

Juniper NETWORKS Security Director Installation Guide

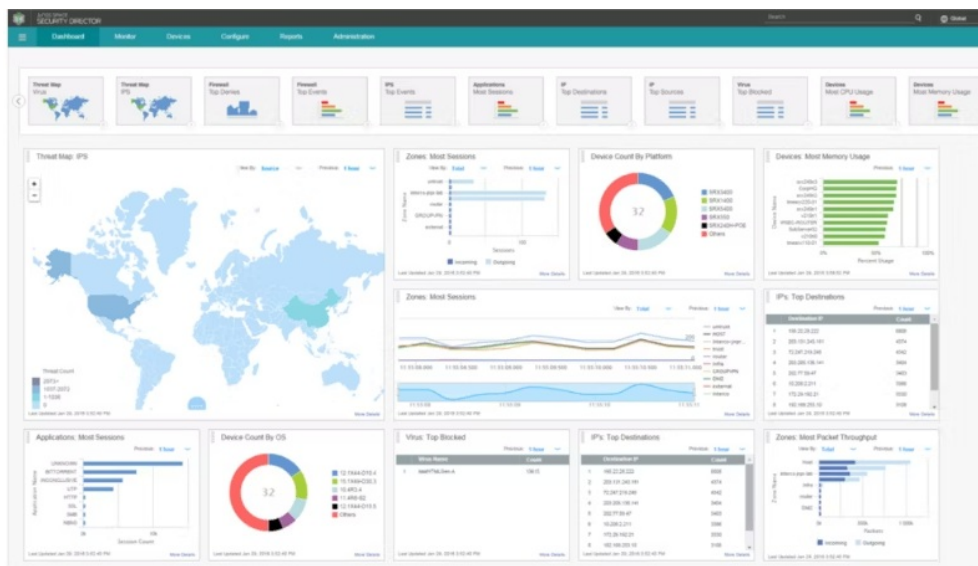
[Home](#) » [JUNIPER NETWORKS](#) » Juniper NETWORKS Security Director Installation Guide 

Contents

- [1 Juniper NETWORKS Security Director](#)
- [2 Specifications](#)
- [3 Product Information](#)
- [4 Product Usage Instructions](#)
- [5 Introduction](#)
- [6 System Requirements](#)
- [7 Deploy](#)
- [8 Upgrade](#)
- [9 FAQs](#)
- [10 Documents / Resources](#)
 - [10.1 References](#)
- [11 Related Posts](#)



Juniper NETWORKS Security Director



Specifications

- **Product Name:** Juniper Security Director
- **Manufacturer:** Juniper Networks, Inc.
- **Release Date:** January 24, 2025
- **Website:** www.juniper.net

Product Information

Juniper Security Director is the next-generation on-premise management product designed for SRX Series Firewall and vSRX devices. Juniper Security Director simplifies the installation and management process for network security devices.

System Requirements

Hardware Requirements

- VM Configuration: 16 vCPU, 80 GB RAM, 2.1 TB storage
- Device Management Capability
- Log Analytics and Storage Capability

Software Requirements

The software requirements for Juniper Security Director will vary based on the specific version and updates. Ensure to refer to the latest software documentation for accurate information.

Product Usage Instructions

Installation Overview

To install Juniper Security Director, follow these steps:

1. Download the open virtual application (OVA) and software bundle from the Juniper Software Downloads page.
2. Deploy the OVA file to create a virtual machine (VM) using VMware vSphere.
3. Power on the VM to automatically install the software bundle.

4. Note: Juniper Security Director is designed for single-node deployment.

Log in to Web UI

To access the Juniper Security Director Web UI, follow these steps:

1. Open a web browser and enter the IP address of the deployed Juniper Security Director.
2. Enter your credentials to log in and access the management interface.

Upgrade Instructions

To upgrade the Juniper Security Director, follow these steps:

1. Refer to the upgrade guide provided by Juniper Networks for detailed instructions.
2. Ensure to back up your configurations before proceeding with the upgrade process.
3. Follow the step-by-step instructions to successfully upgrade your Security Director installation.

About This Guide

Use this guide to install and upgrade Juniper Security Director®.

