

Use the Security Cloud Control Command Line Interface Tool (CLI)

You can use the Command Line Interface tool for managing or troubleshooting devices. The commands supported with this tool depend on the type of device. For the ASA, for example, you can use the full CLI. But for the Firewall Threat Defense, command support is limited to select **show** commands.

You can send commands to a single device or to multiple devices simultaneously.

See the following supported device types:

- ASA

  Commands are entered directly in global configuration mode. For detailed ASA CLI documentation, see ASA Command Line Interface Documentation.

- Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense

  Your command will be sent to either the Firewall Threat Defense CLI or the diagnostic CLI, depending on which command it is. Supported commands for Firewall Threat Defense are shown onscreen. These commands are a subset of commands that you can enter at the CLI. In addition, you cannot filter **show** command by piping the output (|) like you can directly at the CLI or in the Threat Defense CLI tool in the Cloud-Delivered Firewall Management Center.

  For diagnostic CLI output, see the ASA command reference guide.

  For Firewall Threat Defense CLI documentation, see Cisco Firepower Threat Defense Command Reference.

- FDM-managed Firewall Threat Defense

  Commands are entered at the Firewall Threat Defense CLI. You cannot access other modes. For Firewall Threat Defense CLI documentation, see Cisco Firepower Threat Defense Command Reference.

- Cisco IOS

  Commands are entered in user EXEC mode. You need to enter **enable** followed by **configure terminal** to execute them in Global Configuration mode. For Cisco IOS CLI documentation, see Networking Software (IOS & NX-OS) for your IOS version.

- SSH

- Use the Command Line Interface on a single device, on page 2
- Use the bulk Command Line Interface, on page 4

• Run a CLI macro, on page 7
• Export Command Line Interface results, on page 10

Use the Command Line Interface on a single device

When you select a single device, you can enter one or more commands. You can also view and use command history to rerun a set of commands.

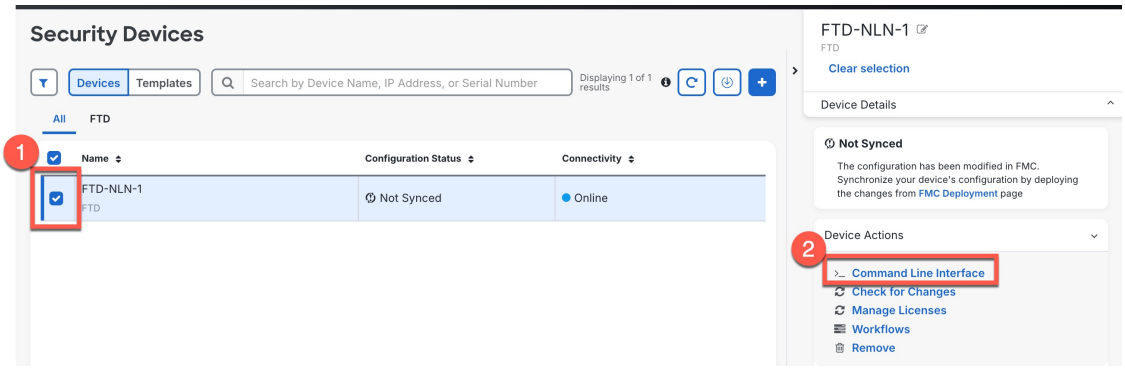
Procedure

Step 1 Choose **Inventory**.

