



# Juniper SRX Series Firewalls Content Security User Guide

[Home](#) » [JUNIPer](#) » Juniper SRX Series Firewalls Content Security User Guide 

## Contents

- [1 Juniper SRX Series Firewalls Content Security](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Juniper Content Security Features](#)
- [5 Activate and Install Juniper Content Security Subscriptions and Licenses](#)
- [6 Activate Your Subscription](#)
- [7 Step 2: Up and Running](#)
- [8 Configure the SRX to Use the Default Avira Antivirus Profile](#)
- [9 Validate Avira Antivirus on the SRX](#)
- [10 Step 3: Keep Going](#)
- [11 General Information](#)
- [12 Documents / Resources](#)
  - [12.1 References](#)



## Juniper SRX Series Firewalls Content Security



## Product Information

The Juniper Networks Content Security solution provides comprehensive protection against malware, viruses, phishing attacks, intrusions, spam, and other threats for SRX Series Firewalls. By consolidating security features and services into one device or service, Juniper Content Security streamlines the installation and management of Juniper's expansive security solutions. Most Juniper Content Security features are available as a subscription service and require a license. The features include:

- **Antispam Filtering:** Allows you to tag or block unwanted email traffic by scanning inbound and outbound SMTP e-mail traffic. It supports third-party server-based spam block lists (SBL) and allows you to create local allow lists and blocklists. This feature complements your existing antispam server.
- **Antivirus Content Filtering:** Blocks or permits certain types of traffic based on MIME type, file extension, and protocol command. It controls file transfers across the gateway by checking traffic against filter lists.
- **Web Filtering:** Manages Internet usage by preventing access to inappropriate Web content. There are three types of Web filtering: redirect Web filtering, local Web filtering, and enhanced Web filtering. Redirect and local Web filtering do not require a subscription license.

## **Product Usage Instructions**

### **Step 1: Begin**

**To get started with Juniper Content Security, follow these steps:**

1. **Meet Juniper Content Security:** Understand the features and benefits of Juniper Content Security.
2. **Activate and Install Juniper Content Security Subscriptions and Licenses:** Learn how to activate your subscription and generate license keys, and how to install the license keys on your SRX Series Firewalls.

### **Meet Juniper Content Security**

The Juniper Networks Content Security solution provides comprehensive protection against malware, viruses, phishing attacks, intrusions, spam, and other threats for SRX Series Firewalls. By consolidating security features and services into one device or service, Juniper Content Security streamlines the installation and management of Juniper's expansive security solutions. Most Juniper Content Security features are available as a subscription service and require a license. In this guide, we walk you through how to activate your subscription and generate license keys, and how to install the license keys on your SRX Series Firewalls. We also show you how to enable a default Avira Antivirus profile.

## **Juniper Content Security Features**

**Here's a summary of the Juniper Content Security features and which ones require licenses:**

Content Security Feature	Requires License	Description
Antispam Filtering	Yes	Antispam filtering allows you to tag or block unwanted email traffic by scanning inbound and outbound SMTP e-mail traffic. Antispam filtering allows you to use both a third-party server-based spam block list (SBL) and to optionally create your own local allow lists and blocklists for filtering against email messages. The antispam feature is not meant to replace your antispam server, but to complement it. To learn more about Antispam filtering, see Antispam Filtering Overview.
Antivirus	Yes	There are two types of Juniper Content Security Antivirus features: Sophos and Avira. Sophos antivirus is an in-the-cloud antivirus solution which offers decoding support for application layer protocols such as HTTP, HTTPS, FTP, SMTP, POP3, and IMAP. To learn more about the content security Sophos antivirus features, see Sophos Antivirus Protection. Avira antivirus is an on-device scan engine which scans network traffic for infected files, trojans, worms, spyware, and other malicious data, and immediately blocks the content. To learn more about the content security Avira antivirus features, see On-Device Avira Antivirus.
Content Filtering	No	Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the gateway by checking traffic against filter lists. To learn more about content filtering, see Content Filtering Overview.
Web Filtering	Varies	The Web filtering module lets you manage Internet usage by preventing access to inappropriate Web content. There are three types of Web filtering: redirect Web filtering, local Web filtering, and enhanced Web filtering. Redirect and local Web filtering do not require a subscription license. To learn more about content security Web filtering, see Web Filtering Overview.

