web Jetadmin to configure multiple devices

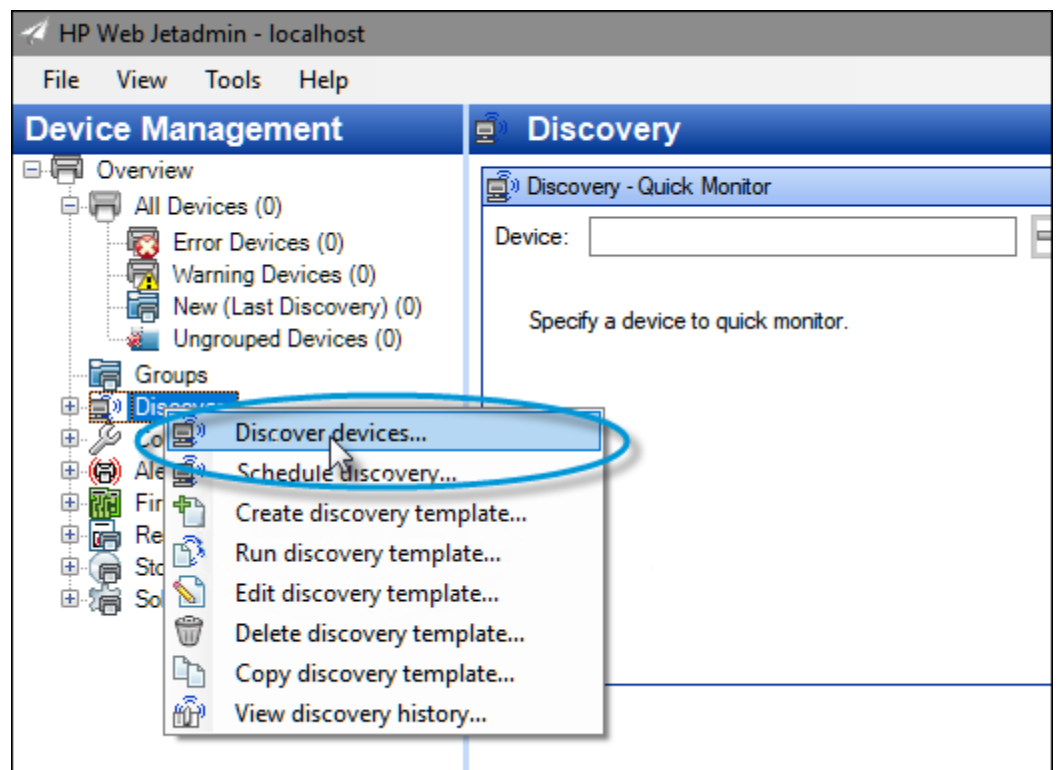
HP's Web Jetadmin fleet management tool can be used to set the two remediation settings simultaneously across multiple devices. The HP Web Jetadmin software is a free tool and is available for download at www.hp.com/go/webjetadmin.

HP Web Jetadmin can be installed on a single workstation or can be installed as a client-server application in an enterprise environment.

