

Quick Start

Junos Space Security Director Quick Start

IN THIS GUIDE

- [Step 1: Begin | 1](#)
- [Step 2: Up and Running | 9](#)
- [Step 3: Keep Going | 16](#)

Step 1: Begin

IN THIS SECTION

- [Meet Security Director | 2](#)
- [Install and Deploy Workflow | 2](#)
- [Install Security Director | 3](#)
- [Install Security Director Insights as the Log Collector | 4](#)
- [Do More with Policy Enforcer | 8](#)

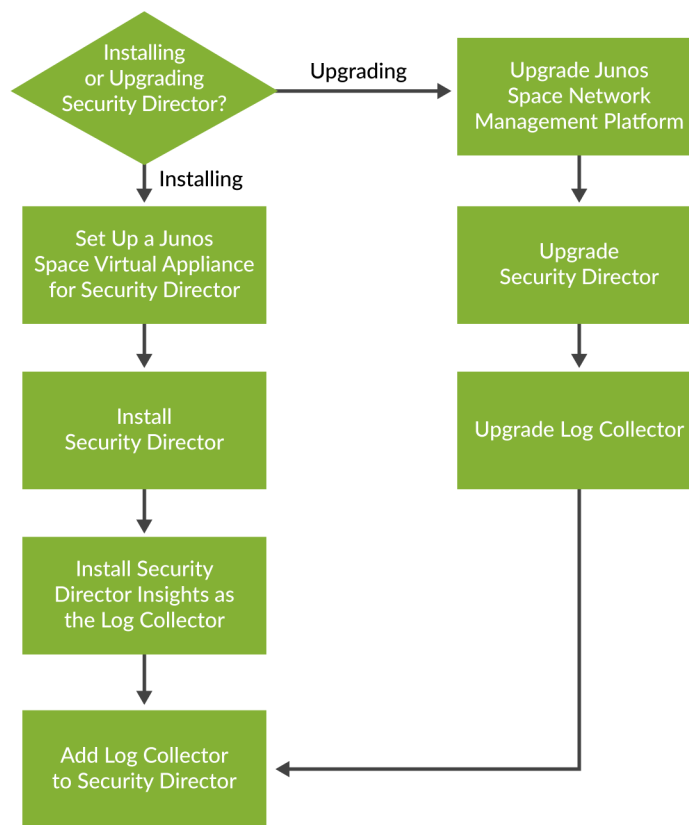
In this guide, we provide a simple, three-step path, to quickly get you up and running with Juniper Networks® Junos® Space Security Director (Security Director). You'll learn how to install and deploy Security Director, and do some initial configuration to start managing the security devices on your network.

Meet Security Director

Security Director provides security policy management through a smart, centralized, Web-based interface. Using intuitive dashboards and reporting features, you gain insight into threats, compromised devices, risky applications, and more.

