JUNIPER NETWORKS | Engineering Simplicity

Security Director Application Guide for JSA and IBM QRadar

Published
2019-10-30

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Security Director Application Guide for JSA and IBM QRadar

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | v

Documentation and Release Notes | **v**

Documentation Conventions | **v**

Documentation Feedback | **viii**

Requesting Technical Support | **viii**

- Self-Help Online Tools and Resources | **ix**
- Creating a Service Request with JTAC | **ix**

1 **Installing and Using the Security Director Application**

Security Director Application Integration Overview | 13

- Benefits of Security Director Application Integration | **13**

Installing the Security Director Application | 14

Registering JSA and IBM QRadar with Security Director | 19

Blocking Offenses in JSA and IBM QRadar with Security Director | 21

Reference Sets | 22

Uninstalling the Security Director Application | 24

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

Use this guide to understand the integration and workflow to create firewall policies in Security Director based on the events triggering the offense in Juniper Secure Analytics (JSA).

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page vi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page vi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

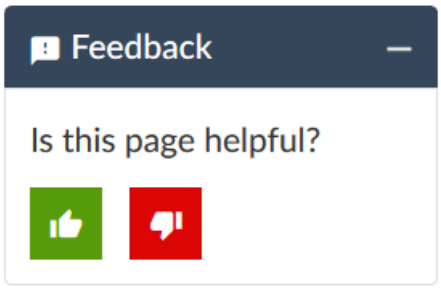
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

1

CHAPTER

Installing and Using the Security Director Application

Security Director Application Integration Overview | **13**

Installing the Security Director Application | **14**

Registering JSA and IBM QRadar with Security Director | **19**

Blocking Offenses in JSA and IBM QRadar with Security Director | **21**

Reference Sets | **22**

Uninstalling the Security Director Application | **24**

Security Director Application Integration Overview

The Security Director application integration provides a workflow to create Security Director firewall policies based on the events triggering the offense. You can create firewall rules in Security Director using the Security Director Extension wizard and apply them on firewall devices. JSA and IBM QRadar work with Security Director to block malicious IP addresses contained within an offense.

Administrators can integrate Security Director with the Juniper Secure Analytics (JSA) or IBM QRadar offense workflow by installing the Security Director application on JSA or IBM QRadar. The application is supported on JSA Release 2014.8 (IBM QRadar Release 7.2.8) and later.

You must register Security Director with JSA or IBM QRadar. After successful registration, you can create firewall rules using the Security Director Extension wizard.

This integration allows the JSA and IBM QRadar administrators to seamlessly create firewall rules for an offense and navigate to Security Director to view or modify firewall rules. In addition, after registration, all available reference sets in JSA or IBM QRadar are automatically converted to dynamic address groups in Security Director. Whenever an administrator creates a reference set, the corresponding dynamic address group is created in Security Director. The JSA and IBM QRadar administrators can use these dynamic address groups to configure firewall policy rules.

NOTE:

- Administrators with policy create and edit access in Security Director can automatically create firewall rules from JSA and IBM QRadar.
- Administrators can create rules and update the devices in their administrative domain, only.

Benefits of Security Director Application Integration

- Administrator can quickly create firewall rules for an offense reported in JSA or IBM QRadar and deploy the rules to security devices using Security Director, resulting in faster threat prevention. This increases the speed at which malware can be blocked.
- Reference sets in JSA or IBM QRadar are automatically converted to dynamic address groups in Security Director.

RELATED DOCUMENTATION

Installing the Security Director Application | 14

Registering JSA and IBM QRadar with Security Director | 19

Blocking Offenses in JSA and IBM QRadar with Security Director | 21

Uninstalling the Security Director Application | 24

Installing the Security Director Application

Before You Begin

Download the *JSA_SD_App_19.3R1.zip* file from *Security Director Plugin for JSA Offense Integration* link in the download site.