Discovering devices in Web Jetadmin

1. In the **Device Management** navigation panel, right-click **Discovery**, and then select **Discover devices**.

Figure 9: Launching the Device Discovery wizard

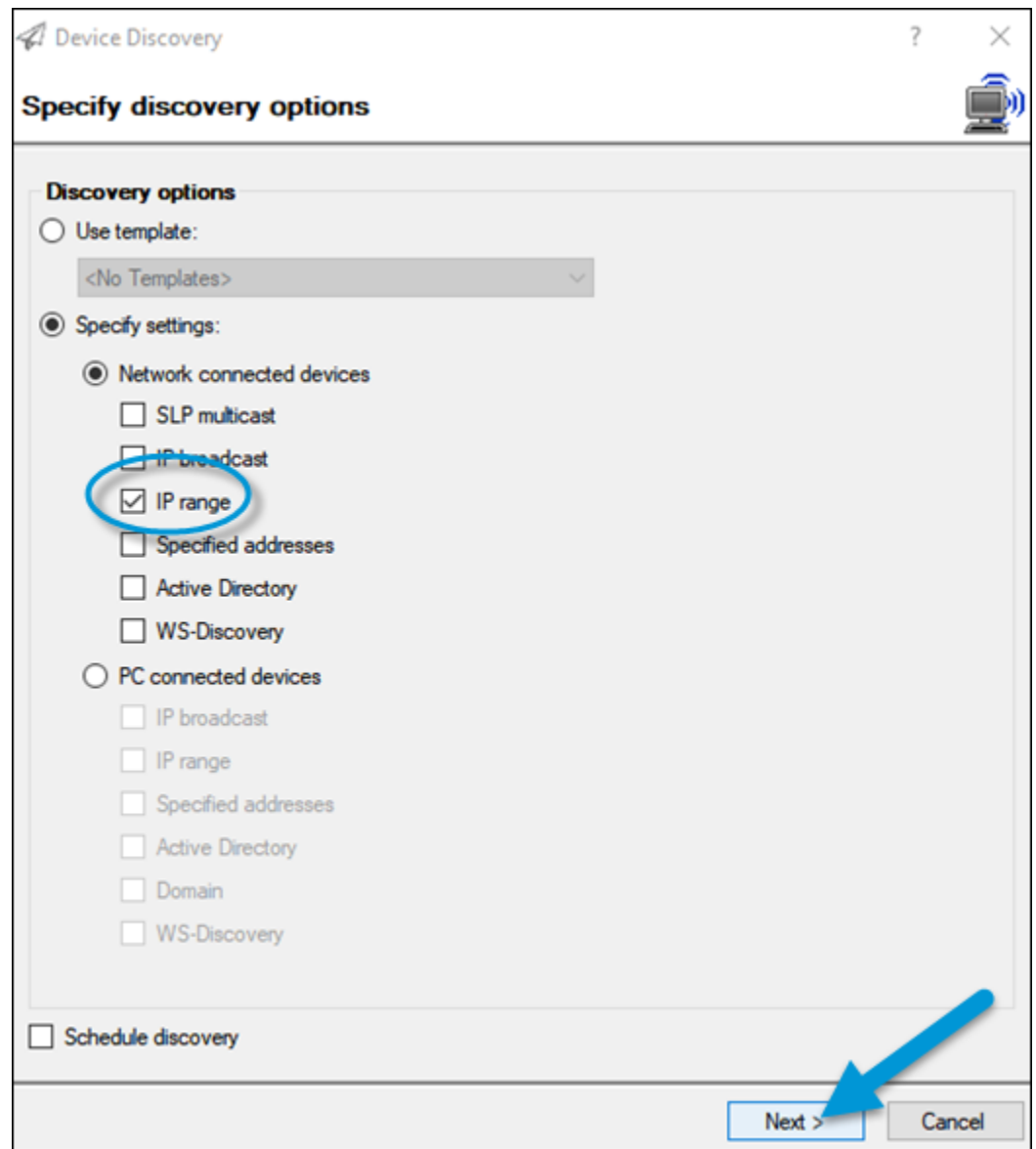


The Device Discovery wizard starts.

2. Select the **Network connected devices** option.

3. Select the **IP range** check box and click the **Next** button.

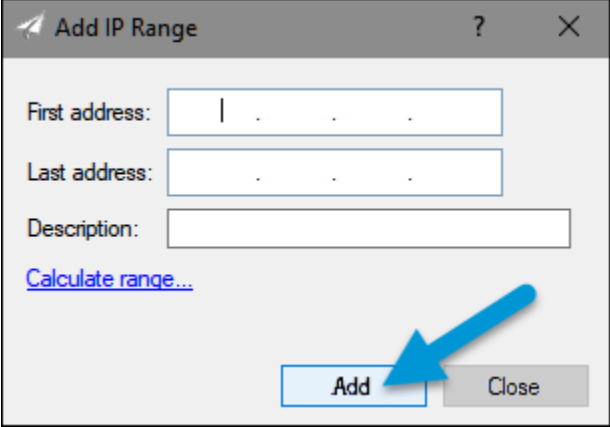
Figure 10: Specifying discovery options



4. Click the **Add** button in the **Select IP ranges** dialog.

5. In the **Add IP Range** panel, enter a starting and ending IP range in the **First address** and **Last address** fields, and then click the **Add** button.

Figure 11: Adding the IP address range



The screenshot shows a dialog box titled "Add IP Range". It features three input fields: "First address:" with a cursor in the first octet, "Last address:" with a cursor in the first octet, and "Description:". Below these fields is a blue link labeled "Calculate range...". At the bottom of the dialog are two buttons: "Add" and "Close". A blue arrow points to the "Add" button.

6. Click the **Close** button on the **Add IP Range** panel, then click the **Next** button.
7. If a SNMPv1 get community name is configured for print devices, select **Specify credentials**.

8. Select the **SNMPv1 Get Community Name** checkbox, enter the get community name in the field, and then click **Next**.