Introduction

Juniper Security Director Installation Overview

IN THIS SECTION

- Benefits of Juniper Security Director | 2
- What's Next | 3

Juniper Security Director is the next-generation on-premise management product for SRX Series Firewall and vSRX devices.

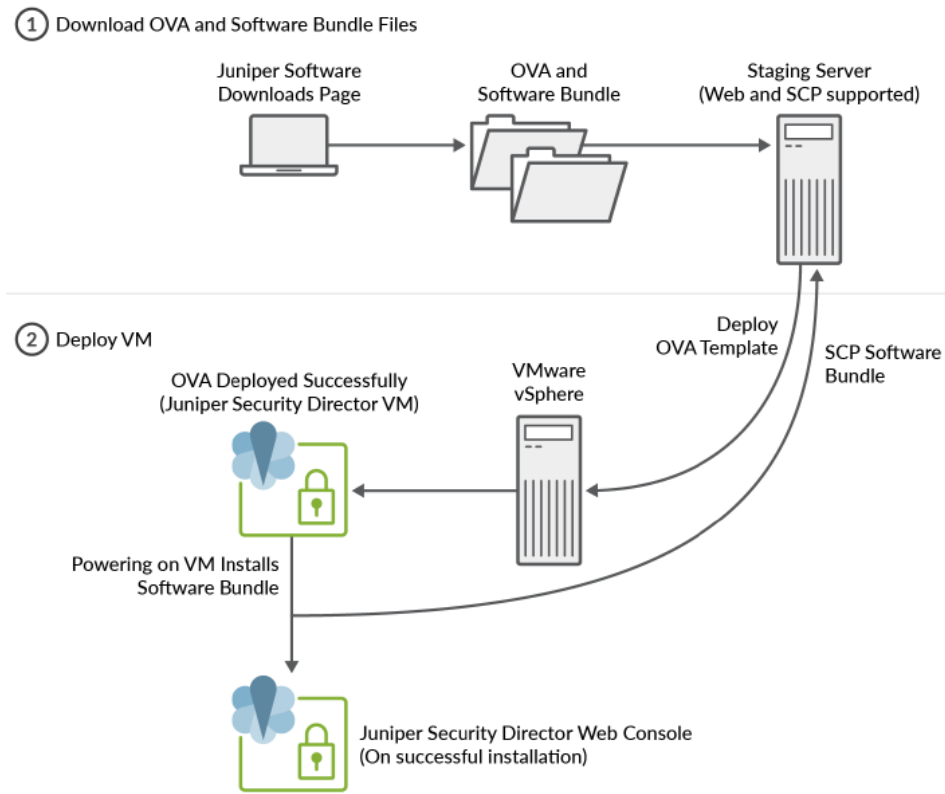
Benefits of Juniper Security Director

- Provides centralized security management
- Provides operational simplicity and efficiency with ease of use
- Offers integrated device management and security management with unified policies
- Offers visibility and analytics
- Manages all SRX Series Firewall and vSRX devices
- Suitable for regulated/air-gapped environments as it can be deployed on-premise.
- "Figure 1" on page 2 shows the installation process for Juniper Security Director. 2

Figure 1:

Juniper Security Director Installation Process

You can install Juniper Security Director by downloading the open virtual application (OVA) and the software bundle from the Juniper Software Downloads page. Use the OVA file to deploy the virtual machine (VM) using VMware vSphere. After the OVA deployment is complete, power on the VM to automatically install the software bundle.



NOTE:

Juniper Security Director is a single-node deployment.

What's Next

“Juniper Security Director System Requirements”

System Requirements

Juniper Security Director System Requirements

SUMMARY

Ensure that your system meets the hardware and software requirements

Hardware Requirements

Table 1: Hardware Requirements for ESXi Server

VM Configuration	Device Management Capability	Log Analytics and Storage Capability
16 vCPU, 80 GB RAM, 2.1 TB storage	<ul style="list-style-type: none"> Up to 1000 devices Up to 10000 policy rules per device Up to 6000 NAT rules per device Up to 1000 VPNs per device/ system 	<ul style="list-style-type: none"> Up to 17000 logs per second Out of the 2.1 TB storage, 1.5 TB is dedicated to log analytics.
40 vCPU, 208 GB RAM, 4.2 TB storage	<ul style="list-style-type: none"> Up to 3000 devices Up to 20000 policy rules per device Up to 10000 NAT rules per device Up to 1500 VPNs per device/ system 	<ul style="list-style-type: none"> Up to 40000 logs per second Out of the 4.2 TB storage, 3.5 TB is dedicated to log analytics.

