Revised: August 18, 2025

Cisco Secure Routers Swim and Onboarding Tool, Release 17.18.x

Cisco Secure Routers Swim and Onboarding tool

The Cisco Secure Routers Swim and Onboarding tool helps users to upgrade autonomous devices to a software version Cisco IOS XE 17.12.1a or higher and onboard them to Cisco Catalyst SD-WAN Manager. This is a standalone tool which runs on the user's host machine. It supports onboarding of autonomous devices to both cloud-hosted and on-premises Cisco Catalyst SD-WAN Manager.

The Cisco Secure Routers Swim and Onboarding tool runs on user's host machine and is designed to support these scenarios:

- Onboard a device

  Onboard an autonomous device running a software image Cisco IOS XE 17.12.1a or higher to Cisco Catalyst SD-WAN Manager for configuration and monitoring purposes.

- Upgrade a device

  Upgrade a device to a software version Cisco IOS XE 17.12.1a or higher and ensure it is compatible for onboarding to Cisco Catalyst SD-WAN Manager.

- Upgrade and onboard a device

  Upgrade a device to a software version Cisco IOS XE 17.12.1a or higher and then onboard it to the Cisco Catalyst SD-WAN Manager for configuration and monitoring purposes.

Prerequisites for Cisco Secure Routers Swim and Onboarding tool

Device prerequisites

The device prerequisites include details about protocol configuration and port requirements that must be verified before installing the Cisco Secure Routers Swim and Onboarding tool.

- The device must be operational.
- To establish an SSH connection with the device, SSH connectivity from the Cisco Catalyst SD-WAN Manager to the device with valid SSH username and password is needed. This user must have admin 15 privileges.

  ```
  username <username> privilege 15 password <encryption_level 0,6,7> <password>
  ```

- Ensure that these configurations are present in the device that is selected for upgrade or onboarding:

Prerequisites	Commands to configure
SCP	Ensure Secure Copy Protocol (SCP) server functionality is enabled. `ip scp server enable`
SSH	Ensure Secure Shell (SSH) Version 2 for secure remote access. `ip ssh version 2`

Prerequisites	Commands to configure
AAA authentication	Ensure that AAA(Authentication, Authorization, and Accounting) is configured on the device to authorize user EXEC sessions using the local database." `aaa authorization exec default local`
Virtual Terminal (VTY)	Configure Virtual Terminal (VTY) lines to allow remote access to the device through protocols like Telnet or SSH. On the terminal, go to the line configuration mode and configure the transport input to “ssh” to allow remote access. `Router(config-line)#transport input ssh`

- Ensure that these ports are reachable on the host machine.

Port Number	Default
3000	Web Interface
8080	Backend API
8081	UDP communication
8088	File Transfer Service

Note

If any of the default ports are busy, user is prompted during the Cisco Secure Router Swim and Onboarding tool installation to specify a new port number.

Cisco Catalyst SD-WAN Manager prerequisites

- The Cisco Catalyst SD-WAN Manager version must be Cisco SD-WAN version 20.15.1 or later.
- Ensure that the hardware device is reachable and has a stable connection. This will help maintain proper connectivity with the Cisco Catalyst SD-WAN Manager and ensure smooth onboarding.

Limitations for Cisco Secure Routers Swim and Onboarding tool

Supported platforms

The Cisco Secure Routers Swim and Onboarding tool currently supports upgrade and onboard only for hardware routing devices.

Supported platforms	Supported PIDs
Cisco 1000 Series Integrated Services Routers	Cisco 1000 ISR
Cisco Catalyst 8200 Series Edge Platforms	C8200-1N-4T, C8200L-1N-4T
Cisco Catalyst 8300 Series Edge Platforms	C8300-1N1S-4T2X|6T, C8300-2N2S-4T2X|6T

Supported platforms	Supported PIDs
Cisco Catalyst 8500 Series Edge Platforms	C8500-12X4QC, C8500-12X, C8500L-8S4X, C8500-20X6C
Cisco Industrial Routers and Gateways	ESR 6300, IR1101, IR1800, IR8140H, IR8340
Cisco 1100 Terminal Services Gateway	C1100TGX-1N24P32A, C1100TG-1N24P32A
Cisco ASR 1000 Series Aggregation Services Routers	ASR1001-HX, ASR1002-HX
Cisco 4000 Series Integrated Services Routers	Cisco 4431 ISR, Cisco 4451 ISR, Cisco 4461 ISR, Cisco 4321 ISR, Cisco 4331 ISR, Cisco 4351 ISR, Cisco 4221 ISR

Note

Cisco Catalyst 8000V devices are not supported by the tool.

Authentication method

The tool supports only Username/Password authentication to configure the Cisco Catalyst SD-WAN Manager. For 17.18.1a, the SSO authentication is currently not supported.