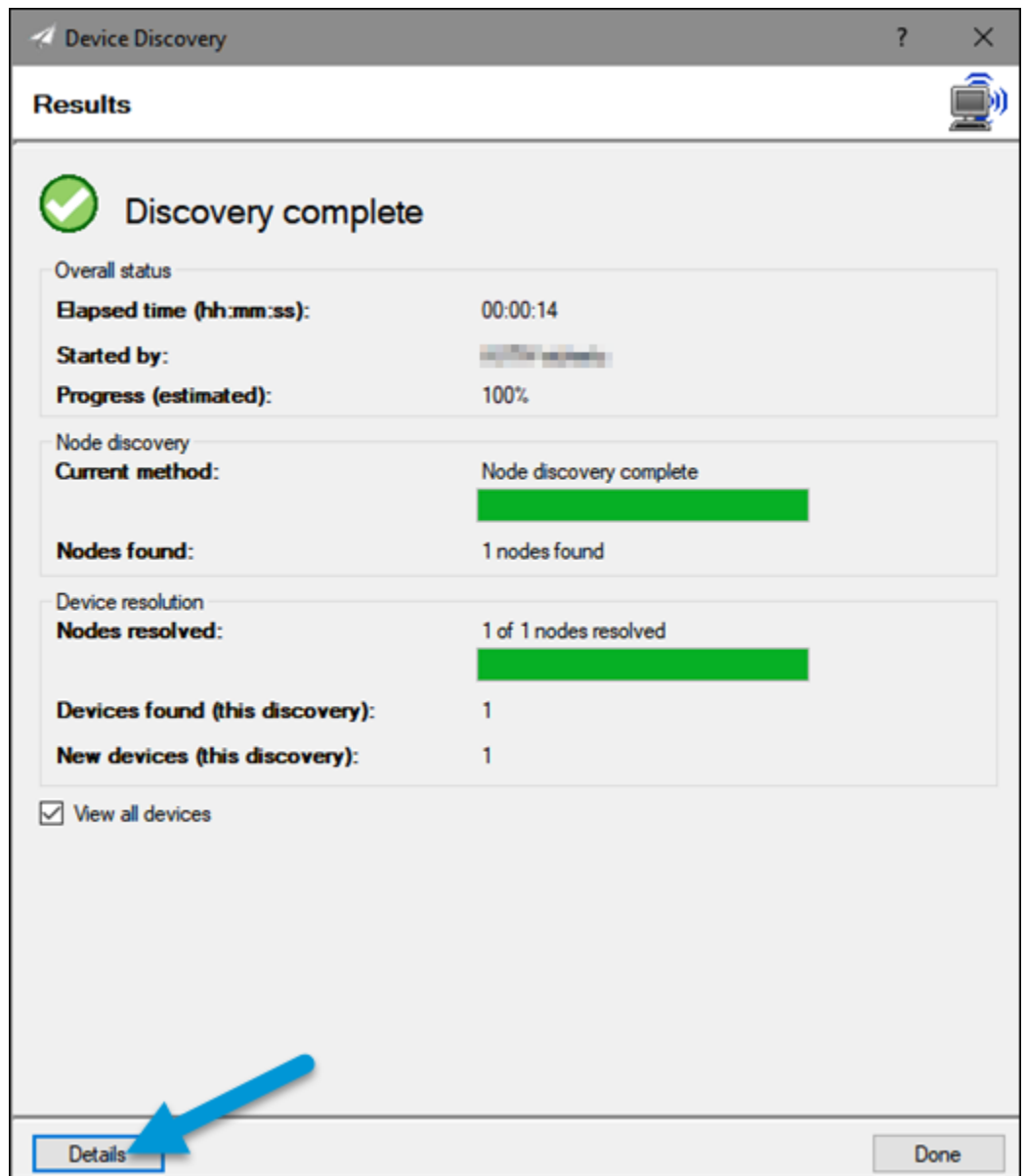
Figure 12: Entering the Get Community Name

The screenshot shows a window titled "Device Discovery" with a "Specify credentials" section. In this section, the radio button "Specify credentials to use for this discovery" is selected. Below it, the "SNMPv1 Get Community Name" checkbox is checked, and there is an empty text input field. The "Global credentials" section has the "Use global credentials" checkbox unchecked. At the bottom right, there are three buttons: "< Back", "Next", and "Cancel". A blue circle highlights the "Specify credentials to use for this discovery" section, and a blue arrow points to the "Next" button.