NOTE:

We do not recommend hyperthreading on the VMware hypervisor (ESXi) Server. You must use dedicated resources for CPU, RAM, and disk as per the hardware requirement. We do not recommend oversubscription or sharing resources.

Software Requirements

- Juniper Security Director runs on a VMware hypervisor (ESXi) Server. Use vCenter and vSphere version 7.0 and later. You must deploy the OVA through the vCenter Server only. We do not support OVA deployment on ESXi directly.
- You must have the following dedicated IP addresses in the same subnet:
 - Management IP address—IP address for the VM that provides access to the Juniper Security Director CLI.
 - UI virtual IP address—Virtual IP address to access the Juniper Security Director GUI.
 - Device connection virtual IP address—Virtual IP address to establish a connection between the managed devices and Juniper Security Director.
 - Log collector virtual IP address—Virtual IP address to receive logs from devices.
- Ensure that you have access to SMTP, NTP, and DNS servers from the VM network (Juniper Security Director).

NOTE:

We support NTP servers with IPv4 addresses only.

What's Next

“Deploy Juniper Security Director Using VMware vSphere

Deploy

Deploy Juniper Security Director Using VMware vSphere

SUMMARY

This topic guides you through the Juniper Security Director VM deployment using VMware vSphere.

Before You Begin

- If you are not familiar with using VMware vSphere, see VMware Documentation and select the appropriate VMware vSphere version.
- Choose the size of the VM, see “Hardware Requirements” on page 5.
- You must have 4 dedicated IP addresses and ensure that you have access to SMTP, NTP, and DNS servers, see “Software Requirements” on page 5.

NOTE:

If the deployment is a regulated/air-gapped environment, ensure that the VM also has access to signatures.juniper.net for IDP/Applications Signatures download. To deploy Juniper Security Director VM using VMware vSphere:

Step 1: Download the OVA and the Software Bundle

1. Download the Juniper Security Director OVA (.ova file) from <https://support.juniper.net/support/downloads/?p=security-director-on-prem> to a Web server or your local machine.
2. Download the Juniper Security Director Software Bundle (.tgz file) to your local machine from <https://support.juniper.net/support/downloads/?p=security-director-on-prem> and then transfer the file to your staging server.

A staging server is an intermediate server where the software bundle is downloaded and is accessible from the VM.

The staging server must support software bundle download from the Juniper Security Director VM through Secure Copy Protocol (SCP). Before you deploy the VM, you must have the details of the staging server, including the SCP username and password.

Step 2: Deploy the VM

1. Open the vSphere Client.
2. Right-click the inventory object that is a valid parent object of a VM and select Deploy OVF Template.
3. On the Select an OVF template page:
 - Enter the webserver OVA URL, where you have downloaded the OVA. The system might warn you about source verification. Click Yes.

- NOTE: Ensure that firewall rules do not block image access from the vSphere cluster. OR
 - Select the Local file option and click UPLOAD FILES to choose the OVA file from your local machine.
- On the Select a name and folder page, enter the VM name and the location.
 - On the Select a compute resource page, select the compute resource for the host on which the VM will be deployed.
 - On the Review details page, review the details of the resources to be provisioned.
 - On the Select Storage page, select the storage for the configuration and the virtual disk format. We recommend you use virtual disk format as a Thick provision.
 - NOTE: We do not recommend thin provisioning. If you choose thin provisioning and the actual disk space available is low, the system might encounter problems once the disk is full.
 - On the Select Networks page, select the network to configure IP allocation for static addressing.
 - On the Customize template page, configure Juniper Security Director on-premise OVA parameters.
- **NOTE:**
Prepare all details for the Custom template page in advance. The OVF template will timeout after 6 to 7 minutes.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- Select storage
- Select networks
- Customize template**
- Ready to complete

Customize template

Customize the deployment properties of this software solution.