Initial setup and usage workflow

The workflow for the Cisco Secure Routers Swim and Onboarding tool involves downloading the tool and installing Docker Desktop or a Docker Engine as a prerequisite for container management. Once Docker Desktop or Docker Engine is set up on your host machine, you can install the tool. A Cisco IOS XE software image is added to the Image Repository, allowing you to get started with upgrading a device to a compatible Cisco IOS XE software version and onboarding it to Cisco Catalyst SD-WAN Manager. You can monitor the task updates using the Task Manager page and verify the completion of each task.

Summary

This workflow outlines the complete setup process of the tool, including Docker installation, software image management, and ensuring the tool is ready for operational use.

Workflow

1. Download the Cisco Secure Routers Swim and Onboarding tool
2. Install a Docker Desktop or Docker Engine
3. Download a Cisco IOS XE software image
4. Install the Cisco Secure Routers Swim and Onboarding tool
5. Add a Cisco IOS XE software image to the Image Repository
6. Get Started with the Cisco Secure Routers and Onboarding tool
7. Upgrade and onboard using the Cisco Secure Routers Swim and Onboarding tool

Step	To know more...
Download the Cisco Secure Routers Swim and Onboarding tool	Cisco Secure Routers Swim and Onboarding tool can be downloaded from Cisco Software Central. See, Download the Cisco Secure Router Swim and Onboarding tool.
Install a Docker Desktop or a Docker Engine	Before you start installing the tool, you must install a Docker application depending on the operating system on the host machine. See, Install a Docker Desktop or Docker Engine.
Download a Cisco IOS XE software image	Identify devices that requires an upgrade. This helps you to choose the relevant software images required for upgrading a device. See, Download a Cisco IOS XE software image.
Install the Cisco Secure Routers Swim and Onboarding tool	Once you have downloaded the tool, follow the onscreen instructions to install the tool on your host machine. See, Install the Cisco Secure Routers Swim and Onboarding tool.
Add a Cisco IOS XE software image to the Image Repository	Add images to the tool Image Repository which can be used for upgrading a device. See, Add a Cisco IOS XE software image to the Image Repository.
Get Started with the Cisco Secure Routers and Onboarding tool	Explore the Cisco Secure Routers Swim and Onboarding tool. See, Get Started with the Cisco Secure Routers and Onboarding tool.
Upgrade and onboard using the Cisco Secure Routers Swim and Onboarding tool	Add devices, upgrade, onboard devices to Cisco SD-WAN Manager using the tool. See, Upgrade and onboard using the Cisco Secure Routers Swim and Onboarding tool.

Download the Cisco Secure Router Swim and Onboarding tool

Cisco Secure Router Swim and Onboarding tool is hosted on Cisco Software Central. Download the file format according to your operating system.

The table lists the file type for each operating system.

Table 1: File Types for Operating Systems

File type	Operating system	Platform architecture
Cisco_Secure_Router_Swim_and_Onboarding_Tool.dmg	Use this file to install the tool on macOS.	ARM64
Cisco_Secure_Router_Swim_and_Onboarding_Tool.exe	Use this file to install the tool on Windows.	AMD64 and x86_64
Cisco_Secure_Router_Swim_and_Onboarding_Tool.zip	Use this file to install the tool on Linux.	AMD64 and x86_64

Install Docker Desktop or Docker Engine

The Cisco Secure Routers Swim and Onboarding tool is a Docker-based application supported on macOS, Windows and Linux. Refer to the official Docker documentation containing installation instructions for each operating system.

Select your operating system to view the appropriate Docker installation instructions:

- Windows: Install Docker Desktop for Windows operating system.
- macOS: Install Docker Desktop or Docker Engine for the macOS.
- Linux: Install Docker Desktop or Docker Engine for Linux operating system.

Note

When a Cisco IOS XE software image is uploaded, a Docker volume is automatically created. It is important to ensure that the host machine has sufficient storage capacity. Insufficient storage on the host machine will prevent the tool from uploading software images.

Download a Cisco IOS XE Image

To onboard a device to Cisco Catalyst SD-WAN Manager, the devices must be upgraded to a software version Cisco IOS XE 17.12.1a or higher. Identify the software version you need to upgrade the device to and download these software images to your host machine. The software images for all the platforms are hosted on Cisco Software Central.

Install the Cisco Secure Router Swim and Onboarding tool

This task provides details on how to install the Cisco Secure Router Swim and Onboarding tool on your host machine.

Before you begin

Ensure that the Docker Desktop or Docker Engine is installed and running on your host machine.

Step 1 Depending on the operating system of the host machine, run the executable file to start installing the tool.