Procedure

To install the Security Director Extension application:

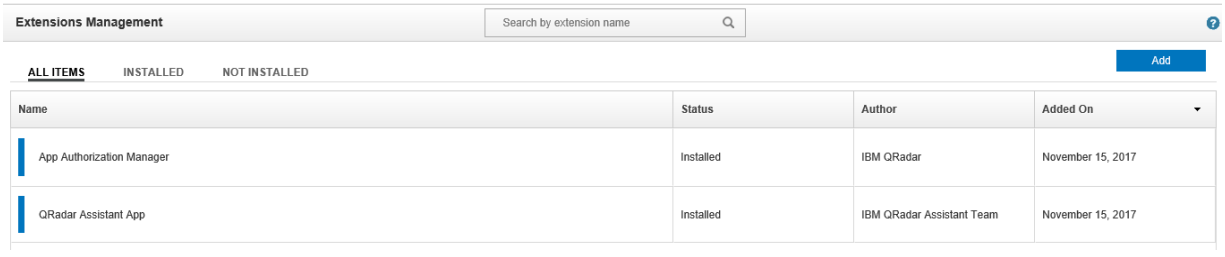
NOTE: You can refer the same procedure to install the application on IBM QRadar.

1. Log in to the JSA application.
2. Select **Admin**.

   The System Configuration options are displayed.
3. Click **Extensions Management**.

   The Extensions Management page is displayed as shown in Figure 1 on page 14.

Figure 1: Extensions Management Page



4. Click **Add**.

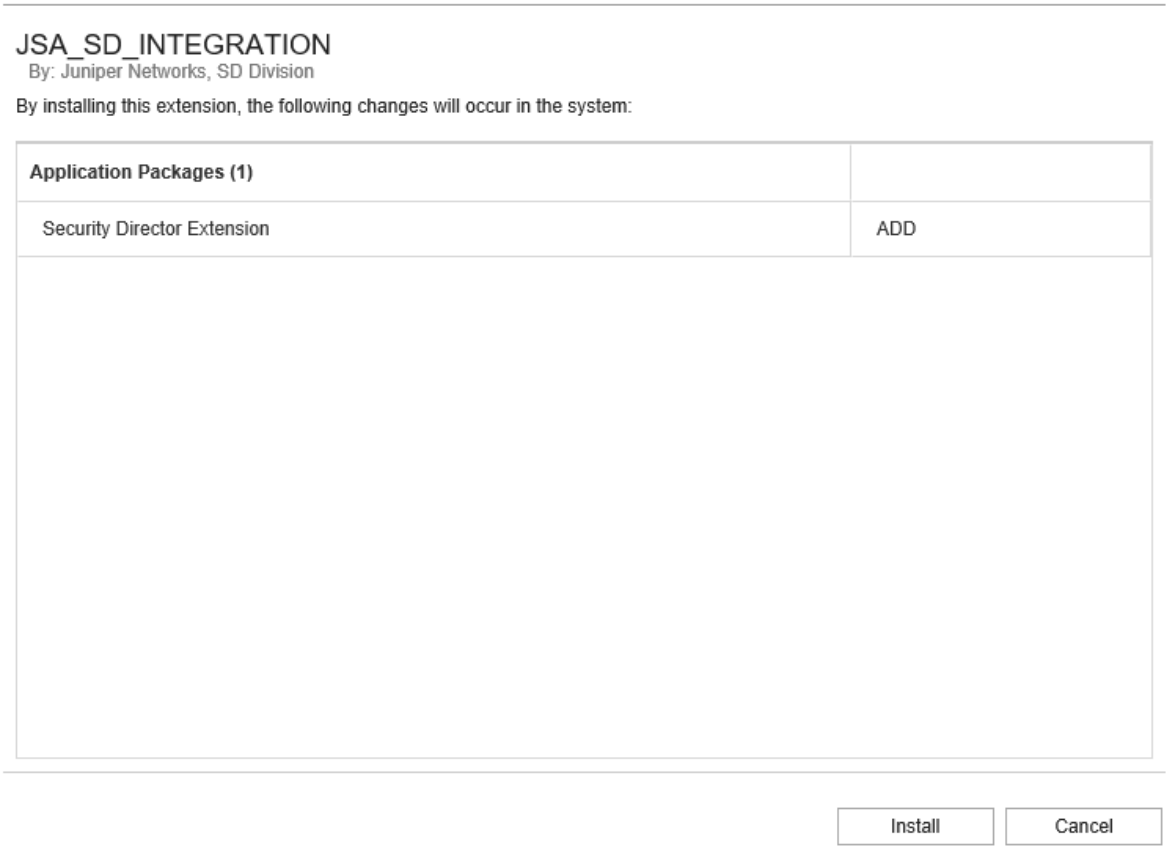
The Add a New Extension page is displayed.