Juniper Security Director On-Premises OVA
Settings
15 settings

Hostname	
cladmin user password	Min Length 8, Max length 32, required at least 3 types: digit, uppercase alphabet, lower case alphabet, special character (~!@# \$%^&*()_+=[]{} ;':",<.>./\`/) Password Confirm Password
Management IP address	Enter the IP address in CIDR format. For example, 10.2.4.5/24. Do not use /32 netmask to indicate the address. Netmask must be at least /29.
Default gateway	Gateway IP address of the network.
DNS servers	Enter the server addresses, each separated by a space.
Search domains	Enter multiple search domains, each separated by a space.
UI virtual IP address	The virtual IP address must be in the same subnet of the management IP address.
UI FQDN	Fully Qualified Domain Name that resolves to UI virtual IP address.
Device connection virtual IP address	The virtual IP address must be in the same subnet of the management IP address.
Device Connection FQDN	Fully Qualified Domain Name that resolves to Device Connection virtual IP address.
Log collector virtual IP address	The virtual IP address must be in the same subnet of the management IP address.
Log Collector FQDN	Fully Qualified Domain Name that resolves to LOG Collector virtual IP address.
Software bundle SCP path	Format with port - user@server:port/relative-path or user@server:port/absolute-path. For example, root@10.0.0.122/var/www/html/sdcp-24.1-898.tgz Format without port - user@server:relative-path or user@server/absolute-path. For example, root@10.0.0.1/root/sdcp-24.1-898.tgz
SCP password	Password Enter a password to enable authentication. Confirm Password
NTP server	

CANCEL
BACK
NEXT

- **NOTE:**

- The sysadmin user password field does not strictly validate password requirements. However, during the installation process, the system enforces strict validations and rejects the password that does not meet the specified requirements, causing installation failure. To avoid issues during installation, ensure that the password meets these criteria:
- Must be at least 8 characters long and not more than 32 characters.
- Must not be dictionary words.
- Must include at least three of the following:
 - Numbers (0-9)
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Special characters (~!@#\$%^&*()_-=+{}[];:'"<,.>./\)

10. We recommend you to FQDN. On the Ready to Complete page, review all the details and if required, go back and edit the VM parameters. These network parameters cannot be changed from the VM configuration after successful installation. However, network parameters can be changed from the CLI. Click Finish to begin the OVA deployment.

You can monitor the OVA deployment progress status in the Recent Tasks window at the bottom of your screen till it is 100% complete. The Status column shows the deployment complete percentage.

Congratulations! Now the OVA deployment is complete.

11. (Optional) Once you've deployed the OVA, create a snapshot. Snapshot is useful if you need to roll back after the software bundle automatically installs. Select the VM and from the Actions menu navigate to Snapshots > TAKE SNAPSHOT.

12. Click the triangle icon to power on the VM.

- **NOTE:**
- By default, the VM will be deployed with the smallest resource configuration as mentioned in Hardware Requirements on page 5. Adjust the resources to match other resource configurations using the VMware Edit VM settings.
- For a successful installation, the resource allocation must match the Hardware Requirements.
- Once the VM powers on, navigate to the Summary tab and click LAUNCH WEB CONSOLE to monitor the software bundle installation status.
- **NOTE:**
- Avoid performing any operation on the console until the installation is complete.
- You can view the installation progress on the console. After the installation is complete, the console displays a Successfully installed software bundle on the cluster.
- A successful installation requires approximately 30 minutes. If the installation lasts longer, check the Web console for potential errors. You can ssh to the VM IP using the sysadmin user and the password you configured during the OVA deployment. Then, use the show bundle install status command to check the installation status.
- To rectify errors, power off the VM, then navigate to Configure click vApp options to modify the parameters, and then power on the VM.
- Congratulations! The software bundle installation is now complete.

Step 3: Verify and Troubleshoot

To verify if the installation is successful, you must log into the VM IP through an SSH connection. VM IP is the value provided in the IP address field in "Step 9" on page 10. Use the following default credentials:

- **User:** sysadmin
- **Password:** abc123
- After you have logged in, you will be prompted to change the default credentials.
- Log in with your new credentials and run the following commands:
 - Show the service health monitor status command to view the installation status.
 - List `/var/log/cluster-manager` command to list the log file.
 - Show file `/var/log/cluster-manager/cluster-manager-service.log` command to view the content of the log file.
- **Troubleshoot Using UI**

You can generate and download the system logs for issues related to feature groups such as device management, policy management, and log analytics. A feature group is a logical grouping of related microservices whose logs are required to debug an issue.