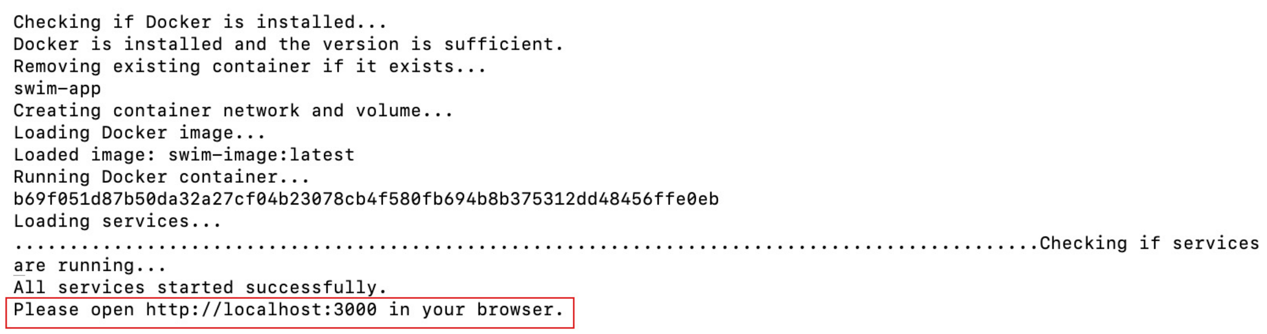
Table 2:

Operation system	File name	Action
macOS	Cisco_Secure_Router_Swim_and_Onboarding_Tool.dmg	Open the DMG file and follow the Installations instructions contained in the image to complete the installation.
Windows	Cisco_Secure_Router_Swim_and_Onboarding_Tool.exe	Double click the .exe file to start the installation.

Operation system	File name	Action
Linux	Cisco_Secure_Router_Swim_and_Onboarding_Tool.zip	Double click the .zip file to extract these files: • Install_and_run.sh • swim-app.tar **Note** For Linux files, add execute permission to allow users to run the file as a script or program. On the terminal, use this command to add the executable permissions: `chmod +x <file name>` For example, chmod +x Install_and_run.sh Run the Install_and_run.sh to start the installation.

Step 2 Monitor the progress of the installation through the terminal process window. The local host are provided at the end of the installation process.

Figure 1: Example of installation window for macOS



```
Checking if Docker is installed...
Docker is installed and the version is sufficient.
Removing existing container if it exists...
swim-app
Creating container network and volume...
Loading Docker image...
Loaded image: swim-image:latest
Running Docker container...
b69f051d87b50da32a27cf04b23078cb4f580fb694b8b375312dd48456ffe0eb
Loading services...
.............................................................................................Checking if services
are running...
All services started successfully.
Please open http://localhost:3000 in your browser.
```

Step 3 Copy the local host URL from the terminal window which is in the format http://localhost:<port number> and paste the link on a web browser.

Step 4

Note Docker Desktop or Docker Engine must be running in the background for the tool to work. If Docker Desktop or Docker Engine stops running due to a restart, shutdown, or any other reason, the tool will also stop functioning. To restart the tool, install the tool again using the Install_and_run.sh script.

Click **Get Started** to start exploring the Cisco Secure Routers Swim and Onboarding tool.

Get started with the Cisco Secure Routers and Onboarding tool

You can add hardware devices to the Cisco secure Routers Swim and Onboarding tool and enter the device details and configuration. The tool ensures all the required information is collected and validates them. You can upload Cisco IOS XE software images to the tool and use them to upgrade the devices and onboard them to Cisco Catalyst SD-WAN Manager.Additionally, the tool allows you to monitor the progress and view logs of ongoing operations using the Task Manager.

The Cisco Secure Routers Swim and Onboarding tool homepage has three main options on the left navigation pane:

The Cisco Secure Routers Swim and Onboarding tool homepage has three main options on the left navigation pane:

- Device Operation
- Image Repository
- Task Manager

Device Operations

You can add, onboard and upgrade a device from this page. All the devices that the user has added will be listed on the Device Operations page.

Option	**Description**
Add Device	Add devices to the tool either manually or importing a CSV file. Edit the device Username, Password, Enable Password, WAN Interface fields under **Actions**. IP address cannot be edited.
Onboard	Devices running a software version above Cisco IOS XE17.12.1a or a device with SD-Routing compatibility can be onboarded it to Cisco Catalyst SD-WAN Manager.
Upgrade	Devices that are running a software version earlier than Cisco IOS XE 17.12.1a, can be upgraded to a compatible software version.
Configure SDWAN Manager Details	Configure Cisco Catalyst SD-WAN Manager details for onboarding a device.
Import	Import a CSV file which contains a list of devices and configurations that the upgrade process needs to reference.
Export	Export a CSV file which contains the list of devices and configurations.
Filters	

Option	Description
Search	Search for a particular device from the list of devices.
Status	Search for a device based on the status of the device. For example, select **Success** to list all the devices that are added to the tool.
Reset all	Resets the applied filters.

Image Repository

Identify the current version of the device. If the current version of the device is less than Cisco IOS XE 17.12.1a, to upgrade the device to a minimum of Cisco IOS XE 17.12.1a to onboard it to Cisco Catalyst SD-WAN Manager.