5. Browse and select the *JSA_SD_App_19.3R1.zip* file that you want to upload to the JSA console.

   For JSA to install the application immediately, select the **Install immediately** check box and click **Add**.

   The JSA_SD_INTEGRATION page is displayed as shown in Figure 2 on page 15.

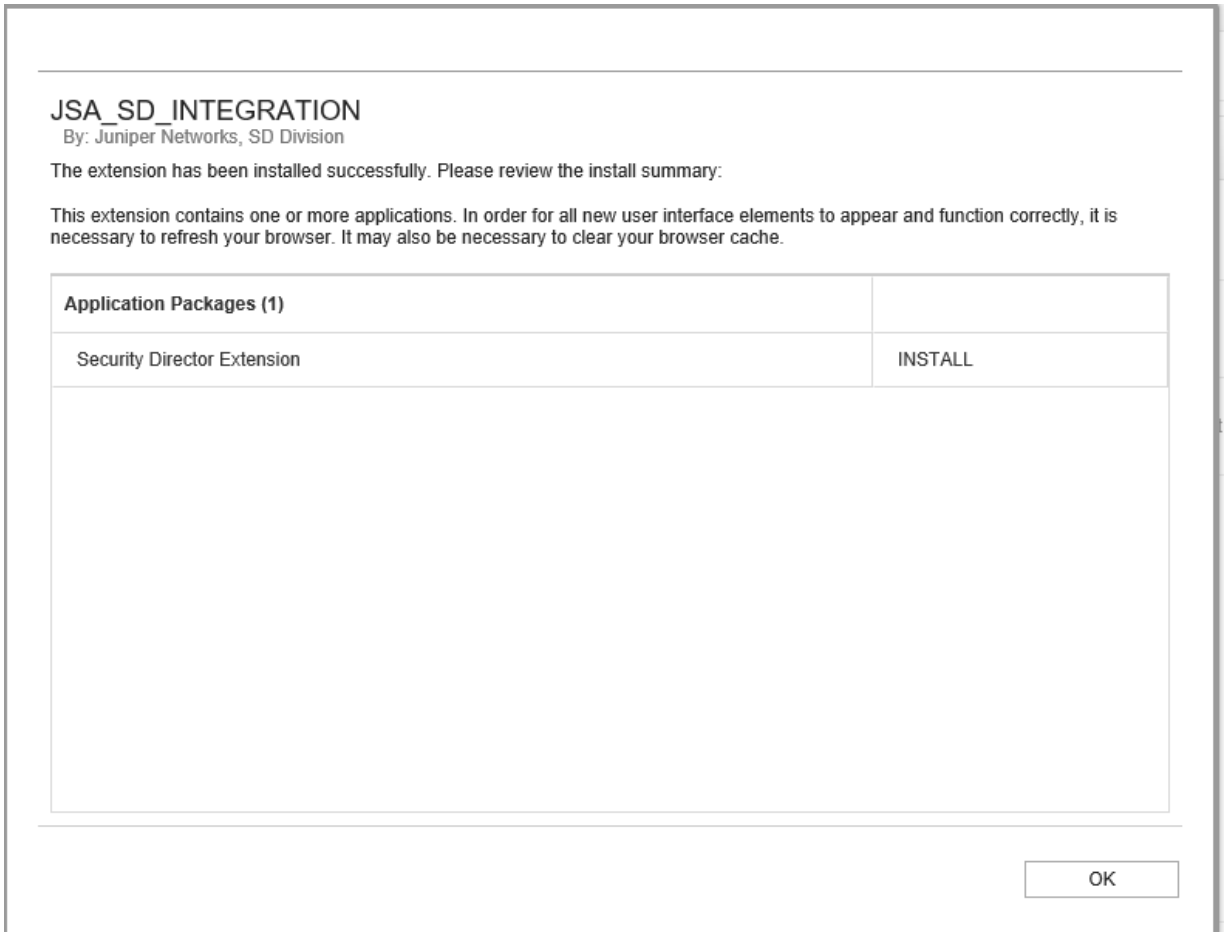
Figure 2: JSA_SD_INTEGRATION Page



6. Click **Install**.

   A success message is displayed as shown in Figure 3 on page 16.