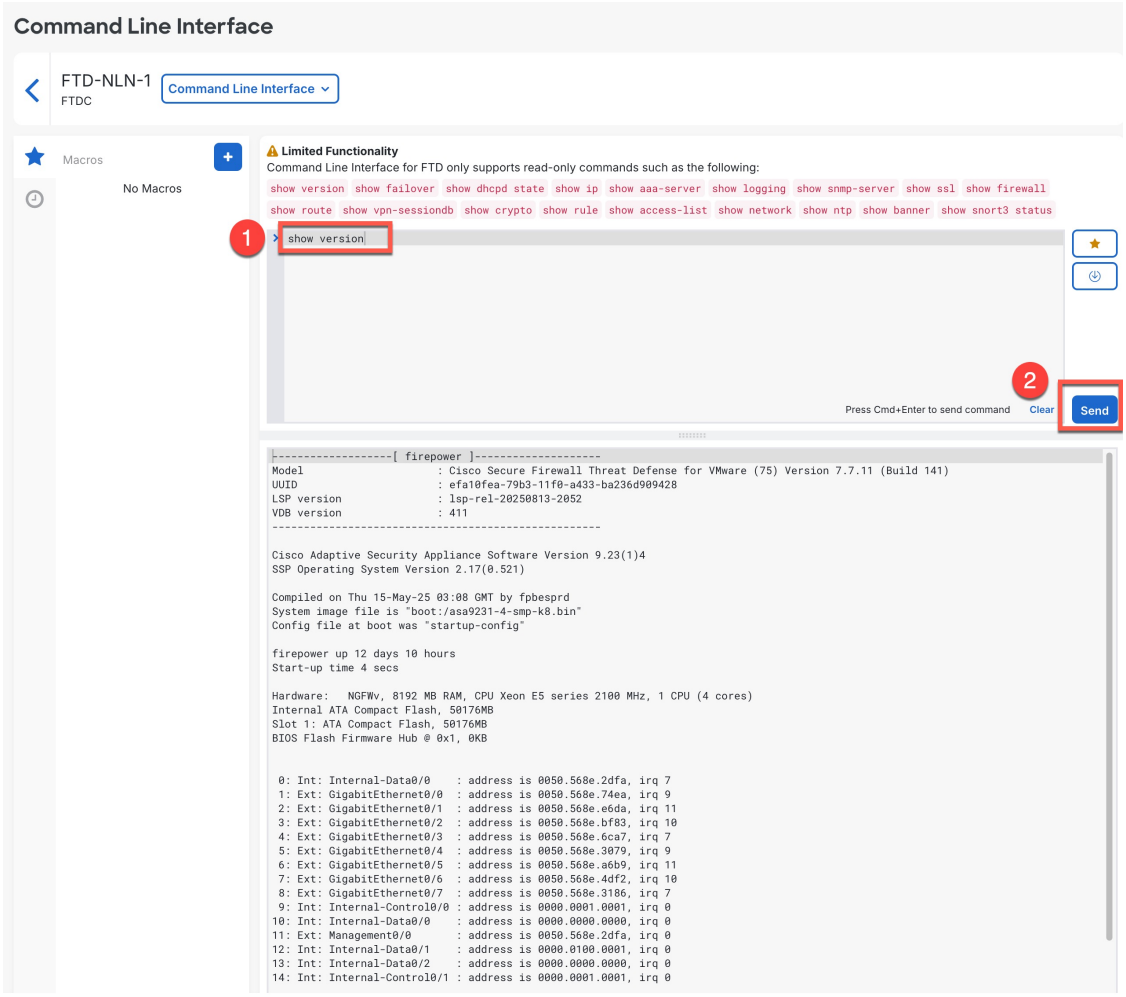
Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Select the device, and in the **Device Actions** pane, click **>_Command Line Interface.**



Step 5 Enter one or more commands in the command pane, and click **Send**.



If there are limitations on the commands you can run, they appear in the area above the command pane.

The response to your commands is displayed in the response pane. If there is no output for a command (either it was executed successfully, or there was no output to show), you will see `Done!` in the results pane.

Note
If you enter a very long list of commands, you may exceed the limitations of Security Cloud Control's interface with the device. If you see an error, you can add extra blank lines between groups of commands so Security Cloud Control can send the commands in batches.