Compatible Cisco IOS XE software images for upgrading an autonomous router can be added in the Image Repository page. These images can be directly uploaded to the tool from the host machine.

Table 3: Image Repository

Options	Description
Add New Software	Add software images from the host machine to the tool.
Delete a Software	Delete software images from the tool.

Task Manager

The Task Manager page lists all the tasks created for a device. Detailed logs for specific tasks and the check automated workflow to monitor the status of the device from this page.

Table 4: Task Manager

Option	Description
IP address	Displays the IP address of a device.
Status	Monitor if the task status is **In progress**, **Success** or **Failed**.
Action	Click **View Details** for detailed logs for a specific task.

Add a Cisco IOS XE software image to the Image Repository

This section outlines on how to add software images to the Cisco Secure Router Swim and Onboard tool.

Before you begin

Ensure you have the relevant software image on the host machine.

Step 1 On the **Image Repository** page, click **Add New Software** to add an image. Only .bin files are supported by the tool.

Step 2 Select images from the host machine or drag a file to the image repository and click **Upload.** You can upload only one image at a time.

Step 3 The **Software Version** and the **Device Platform** information are auto populated.

Upgrade and onboard using the Cisco Secure Routers Swim and Onboarding tool

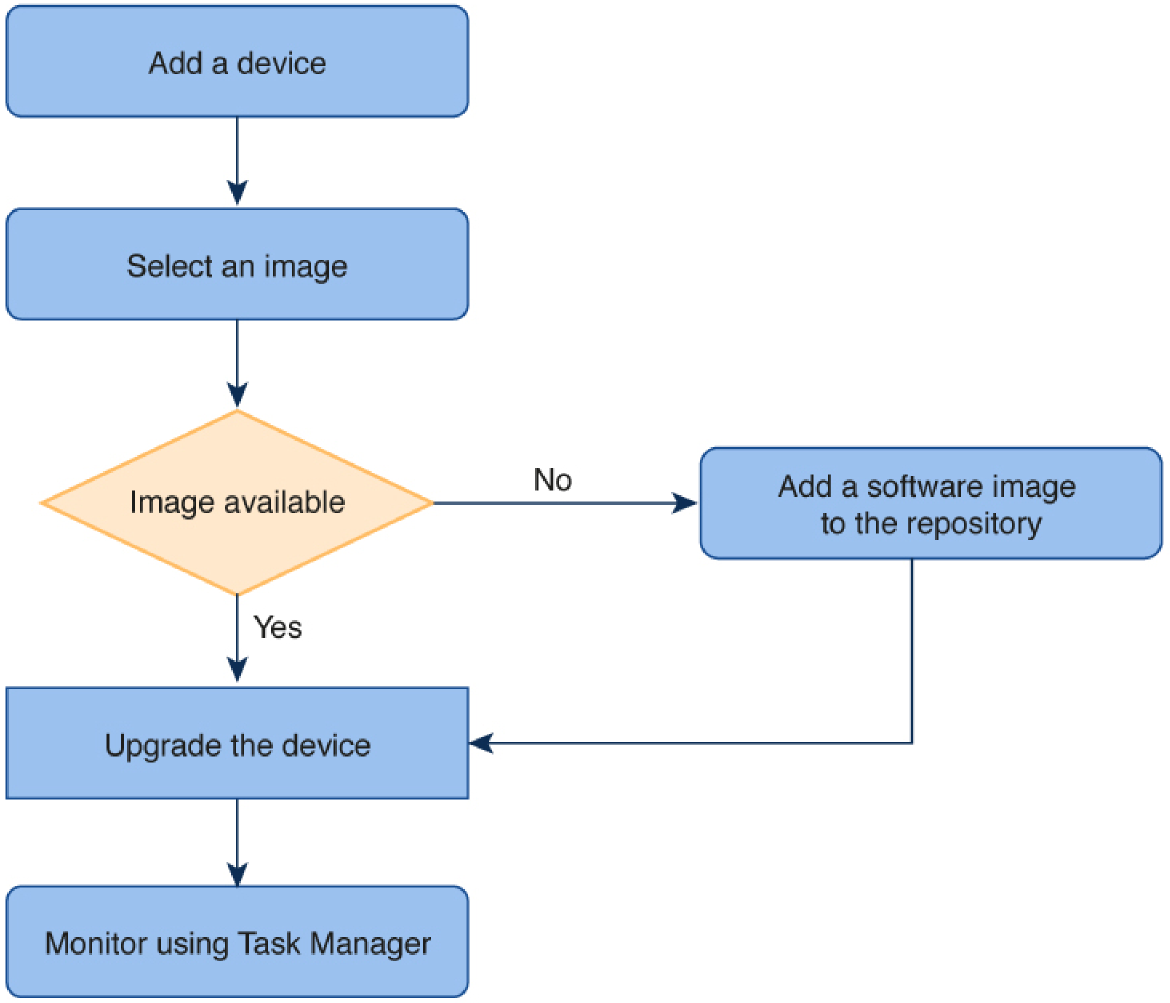
The Cisco Secure Routers Swim and Onboarding tool is designed to supports three different scenarios:

- Upgrade a device: Upgrade devices to versions higher than Cisco IOS XE 17.12.1a.
- Onboard a device: Onboard devices that is already SD-routing compatible and running a Cisco IOS XE 17.12.1a or higher to Cisco Catalyst SD-WAN Manager.
- Upgrade and onboard a device: Upgrade a device and then onboard it to Cisco Catalyst SD-WAN Manager.

Upgrade a device

Autonomous device that are running a software version earlier than Cisco IOS XE 17.12.1a, must be first upgraded to a compatible software version before you can onboard it into the Cisco Catalyst SD-WAN Manager.

Figure 2: The process of upgrading a device



Follow these steps to upgrade the device to a comaptible Cisco IOS XE software version:

Step 1 On the home page, navigate to **Device Operations** page and click **Add Device**.

Step 2 Add a device using one of these options:
Choose from:

- Add a device manually

a. Click **Add Device**. Enter these mandatory device details.

Option	Description
IP Address	Specify the IP address of the device to be added.
Username and Password	Specify the username and password.

Option	Description
Enable Password	Specify password if configured on the device (optional, if not using admin 15 privileges).
WAN Interface	Specify the WAN Interface details. (mandatory for onboard).

b. Click **Save**.

- Import multiple devices using a CSV file

a. Create a CSV file by referring to the format which includes these fields.

IP Address	Username	Password	Enable Password	WAN Interface

b. Enter the **`IP Address`**, **`Username`**, **`Password`**, **`Enable Password`** and **`WAN Interface`**.

c. On Cisco Secure Routers Swim and Onboarding tool homepage, Click **Import**. Select the CSV file from the host machine.

d. Click **Upload**.

Step 3 Monitor the device status in the **Status** column.

Option	Description
In Progress	The device addition to the Cisco Secure Routers Swim and Onboard tool is in progress.
Green	The device was added successfully. The tool has established a connection with the device.
Red	The device could not be added. The tool did not establish a connection with the device. To view error details, hover your cursor over the status to see the tooltip.

Once the device is added successfully, the device information such as **`Chassis Number`**, **`Device Model`**, **`Current Version`** and **`OnboardCompatibility`** is auto populated.

Note The tool and the host machine must run on the same network as the host. If the device is not reachable from the host machine, the tool will not be able to reach the device.

Step 4 Select a device. Ensure that the **Status** of the device is **`Green`** and Click **Upgrade**.

Step 5 Choose a software image from the **Software Upgrade** drop-down list. Click **Upgrade** to initiate the upgrade process.

Step 6 An upgrade task is created on the **Task Manager** page. Upgrade checks are performed by the tool.

Step 7 Click **View Details** on the **Task Manager** page and monitor the automated workflow. After a successful upgrade, the **Status** of the task is marked as **Success**.

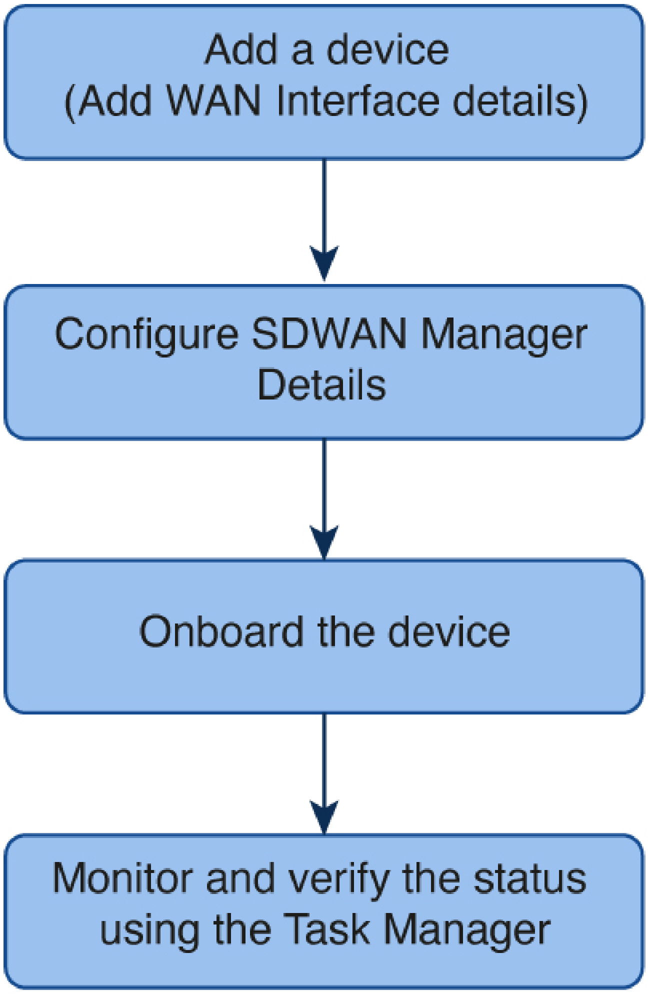
Step 8 On the **Device Operations** page, verify **Onboard compatibility** is **Green** and the **Current Version** of the device is upgraded to the newer software image version.