Figure 3: Installation Success Page

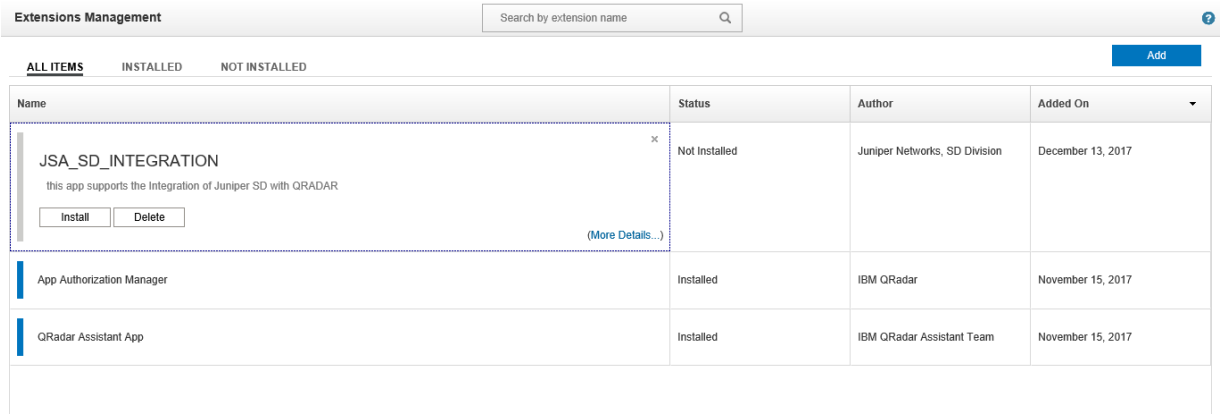


7. Click **OK**.

   In the Extensions Management page, you can view the JSA_SD_Integration application in the ALL ITEMS or INSTALLED tab.

   If you choose not to install the application on upload, then you can select your application in the Extension Management page from ALL ITEMS or NOT INSTALLED tab and install the same as shown in Figure 4 on page 17.

Figure 4: Installation After Upload



Before the application is installed, a preview list of the content is displayed. To preview the contents of an application after it is added and before it is installed, select from the list of extensions, and click **More Details**. Expand the folders to view the items in each group.

a. Click **Install** to install the application.

   The JSA_SD_INTEGRATION page is displayed.

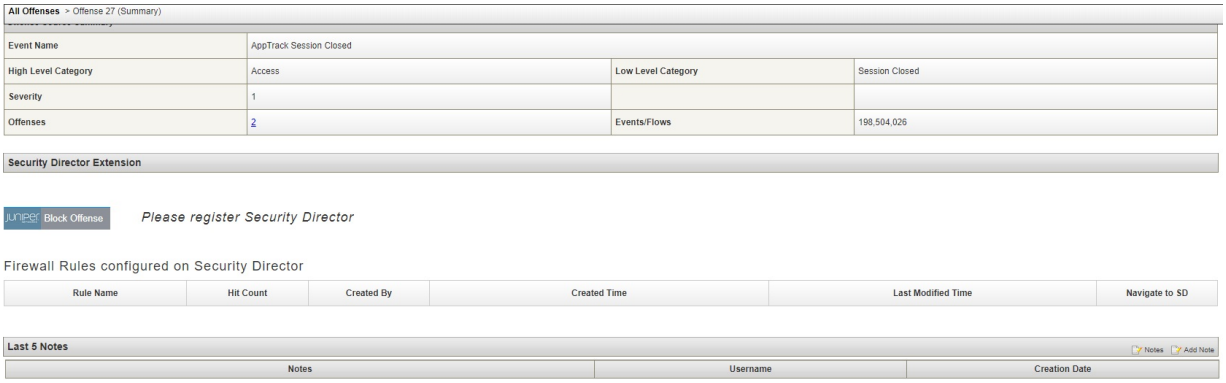
b. Click **Install**.

Before the application is installed, the content is compared with those items that are already in the deployment. If the item exists, you can choose to overwrite or retain the data.