9. Select **Start** to begin device discovery.

10. Click the **Details** button in the lower-left area to view discovered devices.

Figure 13: Viewing details for discovered devices

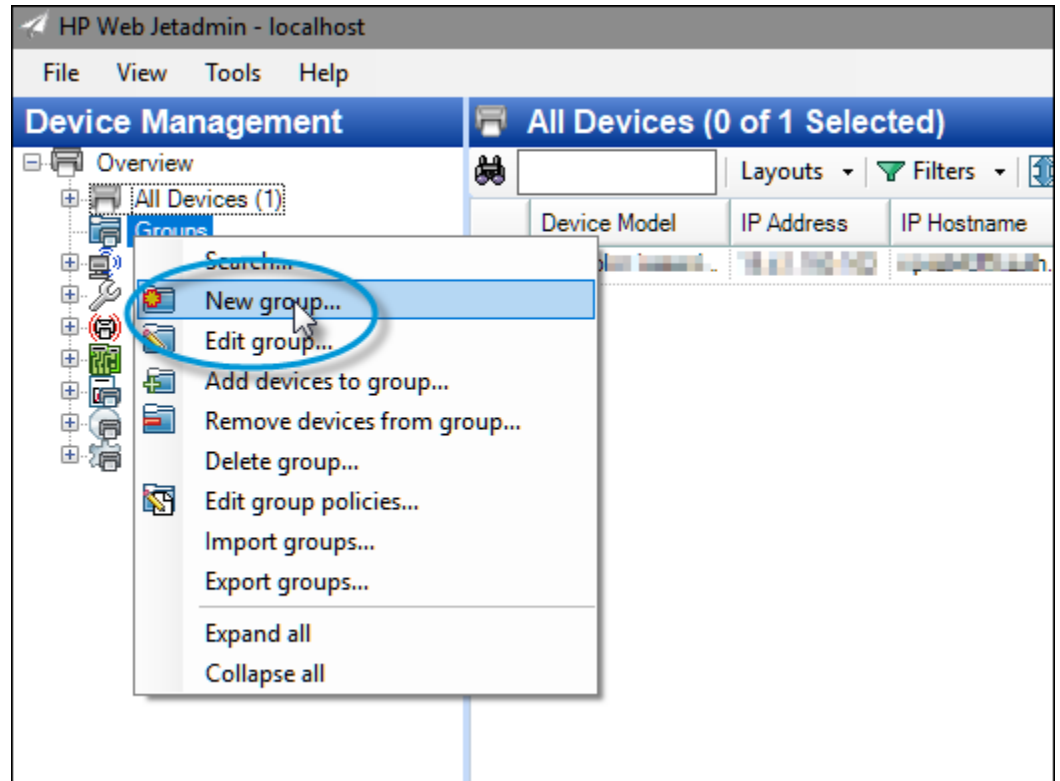


11. Close the **Discover Results** dialog and click the **Done** button.

Creating and Adding Devices to a Web Jetadmin Group

1. In the **Device Management** navigation panel, right-click **Groups**, and then select **New Group**.

Figure 14: Creating a new group

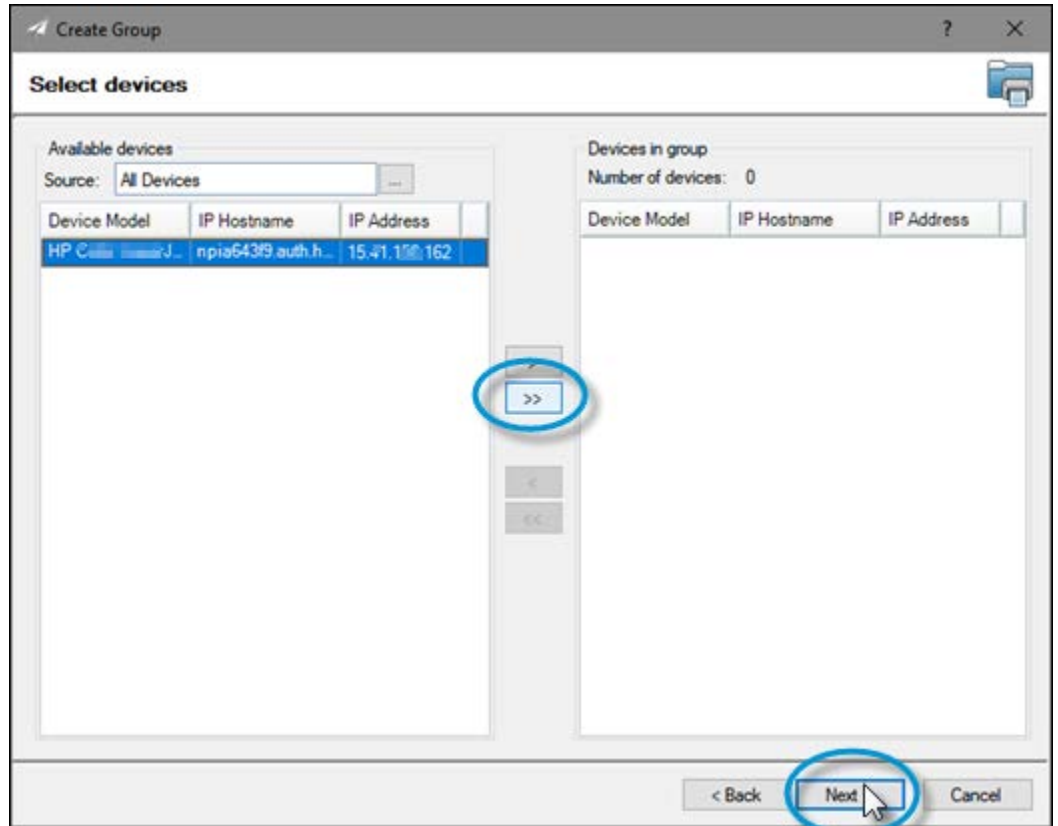


The Create Group wizard starts.