- **Antispam Filtering:** Requires a license. It allows you to tag or block unwanted email traffic by scanning inbound and outbound SMTP e-mail traffic. It supports third-party server-based spam block lists (SBL) and allows you to create local allow lists and blocklists.
- **Antivirus Content Filtering:** Requires a license. It blocks or permits certain types of traffic based on MIME type, file extension, and protocol command.
- **Web Filtering:** Varies. There are three types of Web filtering: redirect Web filtering, local Web filtering, and enhanced Web filtering. Redirect and local Web filtering do not require a subscription license.

## Activate and Install Juniper Content Security Subscriptions and Licenses

Before you begin the activation process, make sure you have purchased your Juniper Content Security subscription license(s). Once purchased, you will receive a Juniper Software Entitlement Certificate by email containing an authorization code and Software Support Reference Number (SSRN).

### Follow these steps:

1. **Activate Your Subscription:** Use the provided authorization code and SSRN to activate your subscription.
2. **Install the Subscription License on an SRX Series Firewall:** Generate license keys for your SRX Series Firewalls and install them.

For more information about Juniper licensing, refer to the [Juniper Licensing User Guide](#).

**NOTE:** You can also find the activation code by running the “show system license” command through the J-Web Monitor Dashboard.

Once you’ve purchased your Juniper Content Security subscription license(s), we’ll send you a Juniper Software Entitlement Certificate by email that contains an authorization code and Software Support Reference Number (SSRN). You’ll need these to activate your subscription and generate license keys for installing the subscription licenses on your SRX Series Firewalls. Check out this link for more information about Juniper licensing: Juniper Licensing User Guide


## Before You Begin

- Install your SRX Series Firewalls and verify you have network access. The quickest and easiest way to do this is to follow the three-step instructions in the Quick Start guide for your SRX Series Firewall model. See Quick Start
- Set up a Juniper Networks user account to access the Customer Support Center or Partner Center. If you don’t already have one, see Account Setup. If you need help with account registration, see Login Assistance.
- (For hardware devices only), have the product serial number handy.  
You can find the product serial number by running the show chassis hardware command through the J-Web Monitor Dashboard.
- Verify that you’ve received the Juniper Software Entitlement Certificate we sent you in email. The certificate contains a 17-character activation code (sometimes referred to as authorization code or security key) and the SSRN.

**NOTE:** You can also find the activation code by running the show system license command through the J-Web Monitor Dashboard.

- The activation code expires in three days.

Here’s an example of the Juniper Software Entitlement Certificate.



Juniper Networks (US), Inc.  
 (California)  
 370 W Caribbean Drive  
 Sunnyvale  
 94089

Date Issued : 15-AUG-2018		Customer PO : 12AB345C	
Order Number : 15012345		Model Number :	SRX320-CS-BUN-3
		Model Description :	3 YR CONTENT SECURITY BUNDLE ON SRX320

Juniper Software Entitlement Certificate

Item#	Activation Code	Support Ref.No.	Quantity
1	AbcdEF-GHiJK-lmNoPQ	123456789123	2

## Activate Your Subscription

1. Log in to the Juniper Networks Agile Licensing Portal using the credentials you set up in your user account.
2. On the home page, enter your activation code in the Activate field and click Activate.

The Product Activation page displays.

3. For hardware products, enter the device serial number in the Device Serial Number field.

If the device serial number is not registered, you'll be routed to the product registration page. Fill in the page to register your device. Only hardware devices need to be registered.

4. In the Select an Option section, specify if you're activating the license for yourself or on behalf of an end customer. Only channel partners will see the option for activating on behalf of an end customer.
5. Enter the relevant email address in the Send License Key via E-mail field to email the license key.
6. Select the I Agree with Terms & Conditions checkbox.
7. Click Activate.
8. Enter a new location or use the default address.
9. Click Submit.

The Confirmation page displays to confirm that the subscription is activated.

10. Click I'm Done to return to the Home page.

Content security will generate your license keys and send them to the email address you specified. If you don't receive the email message, check out the Troubleshooting section in the Juniper Knowledgebase article KB9861.