NOTE: It can take several minutes for an application to become active after installation is complete. When the installation is complete, clear your browser cache and refresh the browser window before you use the application.

After installing the application, navigate to **Offenses** > **All Offenses**. Double-click an offense, the Security Director Extension wizard is displayed in the offense summary page as shown in Figure 5 on page 18. The Block Offense button is disabled.

Figure 5: Security Director Extension Wizard After Application Installation



NOTE: Administrator can block the offense only after registering with Security Director. See "Registering JSA and IBM QRadar with Security Director" on page 19.

RELATED DOCUMENTATION

Security Director Application Integration Overview | 13

Registering JSA and IBM QRadar with Security Director | 19

Blocking Offenses in JSA and IBM QRadar with Security Director | 21

Uninstalling the Security Director Application | 24

Registering JSA and IBM QRadar with Security Director

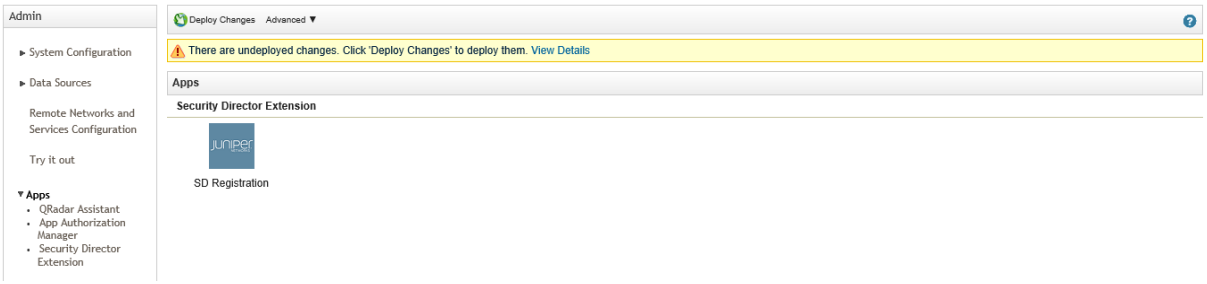
Administrator must register JSA or IBM QRadar with Security Director. After registration, administrator can block an offense.

NOTE: You can refer the same procedure for IBM QRadar.

1. Log in to the JSA application.
2. Select **Admin**.
3. Select **Apps** > **Security Director Extension** in the left hand navigation.

   The Apps page is displayed as shown in Figure 6 on page 19.