Note If the device is upgraded to a version lower than Cisco IOS XE 17.12, then the Onboard compatibility remains red.

Onboard a device

Autonomous devices that are in SD-Routing mode and are running a compatible Cisco IOS XE version of 17.12.1a, can be onboarded to Cisco Catalyst SD-WAN Manager using the Cisco Secure Routers Swim and Onboarding tool.

Figure 3: Process for onboarding a device


Add a device
(Add WAN Interface details)
Configure SDWAN Manager Details
Onboard the device
Monitor and verify the status using the Task Manager

Follow these steps to onboard a device to a comaptible Cisco IOS XE software version:

Before you begin

Identify devices that needs to be onboarded.

Ensure all the device prerequisites are met.

Step 1 On the home page, navigate to **Device Operations** page and click **Add Device**.

Step 2 Add a device using one of these options:
Choose from:

- Add a device manually

  a. Click **Add Device**. Enter these mandatory device details.

Option	**Description**
IP Address	Specify the IP address of the device to be added.
Username and Password	Specify the username and password.
Enable Password	Specify password if configured on the device (optional, if not using admin 15 privileges).
WAN Interface	Specify the WAN Interface details. (mandatory for onboard).

  b. Click **Save**.

- Import multiple devices using a CSV file

  a. Create a CSV file by referring to the format which includes these fields.

IP Address	Username	Password	Enable Password	WAN Interface

  b. Enter the **`IP Address`**, **`Username`**, **`Password`**, **`Enable Password`** and **`WAN Interface`**.

  c. On Cisco Secure Routers Swim and Onboarding tool homepage, Click **Import**. Select the CSV file from the host machine.

  d. Click **Upload**.

Step 3 Configure SDWAN Manager Details:

- **SD-WAN Manager IP** address
- **Username** and **Password**
- **Port** number (optional)

Step 4 Monitor the device status in the **Status** column.

Option	**Description**
In Progress	The device addition to the Cisco Secure Routers Swim and Onboard tool is in progress.
Green	The device was added successfully. The tool has established a connection with the device.
Red	The device could not be added. The tool did not establish a connection with the device. To view error details, hover your cursor over the status to see the tooltip.

Once the device is added successfully, the device information such as `Chassis Number`, `Device Model`, `Current Version` and `OnboardCompatibility` is auto populated.

Note The tool and the host machine must run on the same network as the host. If the device is not reachable from the host machine, the tool will not be able to reach the device.

Step 5 Select a device or multiple devices. Ensure that the **Onboard Compatibility** is green. Click **Onboard** to initiate the onboarding process.

Note If **Onboard Compatibility** is red or **WAN interface**/ **Configure SDWAN Manager Details** are missing, the **Onboard** option is disabled.