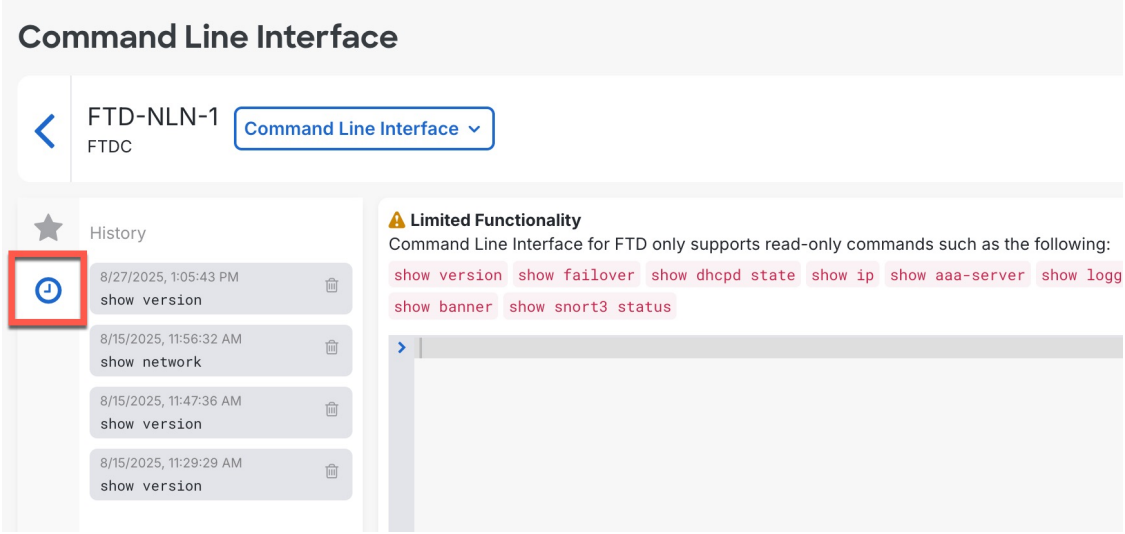
Example:

The following ASA example sends a batch of commands that creates three network objects and a network object group that contains those network objects.



Step 6 After you send commands, Security Cloud Control records that command in the **History** pane. You can rerun the commands saved in the **History** pane or use the commands as a macro.

a) Click the clock icon to open the **History** pane.



b) Select the command in the **History** pane that you want to modify or resend.

c) Reuse the command as it is or edit it in the command pane and click **Send**.

Use the bulk Command Line Interface

Send CLI commands to multiple devices of the same type at once.

Procedure

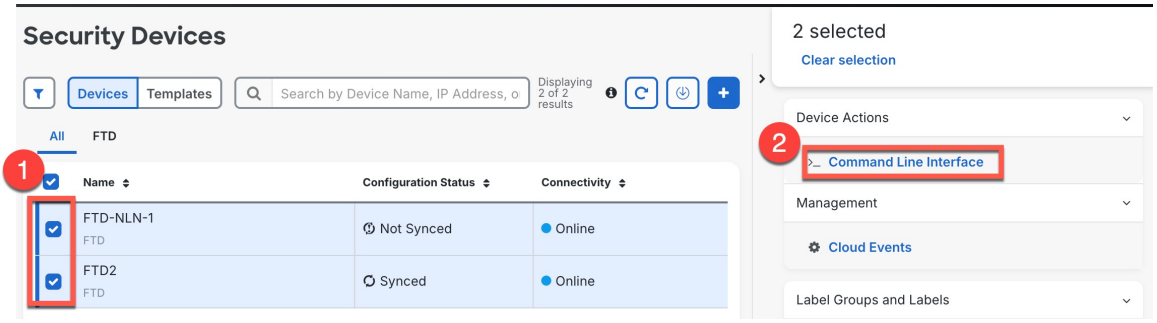
Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Devices** tab.