### **Here are a few things to note about activating a subscription:**

- The Entitlements section in the Juniper Agile Licensing portal lists the activation codes that are linked to your Juniper Networks company account and awaiting activation.
- You use the Juniper Networks Agile Licensing Portal to activate perpetual and subscription software licenses.
- During the activation process, the Juniper Networks Agile Licensing Portal also registers the products to your company.

### **Install the Subscription License on an SRX Series Firewall**

Now that you've activated your Juniper Content Security subscription and have your license keys, you're ready to install the subscription license on your SRX Series Firewall.

1. Establish basic network connectivity with the SRX Series Firewall.
2. Run the set system license keys key name command.

The name parameter includes the license ID and the license key.

#### **For example:**

```
[edit] user@device# set system license keys key "ANTI_SPAM_KEY_SBL" xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx  
xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
```

**To install multiple license keys, run the set system license keys key name command for each license key to install. For example:**

```
[edit] user@device# set system license keys key "key_1"  
set system license keys key "key_2"  
set system license keys key "key_2"  
set system license keys key "key_4"
```

3. Commit the configuration.

```
[edit] user@device# commit  
commit complete
```

4. Verify that the license keys were installed.

```
user@device# show system license
root> show system license
License usage:

Feature name          Licenses used  Licenses installed  Licenses needed  Expiry
anti_spam_key_sb1      0             1                   0                2021-06-11 09:36:04 UTC
av_key_sophos_engine    0             1                   0                2021-06-11 09:36:04 UTC
wf_key_websense_ewf     0             1                   0                2021-06-11 09:36:04 UTC
```

**NOTE:** You can also run the show system license command from operational mode.

For SRX300, SRX320, SRX340, SRX345, and SRX550M firewalls, reboot the device after you install the license(s). The SRX Series Firewall reserves additional memory for Juniper Content Security features. This decreases the session capacity.

For SRX4600, SRX5600 and SRX5800 firewalls, run the following command to manually reallocate the memory for content security features:

```
user@host> set security forwarding-process application-services enable-utm-memory
```

Reboot the device for the configuration to take effect.

**NOTE:** SRX1500, SRX4100 and SRX4200 firewalls have enough memory for Juniper Content Security. You don't need to allocate memory for these devices.

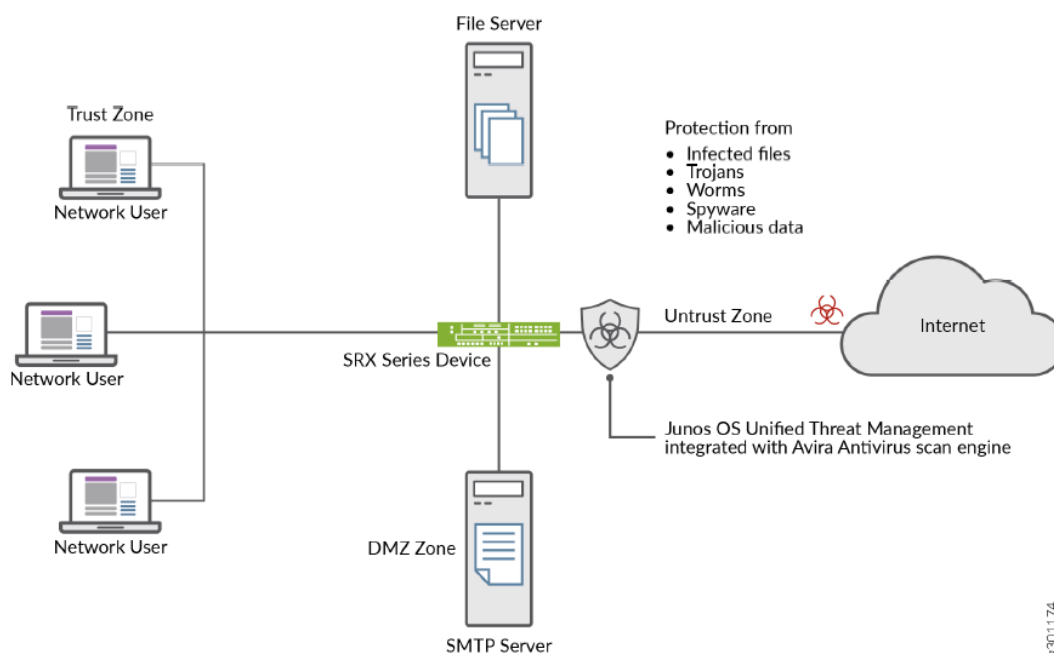
- You'll need to reinstall the license after installing or upgrading to a new Junos OS Release version. Unlicensed features, such as Juniper Content Security blocklists and allowlists, will continue to function without a license.