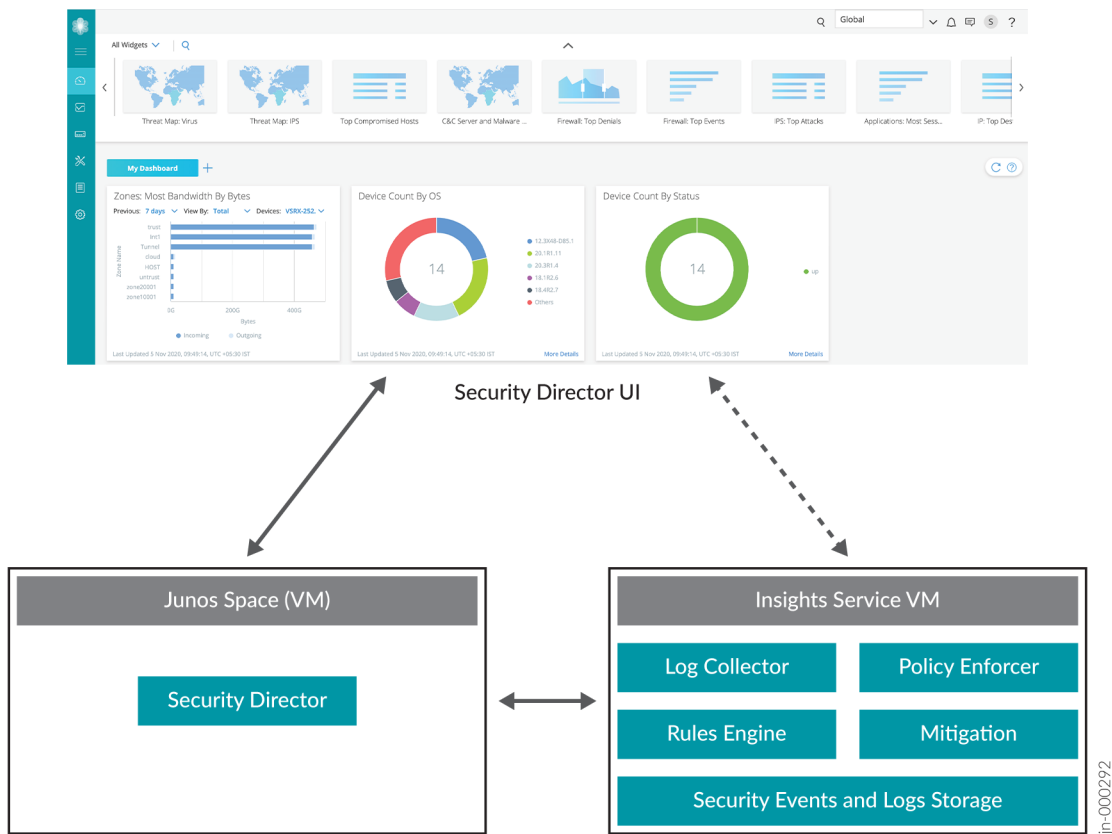
Install and Deploy Workflow

Here's an overview of the process to install Security Director and deploy log collector.



jn-000291

You'll need to use Security Director Insights as the log collector. Security Director Insights is a single virtual appliance (Service VM) that runs on the VMware vSphere infrastructure. The Security Director Insights GUI is integrated with the Security Director GUI, and the log collector and Policy Enforcer are integrated within the Security Director Insights VM. Here's an illustration of how Security Director Insights integrates with the Security Director ecosystem.



Before You Begin

Install and configure Junos Space Virtual Appliance. You'll need to set up the virtual appliance to run as a Junos Space node. See the [Junos Space Virtual Appliance Installation and Configuration Guide](#).



NOTE: Starting in Junos Space Network Management Platform Release 22.1R1, you cannot install the Platform on the JA2500 Junos Space appliance.

Install Security Director

Installing Security Director is easy. First, verify the supported Junos Space Network Management Platform version by logging in to Network Management Platform > Administration > Application. Then, download the Security Director release image from the [download site](#), upload it to the Junos Space Platform server, and install it. You can find all the details in [Adding a Junos Space Application](#).



NOTE: You can install Junos Space Security Director only on the supported Junos Space Network Management Platform version.

Install Security Director Insights as the Log Collector

IN THIS SECTION

- [Deploy and Configure the Security Director Insights OVA File | 4](#)

You'll need to use Security Director Insights as the log collector. You install Security Director Insights from an OVA file. Once installed, you can use the Security Director Insights VM as a log collector to view log data across multiple SRX Series Firewall. A single Security Director Insights VM provides up to 25K events per second (eps), making it easier for you to scale up with less virtual resources.

Here are the required specifications for deploying Security Director Insights VM for various eps rates:

EPS Rate	CPU	Memory
5k	4	16
10k	8	16
15k	8	24
25k	16	32



NOTE: In this guide, you learn how to deploy and configure Security Director Insights VM as the log collector. Based on your requirement, you can choose to deploy JSA as a log collector. For details, see the [Security Director Installation and Upgrade Guide](#).

Deploy and Configure the Security Director Insights OVA File

Security Director Insights recommends VMware ESXi Server version 6.5 or later to support a VM with the following initial configuration:

- 12 CPUs
- 24 GB RAM
- 1.2 TB disk space

If you are not familiar with using VMware ESXi servers, see [VMware Documentation](#) and select the appropriate VMware vSphere version.

Here's how to deploy and configure Security Director Insights using the OVA file:

1. Download the Security Director Insights VM OVA image from the Juniper Networks software [download page](#).



CAUTION: Do not change the name of the Security Director Insights VM image file that you download from the Juniper Networks support site. If you change the name of the image file, the Security Director Insights VM creation may fail.