Before You Begin

See “Log In to the Juniper Security Director Web UI”

To generate the system logs:

1. Select Administration > System Management > System Logs.
2. The System Logs page is displayed.
3. Select the feature group.
4. In the Timespan drop-down field, select the period for which you want to generate the logs.
5. Click Generate Log Package.
6. A job is created for the log generation process. The details are displayed at the top of the page. Select Administration > Jobs to view the job. On the Jobs page, you can monitor the status of the log generation process. After the job is finished, a link is created on the System Logs page to download the logs. System logs will be downloaded as a TGZ file and shared with the Juniper Networks support team to analyze the root cause of the issue.

What's Next

“Log In to the Juniper Security Director Web UI”

Log In to the Juniper Security Director Web UI

SUMMARY

Create your Juniper Security Director organization account in two steps—enter your details and your organization's details and then verify your e-mail address to activate your account.

After you deploy the OVA, you can log in to the Web GUI using the UI virtual IP address or FQDN (domain name) that you configured during the OVA deployment.

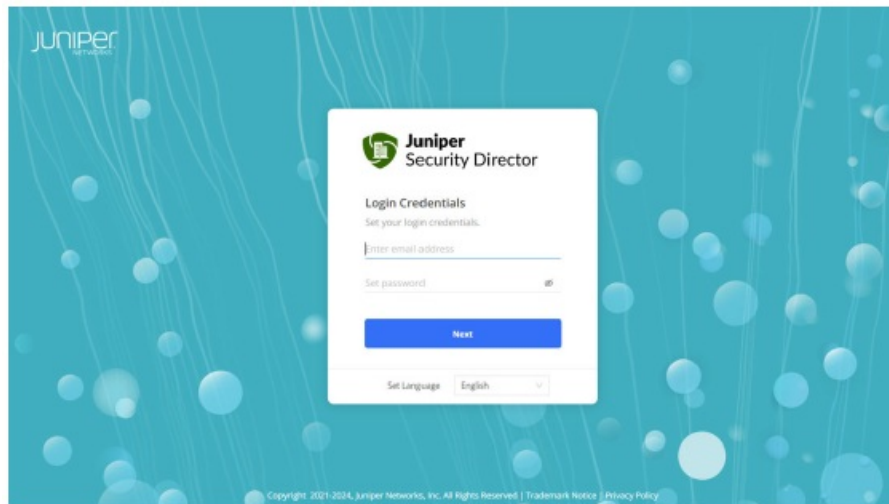
Before You Begin

The following ports must be opened:

- Inbound port 443 for users' connection to the Web
- Outbound port 25 for outbound to configured mail server
- Inbound port 7804 from all managed devices
- Outbound port 443 for signature download URL
- Inbound port 6514 for inbound connection for traffic log

To log in to the Web UI:

1. Enter the UI virtual IP address or FQDN (domain name) in a Web browser to access the Juniper Security Director login page. To view the configured UI virtual IP address, select the deployed VM, navigate to Configure, and click vApp Options. Under Properties, you can view the UI address. The Juniper Security Director login page is displayed.



2. Set your login credentials and click Next:
 - Enter a valid e-mail address.
 - Enter a password containing 8 to 20 characters.
 - The password must contain at least one number, one uppercase letter, and one special character.
3. Enter your contact details and click Next:
 - Enter your name. You can use a maximum of 32 letters. Spaces are allowed.
 - Enter your company name. You can use a maximum of 64 characters. Alphanumeric characters, hyphens (-), underscores (_), and spaces are allowed. Select your country from the drop-down list.
 - Enter a valid phone number. You can use 7 to 18 characters comprising numbers and special characters, such as the plus sign (+), dashes (-), or brackets ().
4. Enter your SMTP details and click Next:
 - Enter the hostname or IP address of the SMTP server.
 - Enter the SMTP server port number.
 - Enter the sender's name in the e-mail.
 - Enter the sender's e-mail address.
 - You can enable SMTP server authentication for sending e-mails and secure your e-mails with Transport Layer Security (TLS) encryption.
 - **NOTE:**
 - Ensure that your SMTP configuration is valid, otherwise you will not receive emails to activate your organization account.
 - You can enable SMTP server authentication for sending e-mails and secure your e-mails with Transport Layer Security (TLS) encryption.
 - **NOTE:**
Ensure that your SMTP configuration is valid, otherwise you will not receive emails to activate your organization account.
5. Test your SMTP server or sthetthe est.
 - If you click Test SMTP Server, an SMTP test e-mail will be sent to your mailbox.