2. Enter RCE Security Template in the **Group Name** field.
3. Select the **Configure group properties now** checkbox, then click the **Next** button.
4. Press the CTRL plus A buttons to select all of the devices in the **Available devices** panel.

- To add the devices to the **Devices in group** list, click the double-arrow **>>** button, and then click the **Next** button.

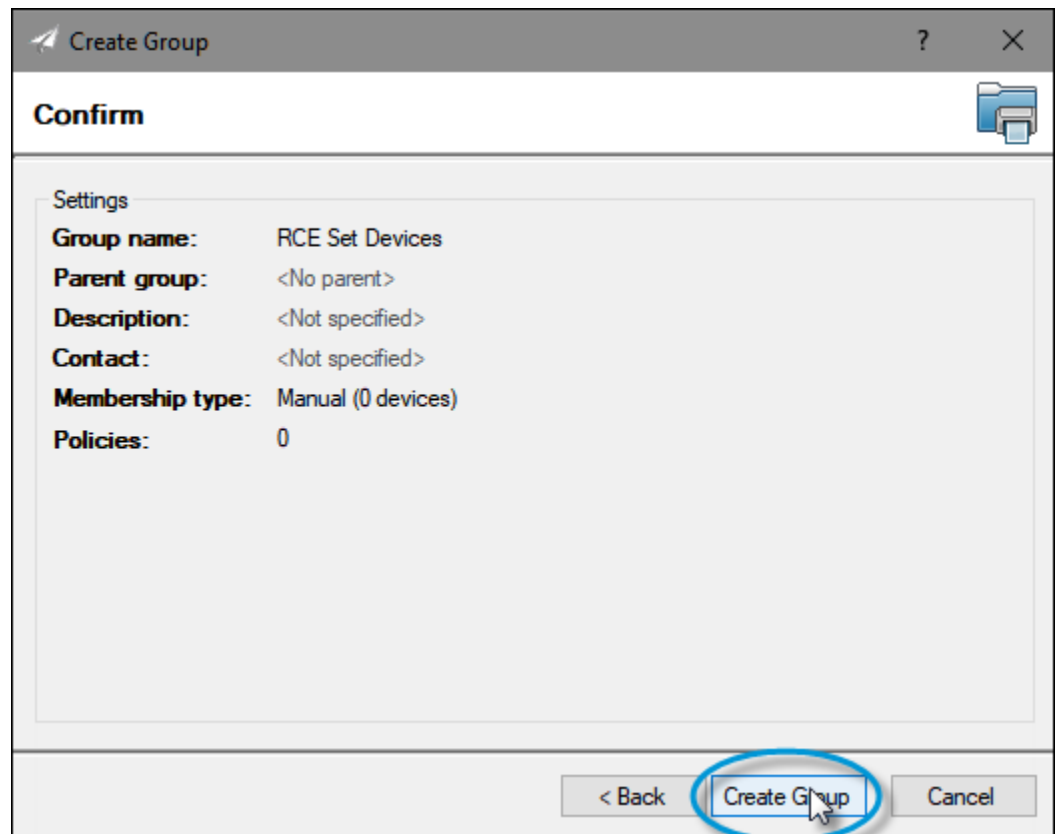
Figure 15: Selecting devices



- Enter a group description, then click the **Next** button.
- Click the **Next** button in the **Configure Group Policies** dialog.