2. Launch the vSphere Client that is connected to the ESXi server where you want to deploy the Security Director Insights VM.
3. Select **File > Deploy OVF Template** to open the Deploy OVF Template page.

4. Select the **URL** option if you want to download the OVA image from the Internet or select **Local file** to browse the local drive and upload the OVA image.
5. Click **Next**.

The Select a name and folder page opens.

6. Enter the OVA file name and installation location for the VM, and click **Next**.

The Select a compute resource page opens.

7. Select the destination compute resource for the VM, and click **Next**.

The Review details page opens.

8. Verify the OVA details and click **Next**.

The License agreements page opens.

9. Accept the EULA and click **Next**.

The Select storage page opens.

10. Select the destination file storage for the VM configuration files and the disk format. (Thin Provision is for smaller disks and Thick Provision is for larger disks.)

Click **Next**. The Select networks page opens.

11. Select the network interfaces that the VM will use.

You can configure IP allocation for Static or DHCP addressing. We recommend using the Static IP Allocation Policy. Since the DHCP option is primarily used only for proof of concept, short-term deployments, we don't cover how to use that option here.

Click **Next**. The Customize template page opens.

12. For Static IP Allocation, configure the following parameters for the virtual machine:

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Juniper Security Analytics		8 settings
Virtual Appliance Network Settings		
IP Allocation Policy	Static ▼	
IP address	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="10.0.0.1"/>	
Netmask	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="255.255.0.0"/>	
Gateway	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="10.0.0.1"/>	
DNS address 1	Ignore this property if the IP allocation policy is DHCP. <input type="text" value="10.0.0.1"/>	
DNS address 2	Ignore this property if the IP allocation policy is DHCP. <input type="text" value=""/>	

[CANCEL](#)
[BACK](#)
[NEXT](#)

- IP Allocation Policy—Select Static
- IP address—Enter the Security Director Insights VM IP address
- Netmask—Enter the netmask
- Gateway—Enter the gateway address
- DNS Address 1—Enter the primary DNS address
- DNS Address 2—Enter the secondary DNS address

Click **Next**. The Ready to complete page opens:

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- ✓ 8 Customize template
- 9 Ready to complete**

Click Finish to start creation.

Provisioning type	Deploy OVF From Remote URL
Name	juniper-security-director-insights-20.3R1.s449c42
Template name	juniper-security-director-insights-20.3R1.s449c42
Download size	4.3 GB
Size on disk	9.8 GB
Folder	Abhishek Gaden
Resource	it-cluster1a.englab.juniper.net
Storage mapping	1
All disks	Datastore: ranch99-vm; Format: Thin provision
Network mapping	2
administrative	Engineering
HA Monitoring	Engineering
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

CANCEL

BACK

FINISH

13. Review the details and click **Finish** to begin the OVA installation.
14. After the OVA is installed successfully, power on the VM and wait for the boot up to complete.
15. Once the VM powers on, in the CLI terminal, log in as administrator with the default username as “admin” and password as “abc123”.

After you log in, you’ll be prompted to change the default admin password. Enter a new password to change the default password.

Congratulations! The Security Director Insights deployment is now complete.
16. You will be prompted with Yes/No. Enter **No** to configure the OVA as LC + SDI on-prem.

Do More with Policy Enforcer

You can install Policy Enforcer to configure Juniper Connected Security. Policy Enforcer integrates with Juniper Networks® Advanced Threat Prevention Cloud (Juniper ATP Cloud) to provide centralized threat management and monitoring to your Juniper Connected Security network. You can use Policy Enforcer to combine threat intelligence from different solutions and act on that intelligence from one management point.

Starting in Security Director Release 24.1R1, standalone Policy Enforcer is not supported. You must use Security Director Insights as the Policy Enforcer.

For details on Security Director Insights as the integrated Policy Enforcer, see [Configure Security Director Insights as Integrated Policy Enforcer](#).