## Step 2: Up and Running

### Enable the Juniper Networks Default Avira Antivirus Profile

As an introduction to using the Juniper Content Security solution, let's enable , Avira antivirus. In this example, we show you how to enable a preconfigured default Avira antivirus profile. When you enable the default Avira antivirus profile, you don't have to configure additional parameters. Instead, you create a security policy with default antivirus profiles for all protocols, and apply the security policy for the permitted traffic.

Here's an example of how an SRX Series Firewall interacts with Avira antivirus in a typical enterprise network.



## Before You Begin

- Verify that you have a Juniper Networks Avira Antivirus license and that it's enabled on the SRX Series Firewalls. For more information on how to verify which licenses are activated on an SRX Series Firewall, see Juniper Licensing User Guide.
- Install your SRX Series Firewalls with Junos OS Release 18.4R1 or later.

We've tested this example using an SRX1500 firewall with Junos OS Release 18.4R1.

## Configure the SRX to Use the Default Avira Antivirus Profile

1. Enable the Avira antivirus scan engine on your SRX Series Firewall.

```
user@host# set security utm default-configuration anti-virus type avira-engine
```

2. Reboot the SRX Series Firewall so the new scan engine can take effect.

3. Set the default antivirus profile for HTTP, FTP, SMTP, POP3, and IMAP protocols.

```
[edit] user@host# set security utm default-configuration anti-virus type avira
```

```
user@host# set security utm utm-policy P1 anti-virus http-profile junos-av-defaults
```

```
user@host# set security utm utm-policy P1 anti-virus ftp upload-profile junos-av-defaults
```

```
user@host# set security utm utm-policy P1 anti-virus ftp download-profile junos-av-defaults
```

```
user@host# set security utm utm-policy P1 anti-virus smtp-profile junos-av-defaults
```

```
user@host# set security utm utm-policy P1 anti-virus pop3-profile junos-av-defaults
```

```
user@host# set security utm utm-policy P1 anti-virus imap-profile junos-av-defaults
```

4. Apply the default antivirus profile to the security policy.

```
[edit] user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match source-address any
```

```
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match destination-address any
```

```
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 match application any
```

```
user@host# set security policies from-zone trust to-zone untrust policy POLICY-1 then permit application-services utm-policy P1
```

5. Commit the configuration.

```
[edit] user@host# commit
```

You can also watch the video Avira Antivirus Solution on SRX Series Firewalls to understand how to install and use Avira antivirus on your SRX Series Firewalls.

## Validate Avira Antivirus on the SRX

**Here's a safe way to verify that the Avira antivirus solution is working on an SRX Series Firewall:**

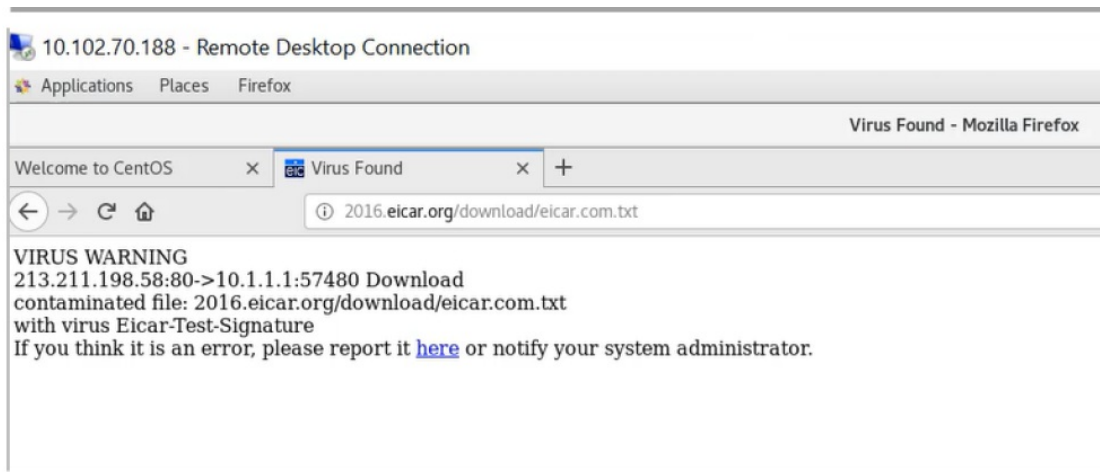
1. Access the EICAR website.