6. Enter a name for the organization account that you will use to manage the security devices and services and click Create Organization Account.
 - You will receive an e-mail to verify your e-mail address and activate your account.
7. Log in to your e-mail account, open the verification e-mail, and click Activate Organization Account.
 - The organization account is now successfully activated and you can now log in with your credentials.
 - **NOTE:**
 - Ensure you verify your e-mail address and click Activate Organization Account within 24 hours of receiving the e-mail. If you don't verify your e-mail, your account details will be removed from Juniper Security Director, and you'll need to re-create your organization.
8. Enter the password, and click Sign in.

Congratulations! You are now signed in to the Juniper Security Director UI. The menu bar on the left of each page allows easy access to various tasks.

Upgrade

Upgrade Juniper Security Director

You can upgrade your existing Juniper Security Director version to the latest available version.

NOTE:

Services will be temporarily unavailable during the upgrade process. The upgrade may take 40 minutes to complete, after which services will be restored. We recommend scheduling the upgrade during a maintenance window with ample time.

Before You Begin

Download the Juniper Security Director Software Bundle (.tgz file) to your local machine from <https://support.juniper.net/support/downloads/?p=security-director-on-prem> and then transfer the file to your staging server.

A staging server is an intermediate server where the software upgrade bundle is downloaded.

The staging server must support the software upgrade bundle download from Juniper Security.

Director VM through SCP. Before you upgrade the VM, you must have the details of the staging server, including the SCP username and password.

To upgrade Juniper Security Director:

1. Log in to the Juniper Security Director UI.
2. Select Administration > System Management > System.

The System page is displayed. You can view the existing software version that is displayed on the page.

3. Click Upgrade System.
4. Complete the configuration by entering the details as described in

Table 2: Fields on the Upgrade System Page

Field	Description
Upgrade bundle location	<p>Enter the staging server location, where the upgrade bundle is available. You must provide the bundle location in the following formats:</p> <ul style="list-style-type: none"> With port — <i>user@server:port/relative-path</i> or <i>user@server:port//absolute-path</i>. For example, root@10.0.0.1:22//var/www/html.sdop-24.1-898.tgz Without port — <i>user@server:relative-path</i> or <i>user@server:/absolute-path</i>. For example, <i>root@10.0.0.1:/root/sdop-24.1-898.tgz</i>
Port	Enter the SCP port number of the staging server.
Username	Enter the username to connect to the staging server.
Password	Enter the password to connect to the staging server.

Click OK.

The upgrade process is triggered, and the Job Status page is displayed. After the upgrade is complete, close the Job Status page. The detailed status of the job is displayed on the Job Status page. The status of the upgrade is displayed on the System page. On successful upgrade, the upgraded version is displayed on the System page. If the upgrade fails, check if:

- VM has connectivity to the staging server. An incorrect bundle location is provided.
- Missing bundle in the specified location.
- Invalid bundle or invalid bundle format is provided.

RELATED DOCUMENTATION

CLI Commands

FAQS


• Q: Is Juniper Security Director compatible with all SRX Series Firewall models?

A: Juniper Security Director is designed to work seamlessly with SRX Series Firewall and vSRX devices. Ensure to check the specific compatibility matrix for detailed information.

• Q: Can Juniper Security Director be integrated with third-party security tools?

A: Yes, Juniper Security Director supports integration with select third-party security tools. Refer to the official documentation for the list of supported integrations and configuration instructions.

Documents / Resources

	<p>Juniper NETWORKS Security Director [pdf] Installation Guide Security Director, Security, Director</p>
---	---

References

- [📄 Downloads](#)
- [📄 Downloads](#)
- [📄 CLI Overview | Juniper Networks](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.