Step 2: Up and Running

IN THIS SECTION

- [Add Security Director Insights as a Log Collector | 9](#)
- [Add a JSA Log Collector Node to Security Director | 12](#)
- [Create a Device Discovery Profile | 12](#)
- [Discover Devices | 13](#)
- [Modify the Configuration of Security Devices | 13](#)
- [Create Addresses | 13](#)
- [Create a Firewall Policy | 14](#)
- [Assign Policies to Domains | 14](#)
- [Assign Devices to a Policy | 14](#)
- [Publish and Update Policies on Devices | 15](#)
- [Configure Juniper ATP Cloud or ATP Appliance with Policy Enforcer | 15](#)

Now that you've installed Security Director and Security Director Insights as the log collector, let's do some initial configuration so you can start managing the security devices on your network. In this section, you'll learn how to add a log collector to Security Director so you can view the log data. Next, we'll show you how to create device discovery profiles and how to discover the security devices on your network. After the security devices are discovered, you can configure basic network settings for them, assign addresses, and set firewall policies. You'll then learn how to configure Juniper ATP Cloud or ATP Appliance with Policy Enforcer.

Add Security Director Insights as a Log Collector

IN THIS SECTION

- [Enable Log Collector | 10](#)
- [Add Security Director Insights VM as the Log Collector Node | 10](#)
- [Configure Log Collector Settings in Junos Space Network Management Platform | 11](#)

To use the log collector functionality that comes with Security Director Insights, you need to add the IP address of the Security Director Insights VM and enable it as the log collector. Before you add the log collector node in the GUI, you'll need to set the administrator password. By default, the Security Director log collector is disabled. You'll need to enable it and then set the administrator password.

Enable Log Collector

1. Go to the Security Director Insights CLI.

```
# ssh admin@${security-director-insights_ip}
```

2. Enter the application configuration mode.

```
user:Core# applications
```

3. Enable Security Director log collector.

```
user:Core#(applications)# set log-collector enable on
```

4. Configure the administrator password.

```
user:Core#(applications)# set log-collector password
```

Enter the new password for SD Log Collector access:

Retype the new password:

Successfully changed password for SD Log Collector database access

Add Security Director Insights VM as the Log Collector Node

To add the Security Director Insights VM IP address as a log collector node:

1. From the Security Director user interface, select **Administration > Logging Management > Logging Nodes**, and click the plus sign (+).

The Add Logging Node page opens.

2. Choose the log collector type as **Security Director Log Collector**.

3. Click **Next**.

The Add Collector Node page opens.

Add Logging Node ?



Add Collector Node

Node 1

Node Name* ?	10. [redacted]
	Valid
IP Address* ?	10. [redacted]
User Name* ?	admin
Password* ?	*****

Cancel

Back

Next

4. Configure settings for the log collector node:

- Node Name—Enter a unique name for the log collector
- IP Address—Enter the IP address of the Security Director Insights VM. The IP address must exactly match the IP address you used for the Security Director insights VM in step "12" on page 6 of the Install Security Director Insights procedure.
- User Name—Enter the username of the Security Director Insights VM
- Password—Enter the password of the Security Director Insights VM

Click **Next**. The certificate details are displayed.

5. Click **Finish** and then click **OK** to add the logging node you just created.

Configure Log Collector Settings in Junos Space Network Management Platform

1. Log in to Junos Space Network Management Platform.
2. Select **Administration > Applications**.
3. Right-click **Log Director** and select **Modify Application Settings**.
4. Enable the following options:
 - Enable SDI Log Collector Query Format

- Integrated Log Collector on Space Server



NOTE:

- The log collector in Security Director Insights supports up to 25K eps.
- Disable the raw log: `user:Core#(applications)# set log-collector raw-log off.`
- Make sure that the SRX Series Firewall configuration points to the corresponding SDI log collector.

Watch and learn how to add the log collector as a special node using Security Director Log Collector.



Video: [Add Log Collector \(Security Director\)](#)

Add a JSA Log Collector Node to Security Director

Let's add a JSA log collector Node to Security Director to view the log data on the Dashboard, Events and Logs, Reports, and Alerts pages.

1. Select **Administration > Logging Management > Logging Nodes**.
2. Click the **+** icon to open the Add Logging Node page.
3. Choose **Juniper Secure Analytics** as the log collector type.
4. Complete the Add Collector/JSA Node configuration. If you're not sure what information to provide for a field, hover over the question mark (?).



NOTE: For JSA, provide the admin log in credentials of JSA console.