8. Click the **Create Group** button in the **Confirm** dialog, then select **Done**.

Figure 16: Creating a group

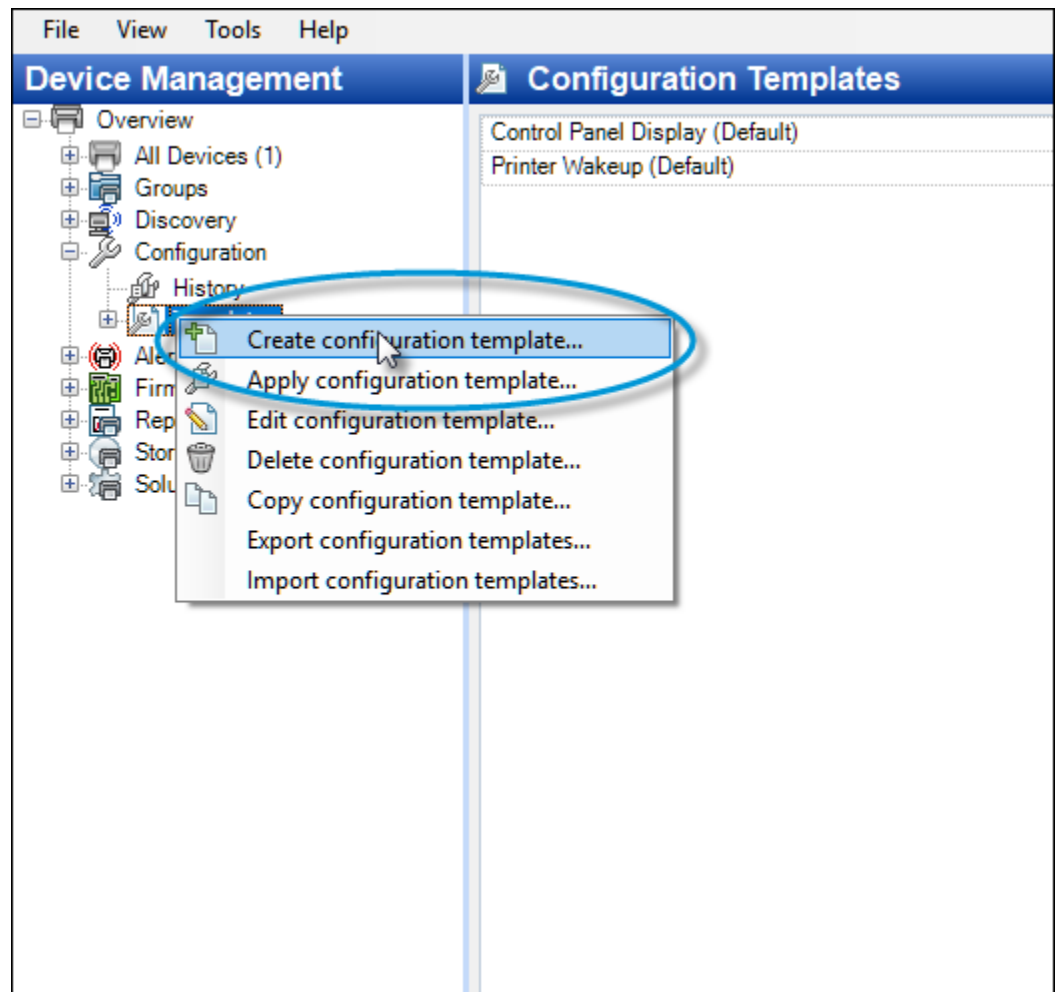


Creating a Web Jetadmin template for Security Migration Settings

1. In the **Device Management** navigation panel, click the plus sign \oplus next to **Configuration** to expand the menu.

2. Right-click **Templates** and select **Create configuration template**.

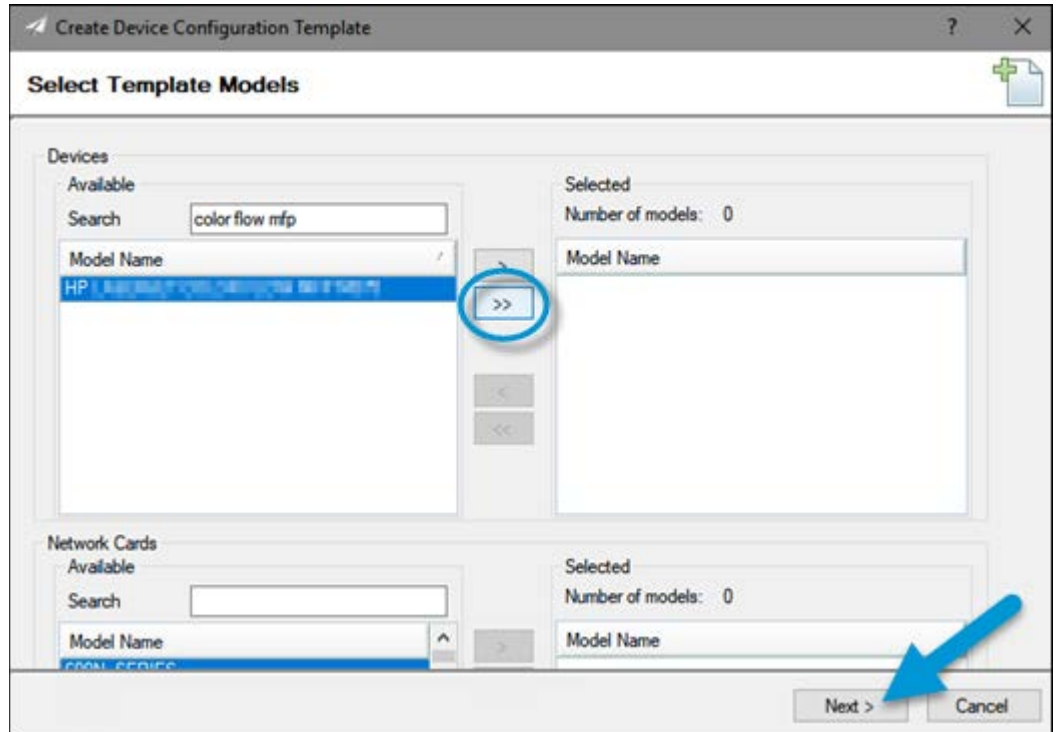
Figure 17: Creating the configuration template



3. In the **Select Template Models** dialog, select the desired printing device models or use the **Search** field to locate specific printer models.