<https://eicar.org>.

2. Download the Anti-malware test file.

3. Follow the instructions on the screen.

When you try to download an unsafe file, your device will display an error message. The message indicates that your device has blocked malicious content.



### Step 3: Keep Going

Congratulations! You've completed the initial steps to get Juniper Content Security up and running. Let's keep going and learn more about what you can do with the Juniper Content Security solution.

#### What's Next?

Now that your devices are subscribed to Juniper Content Security, here are some things you can do next.

If you want to	Then
Continue configuring Antivirus protection	See Antivirus Protection
Configure Antispam filtering	See Antispam Filtering

If you want to	Then
Configure content filtering settings	See Content Filtering
Learn more about Unified Policies	View the Introduction to Unified Policies video

### General Information


Here are some excellent resources that will help you take your Juniper Content Security knowledge to the next level:



If you want to	Then
Find in-depth product documentation for Juniper Content Security	Check out the Juniper Content Security User Guide in the Juniper TechLibrary
Understand the latest security advisories, and get a little extra help implementing your security solution	Take advantage of these awesome Juniper support resources: <ul style="list-style-type: none"> <li>• Security Advisories</li> <li>• Security Services</li> <li>• JTAC and Customer Care Contact Information</li> </ul>
See all documentation available for Junos OS	See the Junos OS Documentation
Stay up to date on new and changed features and known and resolved issues	See the Junos OS Release Notes
Learn about training and certification opportunities	Explore these options: <ul style="list-style-type: none"> <li>• Juniper Security (JSEC) On-Demand</li> <li>• Junos Networks Security Learning Path</li> <li>• Security Certification Track</li> </ul>
Ask your peers. Connect to labs. Find new learning opportunities	Visit the <a href="#">Intrusion Prevention Forum</a>

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2023 Juniper Networks, Inc. All rights reserved.

## Documents / Resources

	<p><a href="#">Juniper SRX Series Firewalls Content Security</a> [pdf] User Guide</p> <p>SRX Series Firewalls Content Security, SRX Series, Firewalls Content Security, Content Security, Security</p>
---	--

## References

-  [Community Home - Elevate Community | Juniper Networks](#)
-  [Eicar – EUROPEAN EXPERT GROUP FOR IT-SECURITY](#)
-  [CEC Juniper Community](#)
-  [CEC Juniper Community](#)

-  [Juniper Security On-Demand](#)
-  [Juniper Networks Certification Tracks](#)
-  [license.juniper.net/licensemanage/](https://license.juniper.net/licensemanage/)
-  [Contact - Support - Juniper Networks](#)
-  [User Registration](#)
-  [User Registration](#)
-  [Quick Start | Juniper Networks](#)
-  [Junos OS Documentation | Juniper Networks](#)
-  [Junos OS Documentation | Juniper Networks](#)
-  [Content Security User Guide | Junos OS | Juniper Networks](#)
-  [Web Filtering Overview | Junos OS | Juniper Networks](#)
-  [On-Device Avira Antivirus | Junos OS | Juniper Networks](#)
-  [Sophos Antivirus Protection | Junos OS | Juniper Networks](#)
-  [Antispam Filtering Overview | Junos OS | Juniper Networks](#)
-  [Content Filtering | Junos OS | Juniper Networks](#)
-  [Juniper Licensing User Guide | Licensing | Juniper Networks](#)
-  [Juniper Licensing User Guide | Licensing | Juniper Networks](#)
-  [Services for Security | Juniper Networks US](#)
-  [Certification Tracks | Juniper Networks US](#)
- [User Manual](#)

Manuals+.