5. Click **Next** to display the certificate details.
6. Click **Finish** and review the summary of configuration changes.
7. Click **OK** to add the node.

When the configuration is complete, the log collector node is shown with an active status on the Logging Nodes page.

Watch and learn how to add the log collector as a special node using JSA Log Collector.



Video: [Add Log Collector \(JSA\)](#)

Create a Device Discovery Profile

Here's how to create a device discovery profile:

1. Select **Devices > Device Discovery** to open the Device Discovery page.

2. Click the **+** icon to open the Create Discovery Profile page.
3. Complete the configuration. If you're not sure what information to provide for a field, hover over the question mark (?).
4. Click **OK**.

A new device discovery profile is created, and you are returned to the Device Discovery page.

Discover Devices

Now, let's discover devices with the device discovery profile you just created.

1. Select **Devices > Device Discovery** to open the Device Discovery page.
2. Select the device discovery profile and click **Run Now** to trigger the device discovery job.
3. Click **OK** to return to the Device Discovery page.

Watch and learn how to discover devices in Security Director.



Video: [Discover Devices in Security Director](#)

Modify the Configuration of Security Devices

If you need to modify the configuration of one or more security devices, here's how:

1. Select **Devices > Security Devices** to open the Security Devices page.
2. Right-click the devices, and select **Configuration > Modify Configuration**. You can also select this option from the More menu.

The Modify Configuration page opens. By default, the Basic Setup section is selected.

3. Complete the configuration. If you're not sure what information to provide for a field, hover over the question mark (?).
4. Click **Save and Deploy** to save the configuration changes and deploy the saved configuration to the device.

Create Addresses

Now, let's create addresses to use in firewall policies and apply them to SRX Series Firewall.

1. Select **Configure > Shared Objects > Addresses** to open the Addresses page.
2. Click **Create** to open the Create Address page.
3. Complete the configuration. If you're not sure what information to provide for a field, hover over the question mark (?).
4. Click **OK**.

You can use the addresses in firewall policies.

Watch and learn how to create addresses in Security Director.



Video: [Create Addresses in Security Director](#)

Create a Firewall Policy

Here's how to create a firewall policy:

1. Select **Configure > Firewall Policy > Standard Policies** to open the Standard Policies page.
2. Click the + icon to open the Create Firewall Policy page.
3. Complete the configuration. If you're not sure what information to provide for a field, hover over the question mark (?).
4. Click **OK**.

A new policy is created. To activate the policy, add rules in one or more rule bases. You can click the policy name to assign rules inline and then click the + icon to configure policy rules.

Watch and learn how to create a standard firewall policy in Security Director.



Video: [Create a Standard Firewall Policy in Security Director](#)

Assign Policies to Domains

To enable a firewall policy, you'll need to assign it to a domain. You can assign only one policy at a time to a domain. Security Director validates the domain assignment. If the assignment is not acceptable, it displays a warning message.

1. Select **Configure > Firewall Policy > Standard Policies** to open the Standard Policies page.
2. Right-click the policy, and select **Assign Standard Policies to Domains**. You can also select this option from the More menu.

The Assign Standard Policies to Domain page opens.

3. Select the required items to assign to a domain.
4. Select the **Ignore** check box to ignore the warning messages, if any.
5. Click **OK**.

Security Director assigns the policy to the selected domain. You can now use the policy.

Assign Devices to a Policy

Now that you've assigned a policy or policies to a domain, let's assign devices to the policy.

1. Select **Configure > Firewall Policy > Standard Policies** to open the Standard Policies page.
2. Right-click the policy, and select **Assign Devices**. You can also select this option from the More menu.
The Assign Devices page opens.
3. Select the device you want to add to the policy.
4. Click **OK**.
Security Director assigns the devices to the policy.

Publish and Update Policies on Devices

Now you're ready to apply your firewall policies to the security devices on your network.

1. Select **Configure > Firewall Policy > Standard Policies** to open the Standard Policies page.
2. Select one or more policies and click **Update** to open the Update Firewall Policy page.
3. Select **Run now** or **Schedule at a later time**.
4. Select the devices on which you want to publish and update policies.
5. Click **Publish and Update**.
A confirmation message appears.
6. Click **Yes** to publish and update policies on the selected devices.