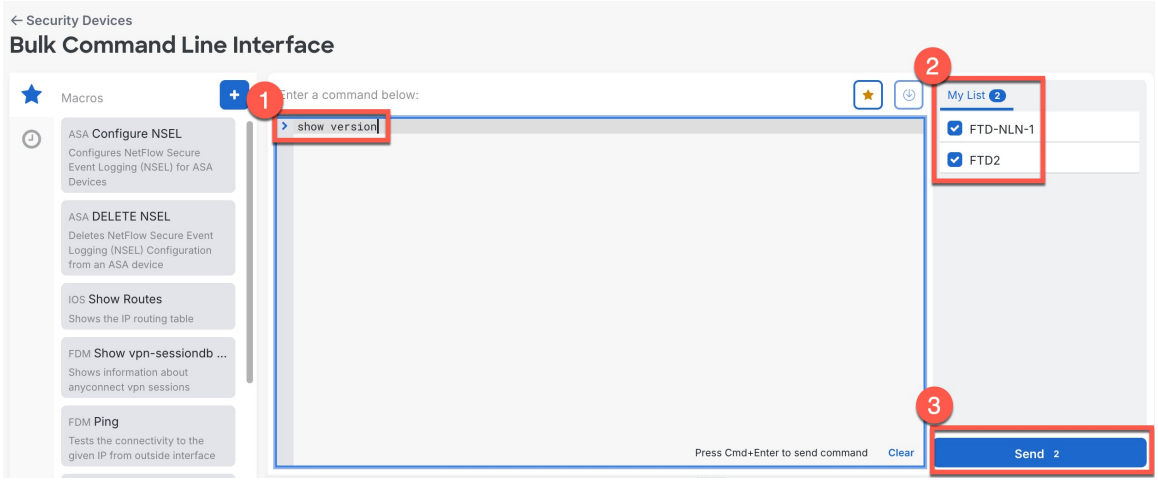
Step 4 Select multiple devices of the same type, and in the **Device Actions** pane on the right, click **>_Command Line Interface**.

Figure 1: Open the Command Line Interface



Step 5 Enter one or more commands in the command pane, check or uncheck devices you want to send the commands to in the **My List** field, and click **Send**.

Figure 2: Command Line Interface



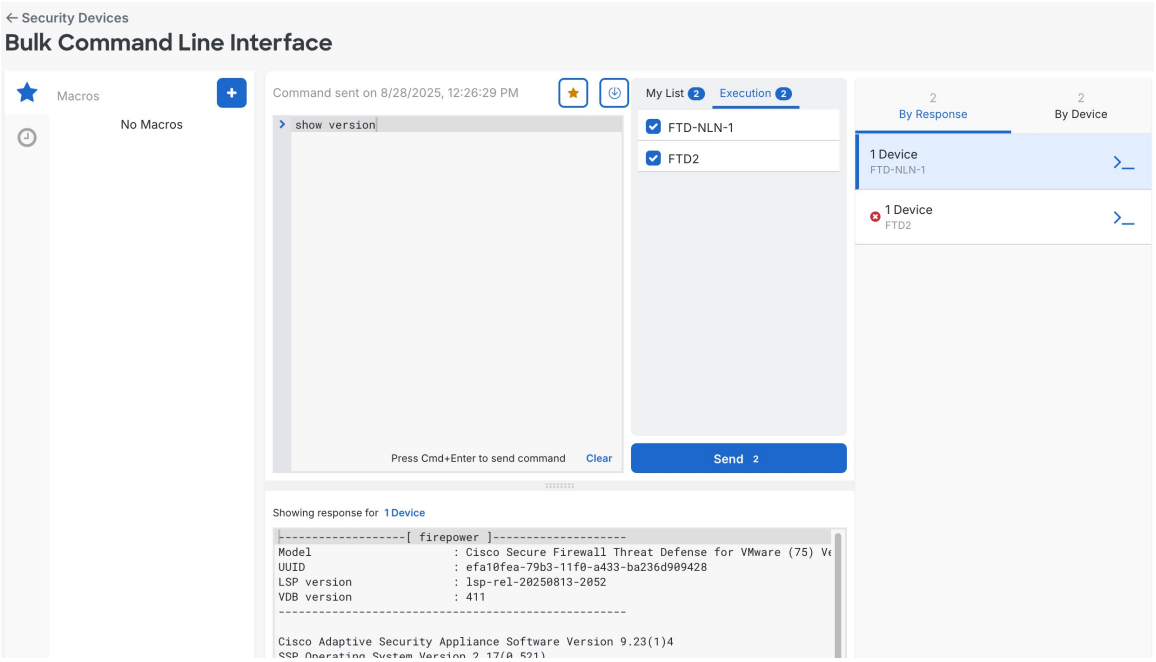
Note
If you enter a very long list of commands, you may exceed the limitations of Security Cloud Control's interface with the device. If you see an error, you can add extra blank lines between groups of commands so Security Cloud Control can send the commands in batches.