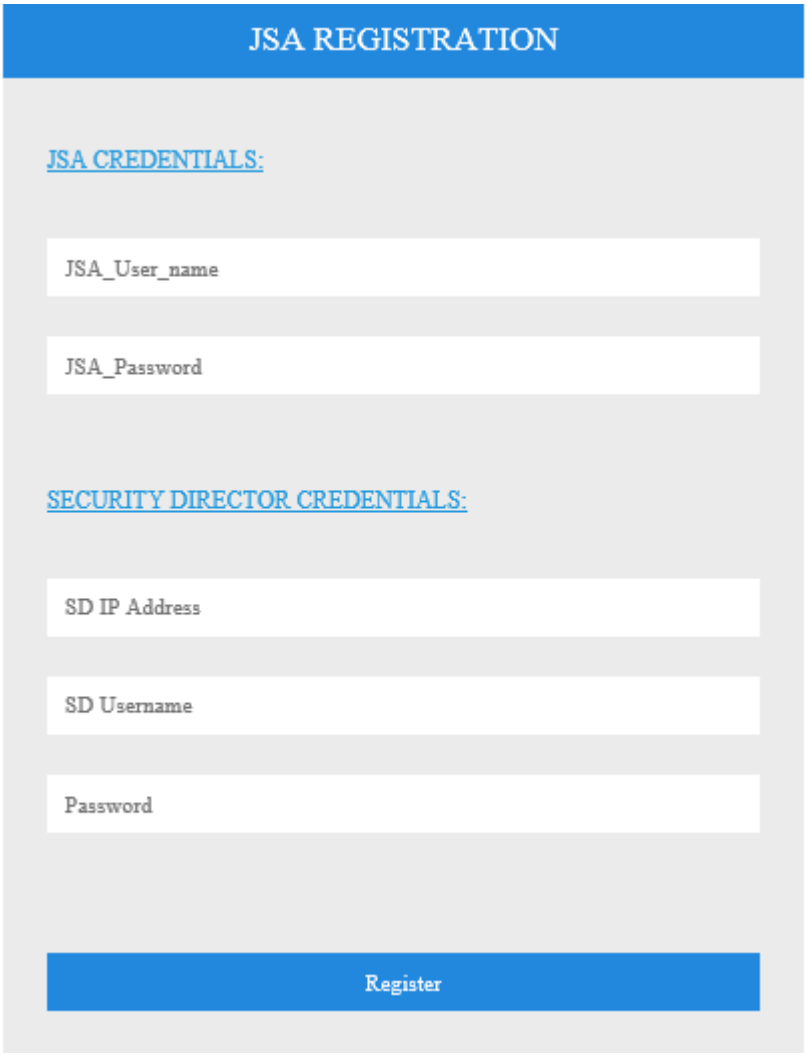
Figure 6: Apps Page



4. Click **SD Registration**.

   The JSA REGISTRATION page is displayed as shown in Figure 7 on page 20.

Figure 7: JSA Registration Page



5. Enter the JSA console and Security Director login credentials and click **Register**.

   The IP address must be in ipv4 format.

   If the JSA and Security Director credentials are valid, then a success message is displayed.

   If the registration is successful, then administrators can block offense using the Security Director Extension wizard in the offense summary page.

RELATED DOCUMENTATION

Security Director Application Integration Overview | 13

Installing the Security Director Application | 14

Blocking Offenses in JSA and IBM QRadar with Security Director | 21

Uninstalling the Security Director Application | 24

Blocking Offenses in JSA and IBM QRadar with Security Director

After successfully registering with Security Director, you can block an offense by selecting source IP addresses and creating rules for them in Security Director.

NOTE: You can refer the same procedure for blocking offense in IBM QRadar.

1. Log in to the JSA application.
2. Select **Offenses** > **All Offenses**.
3. Double-click an offense that you want to block.

   The corresponding offense summary page is displayed. Scroll down to the Security Director Extension wizard as shown in Figure 8 on page 21.

Figure 8: Security Director Extension Wizard

4. Click **Block Offense** to create a firewall rule to block IP addresses from accessing the firewall device.

   The Block Offense page is displayed.

5. Select the source IP addresses causing the offense that you want to block. The table lists the top offending source IP addresses based on events over the past 24 hours, sorted by event count.
6. Click **Create Rules**.

A success message is displayed. Security Director jobs are triggered for publishing and updating the configuration. Then the Job Status button is enabled.

7. Click **Job Status** to monitor the jobs in the Job Management page in Security Director.

The firewall rules are displayed in the Security Director Extensions widget. Click **View in SD** to view the firewall policy rules under Device Specific Policies in the Firewall Policies page in Security Director.

See *Creating Firewall Policy Rules* and *Using Job Management in Security Director* in the Security Director User Guide.

RELATED DOCUMENTATION

- Security Director Application Integration Overview | 13
- Installing the Security Director Application | 14
- Registering JSA and IBM QRadar with Security Director | 19
- Uninstalling the Security Director Application | 24

Reference Sets

You can use reference sets in JSA or IBM QRadar to store data in a simple list format. You can populate the reference set with external data, such as indicators of compromise (IOCs), or you can use it to store business data, such as IP addresses and user names, that is collected from events and flows that occur on your network.

A reference set contains unique values that you can use in searches, filters, rule test conditions, and rule responses. Use rules to test whether a reference set contains a data element, or configure the rule response to add data to a reference set. For example, you can create a rule that detects when an employee accesses a prohibited website, and configure the rule response to add the employee's IP address or user name to a reference set.

Use a reference set to compare a property value, such as an IP address or user name, against a list. You can use reference sets with rules to keep watch lists. For example, you can create a rule to detect when an employee accesses a prohibited website and then add that employee's IP address to a reference set.

After registration with Security Director, all available reference sets are automatically converted to dynamic address groups in Security Director. Whenever an administrator creates a new reference set in JSA or IBM

QRadar, the corresponding dynamic address group is automatically added in Security Director. The dynamic address groups are added with the same name in Security Director.

NOTE: The newly added reference sets are automatically converted to dynamic address groups in Security Director within 5 minutes.