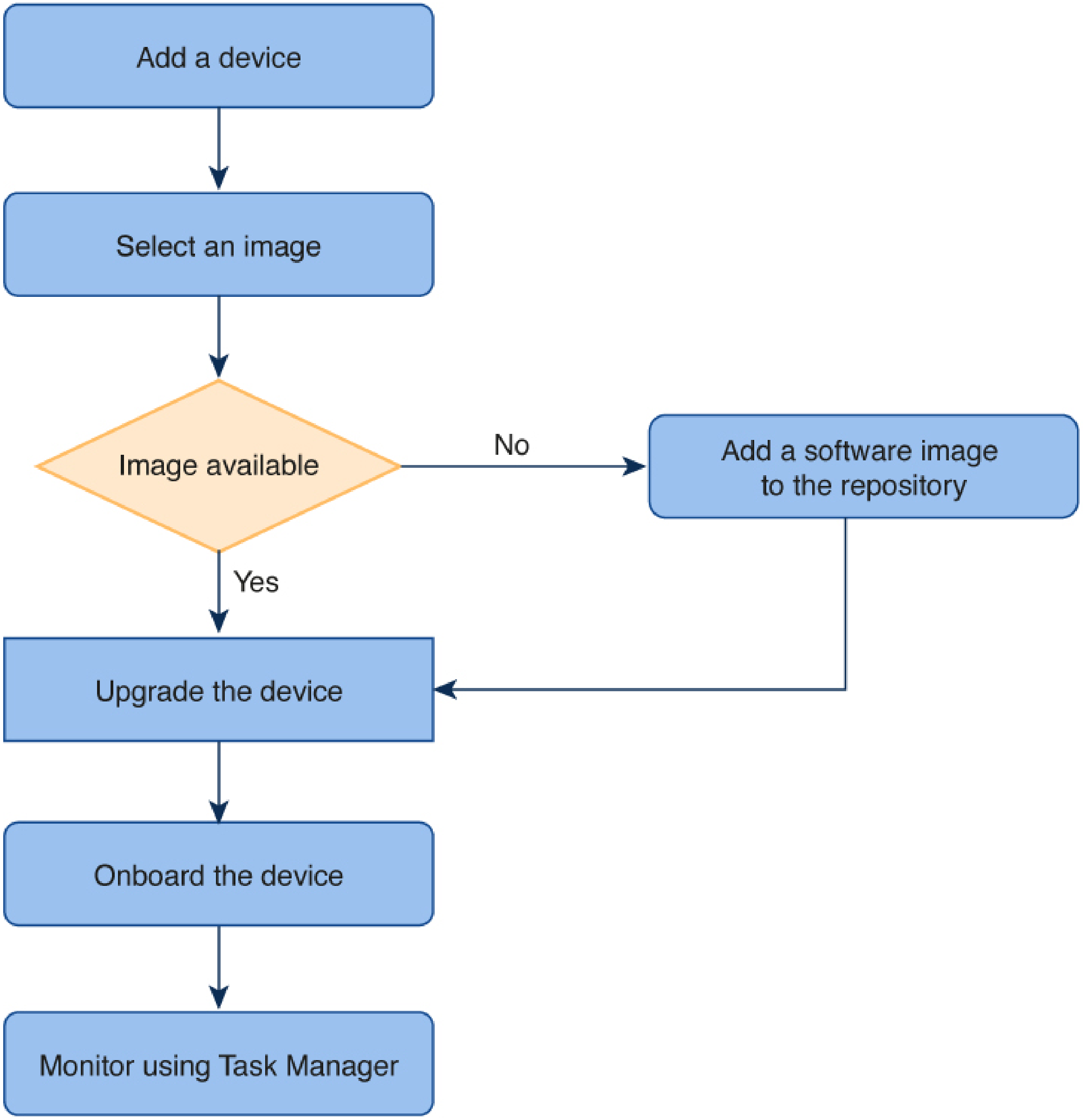
Step 6 An onboard task is created on the **Task Manager** page. The tool performs onboard checks. Click **View Details** and monitor the automated workflow.

Step 7 After successful onboarding of a device, the **Status** of the task is marked as Success. On Cisco Catalyst SD-WAN Manager go to **Configuration** > **Devices** to verify if the device is added successfully.

Upgrade and onboard a device

The Cisco Secure Routers Swim and Upgrade tool helps to upgrade existing autonomous routing devices running an earlier software version to a compatible Cisco IOS XE release. You can then onboard the device to the Cisco SD-WAN Manager.

Figure 4: Process for onboarding a device



Follow these steps to first upgrade a device and then onboard it to Cisco Catalyst SD-WAN Manager:

Step 1 On the home page, navigate to **Device Operations** page and click **Add Device**.

Step 2 Add a device using one of these options:
Choose from:

- Add a device manually

  a. Click **Add Device**. Enter these mandatory device details.

Option	Description
IP Address	Specify the IP address of the device to be added.
Username and Password	Specify the username and password.
Enable Password	Specify password if configured on the device (optional, if not using admin 15 privileges).
WAN Interface	Specify the WAN Interface details. (mandatory for onboard).

b. Click **Save**.

- Import multiple devices using a CSV file

a. Create a CSV file by referring to the format which includes these fields.

IP Address	Username	Password	Enable Password	WAN Interface

b. Enter the **`IP Address`**, **`Username`**, **`Password`**, **`Enable Password`** and **`WAN Interface`**.

c. On Cisco Secure Routers Swim and Onboarding tool homepage, Click **Import**. Select the CSV file from the host machine.

d. Click **Upload**.

Step 3 Configure SDWAN Manager Details:

- **SD-WAN Manager IP** address
- **Username** and **Password**
- **Port** number (optional)

Step 4 Monitor the device status in the **Status** column.

Option	Description
In Progress	The device addition to the Cisco Secure Routers Swim and Onboard tool is in progress.
Green	The device was added successfully. The tool has established a connection with the device.
Red	The device could not be added. The tool did not establish a connection with the device. To view error details, hover your cursor over the status to see the tooltip.

Once the device is added successfully, the device information such as **`Chassis Number`**, **`Device Model`**, **`Current Version`** and **`OnboardCompatibility`** is auto populated.

Note The tool and the host machine must run on the same network as the host. If the device is not reachable from the host machine, the tool will not be able to reach the device.