Note
For the ASA, if any of the selected devices are not synced, only the following commands are allowed: **show**, **ping**, **traceroute**, **vpn-sessiondb**, **changeto**, **dir**, **write**, and **copy**.

Step 6 View the device output.

The **Execution** tab shows the devices where the commands were sent; this list should match the selected devices in **My List**.

Figure 3: Command Line Interface



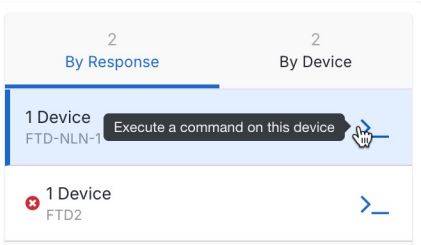
If there is no output for a command (either it was executed successfully, or there was no output to show), you will see `Done!` in the results pane.

The devices' response to the commands are displayed below in the response pane. If the response was the same for more than one device, the response pane displays the message "Showing Responses for X devices." Click **X Devices** to show all the devices that returned the same response in a pane to the right. Click **View Device** to go to that device in **Inventory**.

On the **By Response** tab, devices with identical responses are consolidated in a single row. Click a different row to show the response from other devices.

To re-run the command on the selected devices, click the prompt symbol to the right of the device row, and then click **Send**. You can change the commands you want to send or check and uncheck devices in the **My List** tab.

Figure 4: Execute a Command

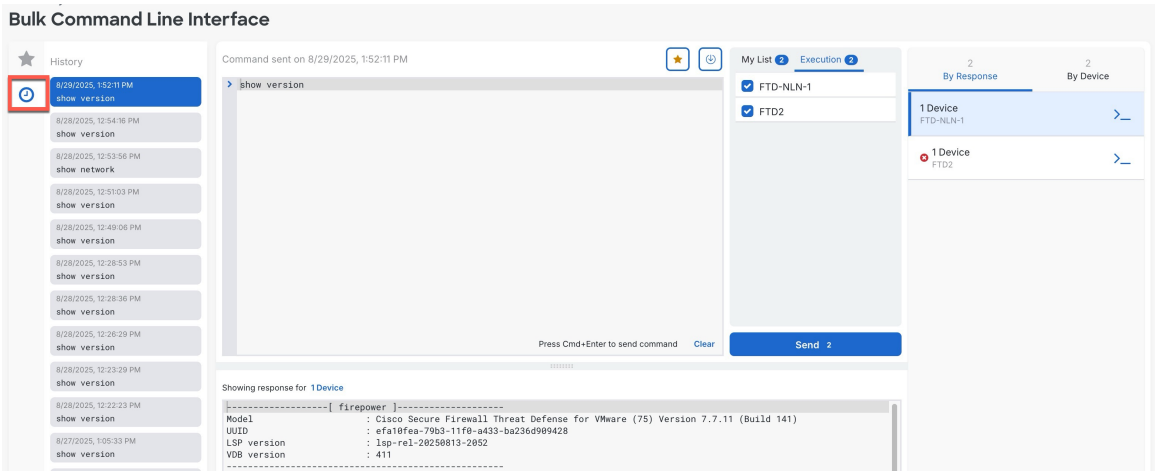


Click the **By Device** tab, and select a device to show only that device's command response.

Step 7 After you send commands, Security Cloud Control records that command in the **History** pane. You can rerun the commands saved in the history pane or use the commands as a macro. The commands in the history pane are associated with the original devices on which they were run.

a) Click the clock icon to open the **History** pane.

Figure 5: History Pane



b) Select the command in the **History** pane that you want to modify or resend.

Note that the command you pick is associated with specific devices (shown on the **Execution** tab) and not necessarily the ones you chose in the first step.

c) Click the **My List** tab to check or uncheck additional devices.

d) Reuse the command as it is or edit it in the command pane, and click **Send**.

Run a CLI macro

A CLI macro is a fully-formed CLI command ready to use on one or more devices of the matching type.

For some device types, Security Cloud Control provides system-defined macros. System-defined macros cannot be edited or deleted.

Procedure

Step 1 In the left pane, click **Inventory**.