NOTE: You can refer the same procedure for creating reference sets in IBM QRadar.

To add a reference set:

1. Log in to the JSA application.
2. Select **Admin**.

   The System Configuration options are displayed.
3. Click **Reference Set Management**.

   The Reference Set Management page is displayed.
4. Click **Add**.

   The New Reference Collection page is displayed.
5. Configure the parameters according to the guidelines in Table 3 on page 23.
6. Click **Create** to create a reference set or **Cancel** to discard the changes.

Table 3: Reference Collection Parameters

parameter	Description
Name	The maximum length of the reference set name is 255 characters.
Type	Select the data types for the reference elements. You cannot edit the Type parameter after you create a reference set. The IP type stores IPv4 addresses. Alphanumeric (Ignore Case) automatically changes any alphanumeric value to lowercase. To compare obfuscated event and flow properties to the reference data, you must use an alphanumeric reference set.

Table 3: Reference Collection Parameters *(continued)*

parameter	Description
Time to Live of elements	Specifies when JSA automatically deletes elements from the reference set. Lives Forever is the default setting. If you specify an amount of time, indicate whether the time-to-live interval is based on when the data was first seen, or was last seen. When a reference set element expires, a Reference Data Expiry event is triggered. The event contains the reference set name and the element value.

A feed server running in Security Director serves feed requests from SRX or vSRX Series Devices for the Dynamic Address Groups. Before configuring Security Director firewall rules, you must configure feed server on SRX or vSRX Series devices with the following CLI:

set security dynamic-address feed-server JSA hostname *SD_IP*

set security dynamic-address feed-server JSA update-interval 600000

set security dynamic-address feed-server JSA hold-interval 36000000

Administrators can use the dynamic address groups to configure firewall policy rules in Security Director. For configuring firewall policy rules in Security Director, see *Creating Firewall Policy Rules* in Security Director User Guide.

For details on Reference Sets, see JSA Administration Guide.

RELATED DOCUMENTATION

Security Director Application Integration Overview | 13

Installing the Security Director Application | 14

Blocking Offenses in JSA and IBM QRadar with Security Director | 21

Uninstalling the Security Director Application | 24

Uninstalling the Security Director Application

You can uninstall the Security Director application from the JSA or IBM QRadar console.

NOTE: You can refer the same procedure to uninstall the application on IBM QRadar.

To uninstall the Security Director extension application:

1. Log in to the JSA application.

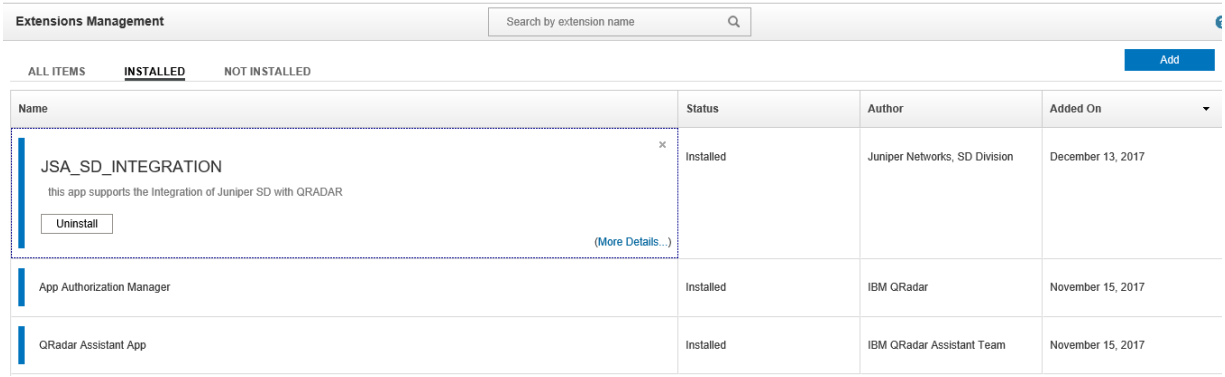
2. Select **Admin**.

   The System Configuration options are displayed.

3. Click **Extensions Management**.

   The Extension Management page appears as shown in Figure 9 on page 25.