Step 5 Select a device. Ensure that the **Status** of the device is **`Green`** and Click **Upgrade**.

Step 6 Choose a software image from the **Software Upgrade** drop-down list. Click **Upgrade** to initiate the upgrade process.

Step 7 The upgrade checks are performed by the tool. You can monitor the automated workflow on the **Task Manager** page. After a successful upgrade, the **Status** of the task is marked as Success.

Step 8 On the **Device Operations** page, select the device. Verify **Onboard compatibility** is **Green** and the **Current Version** of the device is upgraded to the newer software image version.

Note If the device is upgraded to a version lower than Cisco IOS XE 17.12, then the Onboard compatibility remains red.

Step 9 Select a device or multiple devices. Ensure that the **Onboard Compatibility** is green. Click **Onboard** to initiate the onboarding process.

Note If **Onboard Compatibility** is red or **WAN interface**/ **Configure SDWAN Manager Details** are missing, the **Onboard** option is disabled.

The onboarding checks are performed by the tool. You can monitor the automated workflow on the **Task Manager** page.

After successful onboarding of a device, the **Status** of the task is marked as Success. On Cisco Catalyst SD-WAN Manager go to **Configuration** > **Devices** to verify if the device is added successfully.

Appendix

This section provides reference information on common issues encountered during the installation and use of the tool.

Validations when using the Cisco Secure Routers Swim and Onboarding tool

This section lists possible validation failures when using the Cisco Secure Routers Swim and Onboarding tool.

Table 5:

Action	Reasons for failure
Add a device	• The IP address is invalid. • The fields -Username, Password, Enable Password or WAN interface is same as an existing device. • The IP address, Username or Password is invalid/null. • Add, upgrade or onboard is in progress. • If the password is not provided in the CSV during import, the tool will attempt to SSH into the device but will display an error indicating that the credentials are invalid.

Action	Reasons for failure
Edit device details	• The IP address is invalid. • The fields -Username, Password, Enable Password or WAN interface is same as existing device. • Add, upgrade or onboard is in progress. • Editing a device (existing with correct credentials) with wrong values (username, password) will render the device to lose all stored data and will make device unapplicable for upgrade/onboard.
Delete device details	• The IP address is invalid/null. • Add, upgrade or onboard is in progress.
SD-WAN Manager details	The SD-WAN Manager IP address cannot be edited.
Add a Cisco IOS XE image to Image Repository	The Filename is invalid.
Delete a Cisco IOS XE image from Image Repository	Any device upgrade is in progress.

Troubleshoot issues in the tool

The common problems and resolution when you use this tool to upgrade and onboard routing devices are listed in the table. If your solution is not listed here, we recommend that you raise a support ticket at Cisco Support.

Table 6:

Error	Cause	How to resolve

Reachability is red.
From laptop/host machine user can establish SSH but tool is not able to establish a connection.
	Tool is not able to connect to the device.	Establish a Telnet connection to a router.
		`hostmachine ~ % docker exec -it swim-app /bin/bash`
		`root@f68c89686235:/app#`
		`ping router_ip`
		`telnet router_ip 22`

BootStrap File upload to device failed [Device]:Load boostrap CLI can only be used for first time onboarding. To re-enable the feature, manually configure mandatory CLIs and install the root-cert	Onboarding failed: A device that is trying to onboard is already in SD-Routing mode, but it is not converted to autonomous mode.	To re-enable the feature, manually configure mandatory CLIs and install the root-cert.
		To convert to autonomous, follow these steps:
		`delete flash:ciscosdwan.cfg`
		`conf t`
		`no sd-routing`
		`end`
		`request platform software sd-routing erase`

Error	Cause	How to resolve
SCP transfer failed: The target device may not allow SCP connections. Please ensure SCP is enabled on the target machine." [failure] Failed to copy image to device [failure] Finished Pre-Upgrade Check: Aborting requested workflow due to failures	Upgrade task fails for copying image to the device.	On the device terminal, enable the Secure Copy Protocol (SCP) server. `ip scp server enable`

ssh connection to device fails while adding device to the tool	ssh configuration is missing on device but reachability is there from tool to device.	Ensure this configuration is present on device:
		`ip ssh version 2`
		`transport input ssh`

Device status column tooltip shows this error: **User privilege is less than 15. Please use credentials of a privilege 15 user or give enable password in the input and try again.**	Authorization local configuration is missing on the device.	Ensure this configuration is present on device: `aaa authorization exec default local`
Device status column tooltip shows this error **An error occurred: [Errno 110] Connection timed out**	Device IP is not reachable.	Ensure device IP address is reachable to the SWIM tool.
Cannot connect to the Docker daemon at unix:///Users/tugulati/.docker/run/docker.sock. Is the docker daemon running?	Unable to work with the tool and the Docker is not running.	Restart the tool, execute the startup script(install_and_run) again.