Step 2 In the left pane, click **Security Devices**

Step 3 Click the **Devices** tab.

Step 4 Select one or more devices of the same type, and in the **Device Actions** pane on the right, click **>_Command Line Interface**.

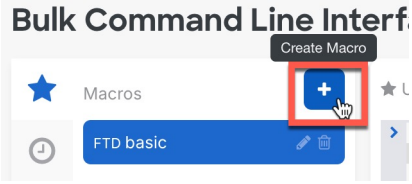
You cannot create macros without first choosing a device.

Step 5 Create a macro for this device type if one does not already exist.

a) Add a macro in one of the following ways:

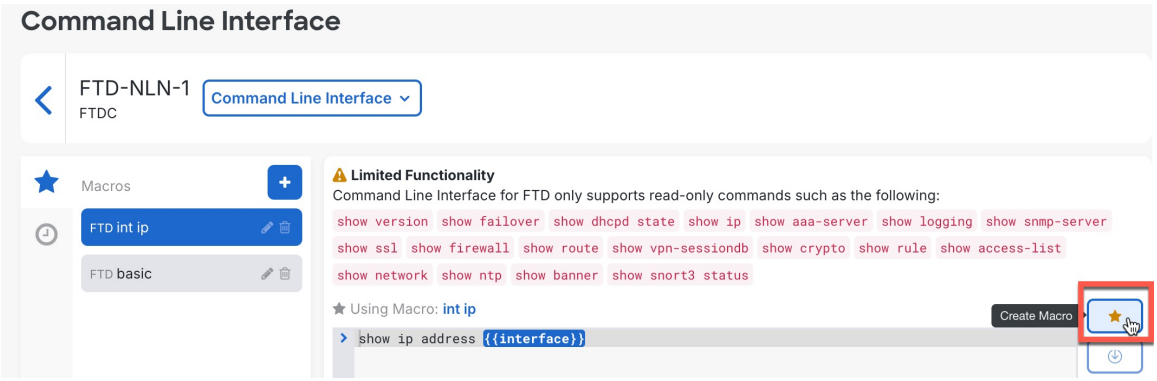
- New macro—On the **Macros** tab ( ), create a new macro by clicking the **Create Macro** ( ) button.

Figure 6: Create New Macro



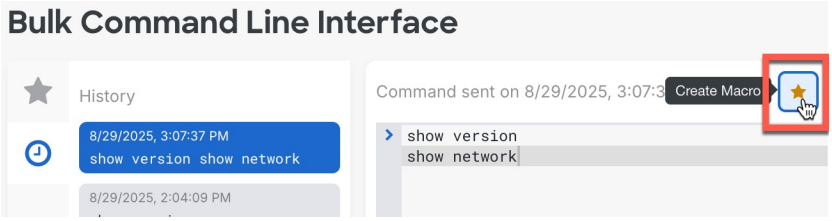
- From an existing macro—On the **Macros** tab ( ), create a macro starting with the same commands by selecting a macro and then clicking the **Create Macro** ( ) button.

Figure 7: Create Macro from Existing



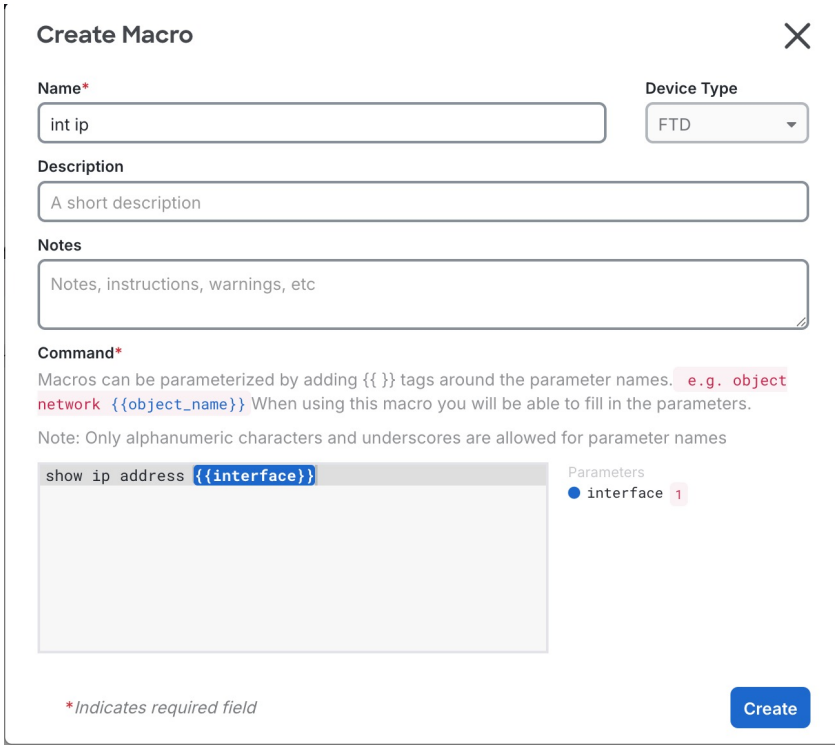
- From history—On the **History** tab ( ), select a command you already ran, and then click **Create Macro** ( ) button.