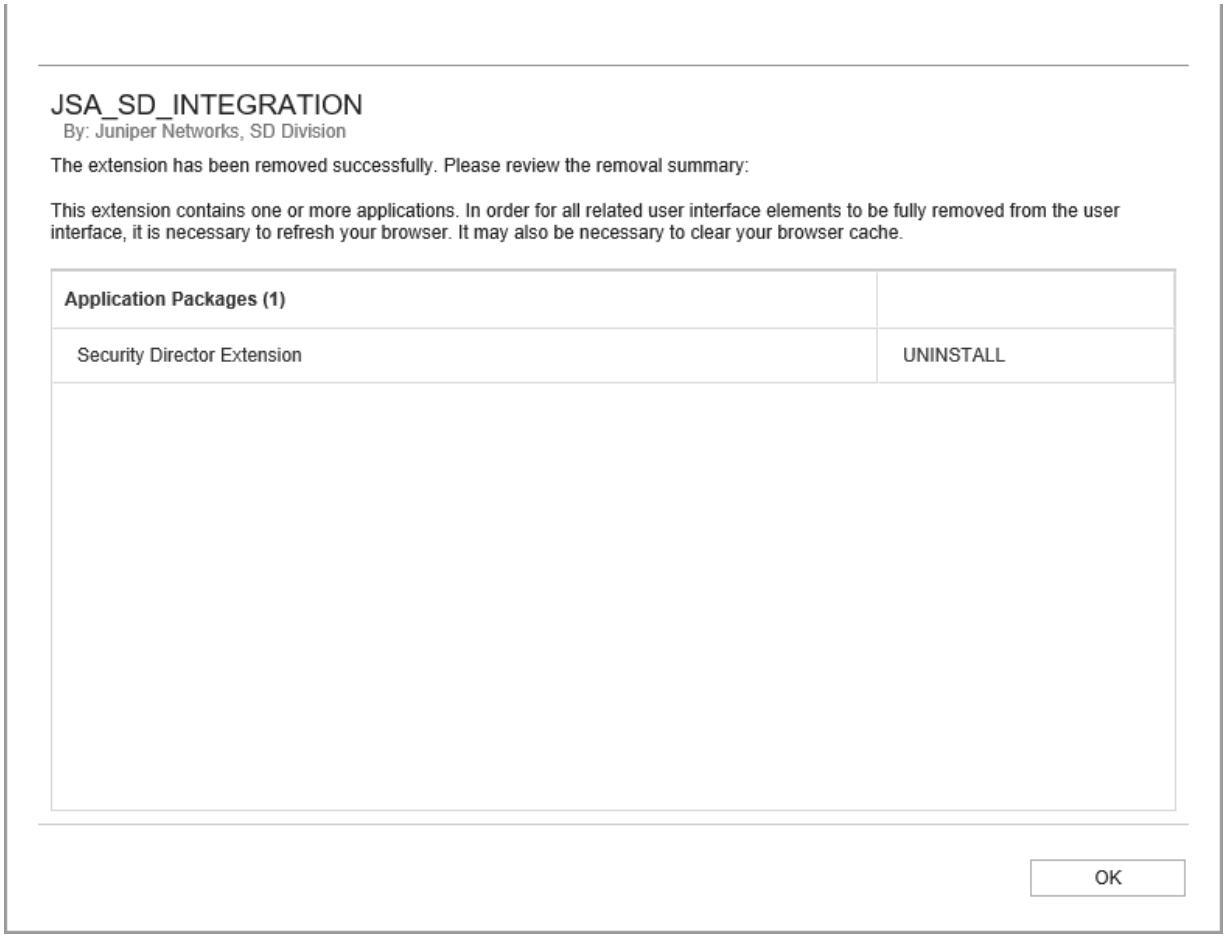
Figure 9: Extensions Management-Uninstall Application



4. Click the **INSTALLED** or **ALL ITEMS** tab and select the application, and then click **Uninstall**.

   A confirmation message is displayed as shown in Figure 10 on page 26.

Figure 10: Success Message-Uninstall Application



5. Click **Uninstall**.

   A success message is displayed.

When you uninstall an application, it is removed from the system. If you want to reinstall it, you must add it again.

RELATED DOCUMENTATION

Security Director Application Integration Overview | 13

Installing the Security Director Application | 14