- To add models to the **Selected** list, click the model name in the **Available** list, click the double-arrow >> button, and then click **Next**.

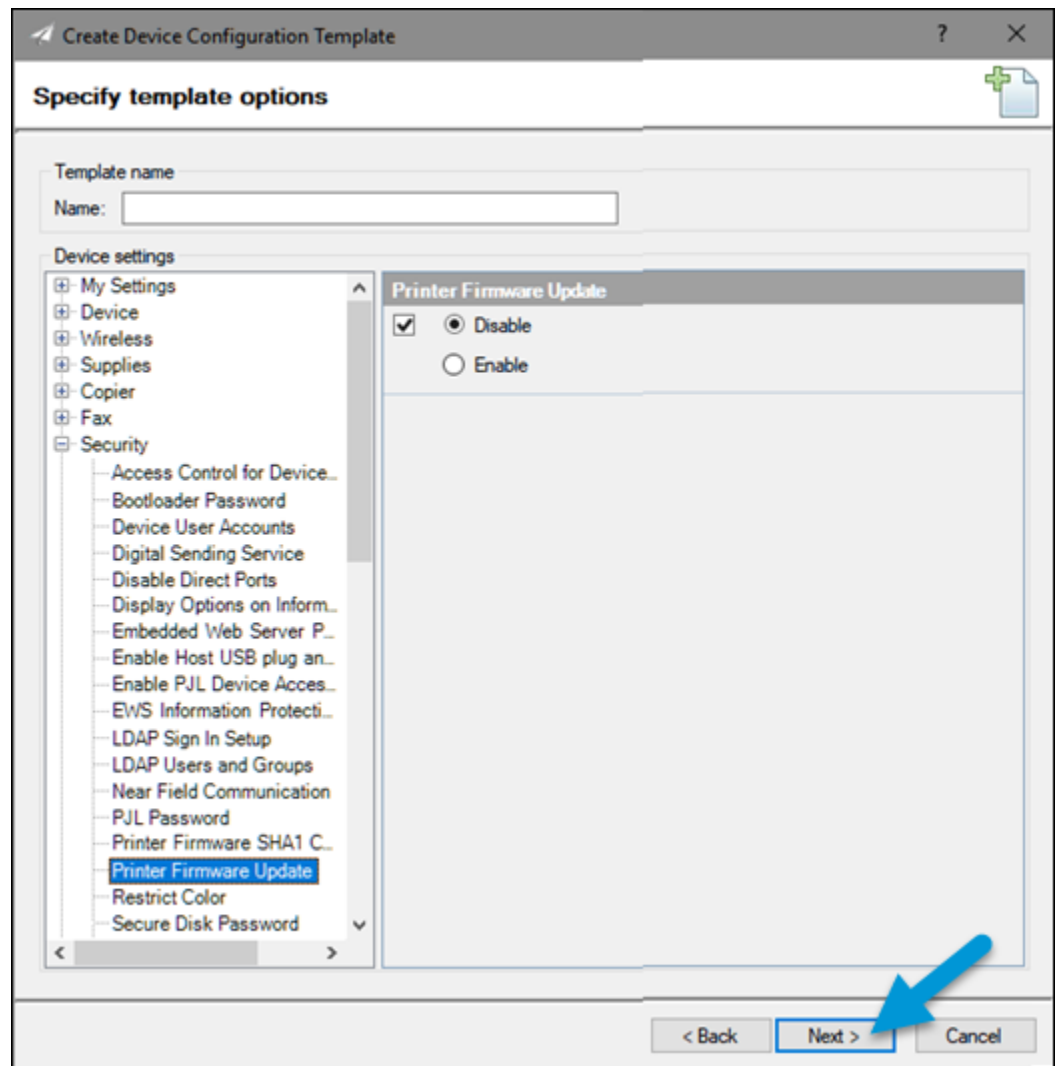
Figure 18: Adding devices



- Enter RCE Security Template in the **Template Name** field.
- In the **Device Settings** list, click the plus sign ⊕ next to **Security** to expand the list.
- Select the **Embedded Web Server Password** setting, and enter a password in the **Password** and **Confirm Password** fields.
- Select the **Printer Firmware Update** setting, and select the **Disable** radio button.