Configure Juniper ATP Cloud or ATP Appliance with Policy Enforcer

If you're using Policy Enforcer with Security Director, you'll need to configure Juniper ATP Cloud or ATP Appliance. You'll need a Juniper ATP Cloud license and a Juniper ATP Cloud account for three of the configuration types (ATP Cloud or ATP Appliance with Juniper Connected Security, ATP Cloud or ATP Appliance, and Cloud Feeds only), but not for the default mode (No Selection). If you don't have an ATP Cloud license, contact your local sales office or Juniper Networks partner to place an order for an ATP Cloud premium or basic license.

Here's how to do the initial configuration of Juniper ATP Cloud or ATP Appliance:

1. In the Security Director user interface, select **Administration > Policy Enforcer > Settings**.
2. Enter the IP address and login credentials of the Security Director Insights VM.
3. Use the Guided Setup, which is the most efficient way, to complete your initial configuration of Policy Enforcer and Juniper ATP Cloud. In the Security Director user interface, navigate to **Configure > Guided Setup > Threat Prevention**. Click **Start Setup** to begin.
4. Configure tenants, secure fabric, policy enforcement groups, ATP Cloud realms, policies, Geo IP, and click **Finish**.

Step 3: Keep Going

IN THIS SECTION

- [What's Next? | 16](#)
- [General Information | 17](#)
- [Learn With Videos | 17](#)

Congratulations! Your Security Director basic configuration is complete. Here are some things you can do next:

What's Next?

If you want to	Then
Learn how to use the Security Director Dashboard	See Dashboard Overview
Create alerts, reports and filters for events and logs	See Events and Logs Overview
Create device discovery profiles	See Overview of Device Discovery in Security Director
Configure additional firewall policies	See Firewall Policies Overview
Create and assign roles to users	See Overview of Users in Security Director
Generate reports and create log report definitions	See Reports Overview
Use Juniper Secure Analytics (JSA) Series Appliance as a Log Collector to view log data in Security Director	Visit JSA Series Virtual Appliance Documentation

General Information

If you want to	Then
See all documentation available for Security Director	Visit Security Director Documentation
See all documentation available for Security Director Insights	Visit Security Director Insights Documentation
See all documentation available for Juniper ATP Cloud	Visit Juniper Advanced Threat Prevention (ATP) Cloud Documentation
See all documentation available for Junos OS	Visit Junos OS Documentation
Configure advanced Security Director features	See the Security Director User Guide
See, automate, and protect your network with Juniper Security	Visit the Security Design Center
Stay up-to-date with new and changed features and known and resolved issues	See the Security Director Release Notes
Find matching schemas for Junos OS releases	See the knowledge base articles KB21796 and KB22263
Understand the specifications and required licensing	See Security Director specifications
Use prebuilt topologies to explore our products and solutions—all for free!	Visit Juniper vLabs

Learn With Videos

Our video library continues to grow! Here are some great video and training resources that will help you expand your knowledge of Juniper Network Products.

If you want to	Then
Watch a video on how to use Security Director to configure Juniper Secure Connect	See Configuring Juniper Secure Connect - Security Director
Watch a video on how to use Security Director to configure LAG interfaces on SRX Series Firewalls	See Configuring LAG Interfaces-Security Director
Watch a video on how to use Security Director with IPS templates on SRX Series Firewalls	See Using IPS Templates With Security Director
Watch a video on how to use Security Director to configure routing instances on SRX Series Firewalls	See Using Routing Instances In Security Director
Watch a video on how to use Security Director with schedulers on SRX Series Firewalls	See Using Schedulers With Security Director
Watch a video on how to use Security Director to configure and monitor screens on SRX Series Firewalls	See Using Screens With Security Director
Watch a video on how to use Security Director to configure security zones for SRX Series Firewalls	See Using Security Zones With Security Director
Watch a video on how to use Security Director to configure static routes on SRX Series Firewalls	See Using Static Routes With Security Director
Get short and concise tips and instructions that provide quick answers, clarity, and insight into specific features and functions of Juniper technologies.	See Learning with Juniper on Juniper Networks main YouTube page.
View a list of the many free technical trainings we offer at Juniper.	Visit the Getting Started page on the Juniper Learning Portal.