Figure 8: Create Macro from History



b) Give the macro a unique name and provide an optional description and notes.

Figure 9: Create Macro



c) Enter the commands in the **Command** field. For variables, enter the parameter surrounded by double curly brackets: **{{***parameter***}}**.

You will define the parameter before you run the macro.



You can name your parameters anything you want.

d) Click **Create**.

Step 6 Click the star ★ to open the **Macros** tab, and select a macro from the list.

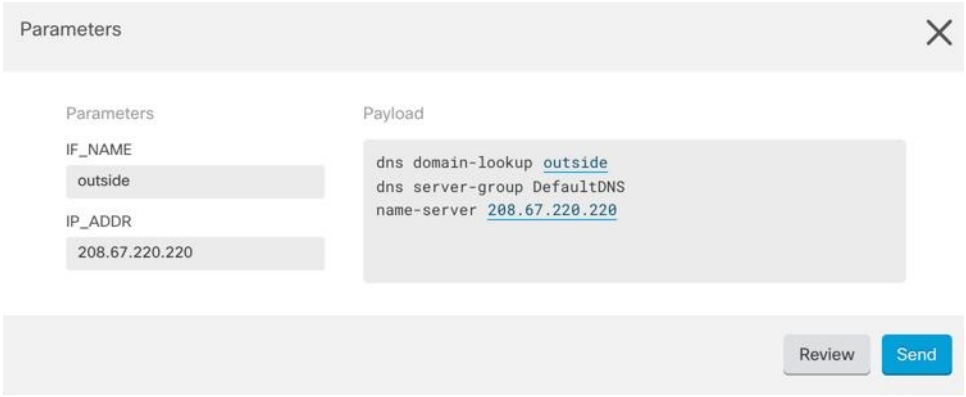
You can edit or delete a macro using the icons next to the macro name.

Step 7 Run the macro one of two ways:

- If the macro has no parameters to define, click **Send**. The response to the command appears in the response pane. You're done.
- If the macro contains parameters, such as the Configure DNS macro below, click **>_ View Parameters.**



a) In the **Parameters** pane, fill in the values for the parameters in the **Parameters** fields.



b) Click **Send**.

Step 8 Save configuration changes if you made any.

After you send the command you may see the message, "Some commands may have made changes to the running config" along with two links.



- Clicking **Write to Disk** saves the changes made by this command, and any other change that in the running config, to the device's startup config.
- Clicking **Dismiss**, dismisses the message and does not save the configuration. You may lose the configuration changes if you reboot the device.

Export Command Line Interface results

You can export the results of CLI commands to a comma separated value (.csv) file, so you can filter and sort the information in it. The exported information contains the following categories:

- Device
- Date
- User
- Command
- Output

Procedure

Step 1 Run your commands according to Use the Command Line Interface on a single device, on page 2, Use the bulk Command Line Interface, on page 4, or Run a CLI macro, on page 7, or choose a command from the **History** pane ( ).

Step 2 Click the **Export results** () button.

Step 3 Give the .csv file a descriptive name and save the file to your local file system.

When reading the command output in the .csv file, expand all the cells to see all the results of the command.