9. Click the **Next** button.

Figure 19: Disabling Printer Firmware Update



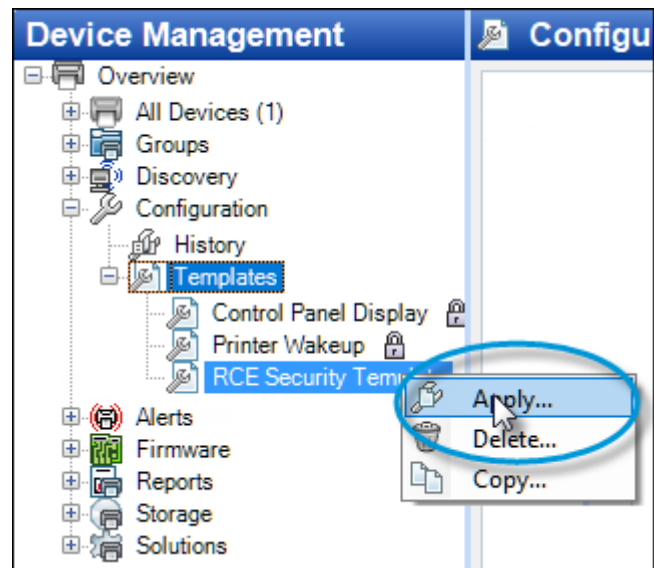
10. Select **Create Template**, then click **Done**.

Applying the Web Jetadmin template for Security Migration Settings

1. In the **Device Management** navigation panel, click the plus sign **+** next to **Configuration** to expand the menu.
2. Expand the **Templates** menu.

3. Right-click the **RCE Security Template** and select **Apply**.

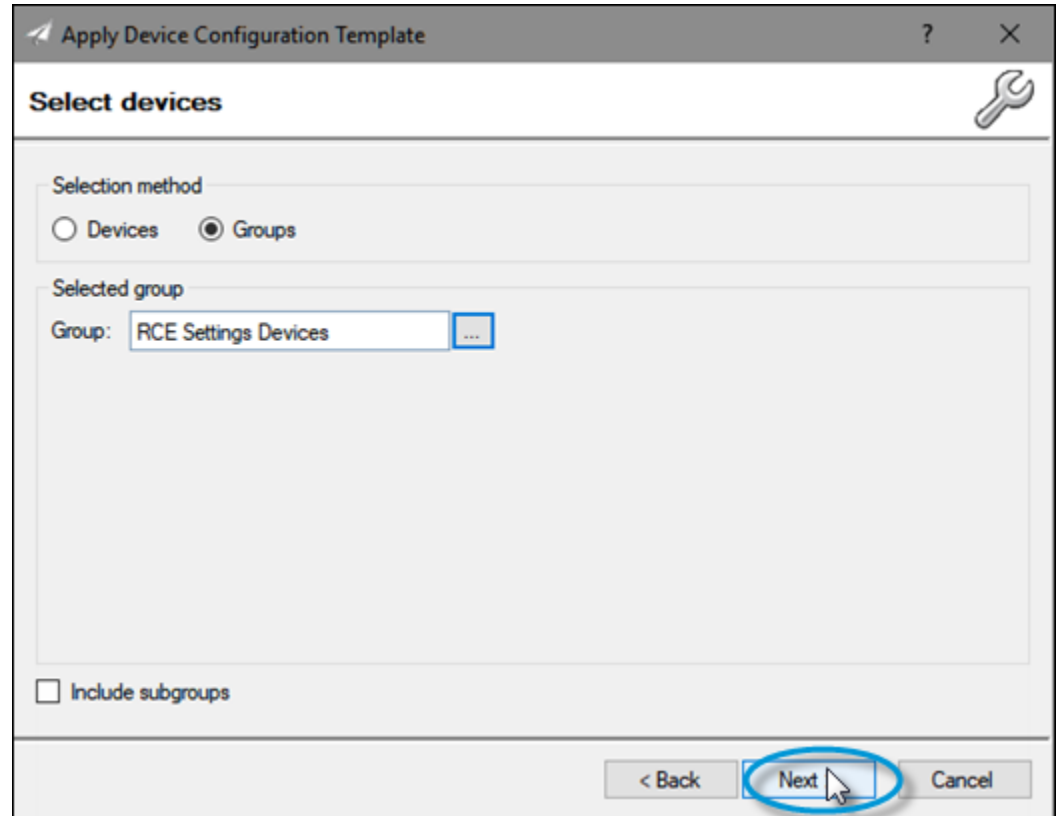
Figure 20: Applying the RCE Security Template



4. In the **Specify configuration options** dialog, click the **Next** button.
5. Select the **Groups** radio button in the **Select devices** dialog.

6. Select **RCE Settings Devices** from the **Group** drop-down list, then click the **Next** button.

Figure 21: Selecting groups



7. Click **Apply Template**.
8. Review the **Results** dialog to confirm the template settings were applied successfully.

9. Click the **Details** button to review the results or address any errors.

Figure 22: Reviewing the Device Configuration Results

