Engineering
Simplicity

Security Director Cloud Insights On-premises Collector Deployment Guide

Published
2023-10-08

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

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.

Security Director Cloud Insights On-premises Collector Deployment Guide

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 This Guide

Use this guide to understand the architecture and deployment of Security Director Cloud Insights.

1

CHAPTER

Overview

Security Director Cloud Insights Overview

IN THIS SECTION

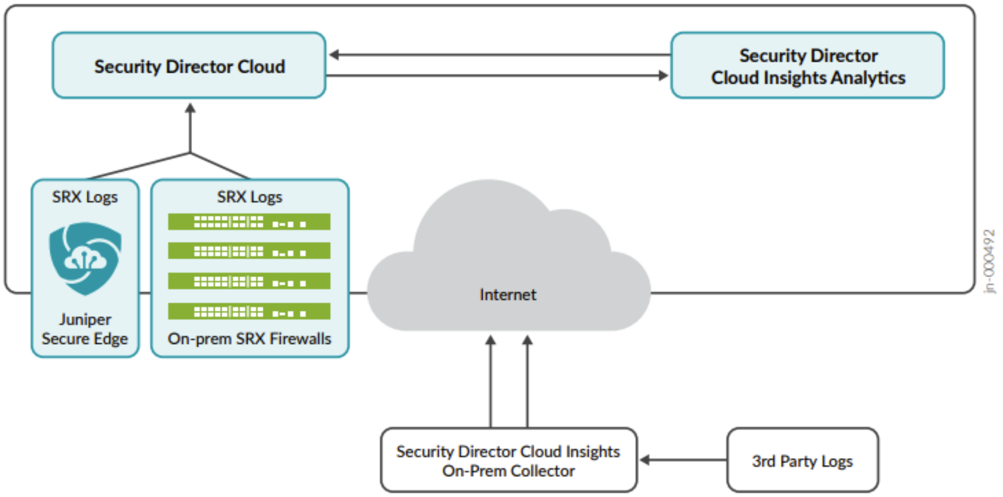
Security Director Cloud Insights facilitates automated security operations. It enables you to take effective actions on security events logged by Juniper Networks security products and third party security products. Security Director Cloud Insights displays events that affect a host or events that are impacted by a particular threat source from different security modules. These events provide instantaneous information about the extent of an attack. The application contains an option to verify the incidents using your trusted threat intelligence provider. After you have verified the incidents, you can take preventive and remedial actions using the rich capabilities of our security products.

Benefits

- Reduce the number of alerts across disparate security solutions.
- Quickly react to active threats with one-click mitigation.
- Improve the security operations center (SOC) teams' ability to focus on the highest priority threats.

Security Director Cloud Insights Architecture

Figure 1: Security Director Cloud Insights Architecture



Security Director Cloud Insights collector collects and aggregates SRX logs and the third party logs. Some of the features in Security Director Cloud uses the SRX logs. You can monitor the incidents and mitigate the events based on your network requirements.

Security Director Cloud Insights receives SRX logs from Juniper Secure Edge or Juniper SRX firewall that are managed by Security Director Cloud. If you have third party security products, then Security Director Cloud Insights receives logs from third party security products. Security Director Cloud Insights correlates the security application logs to tell you what are the most important security incidents in your organization. Security Director Cloud ingests all the security events from different sources and provides unified view to the users.

Security Director Cloud Insights supports the following log collector types:

- Cloud collector—Enable the cloud collector if you receive SRX logs from Juniper Secure Edge or Security Director Cloud managed SRX firewalls. By default, the cloud collector is enabled.

- On-premises collector—If you have a third party log source, such as McAfee, you can deploy Security Director Cloud Insights on-premises collector. You can redirect the output from third party security products to Security Director Cloud Insights on-premises collector. Logs are then filtered and sent to Security Director Cloud.

  If you have any third party security product, you'll need to download Security Director Cloud Insights on-premises collector OVA file from the download site and deploy. See Deploy and Configure Security Director Cloud Insights On-premises Collector.

2

CHAPTER

Deploy On-premises Collector

Deploy and Configure Security Director Cloud Insights On-premises Collector with Open Virtualization Appliance (OVA) Files

Security Director Cloud Insights requires VMware ESXi server version 6.5 or later to support a virtual machine (VM) with the following configurations:

- 16 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.

To deploy and configure the Security Director Cloud Insights on-premises collector with OVA files, perform the following tasks:

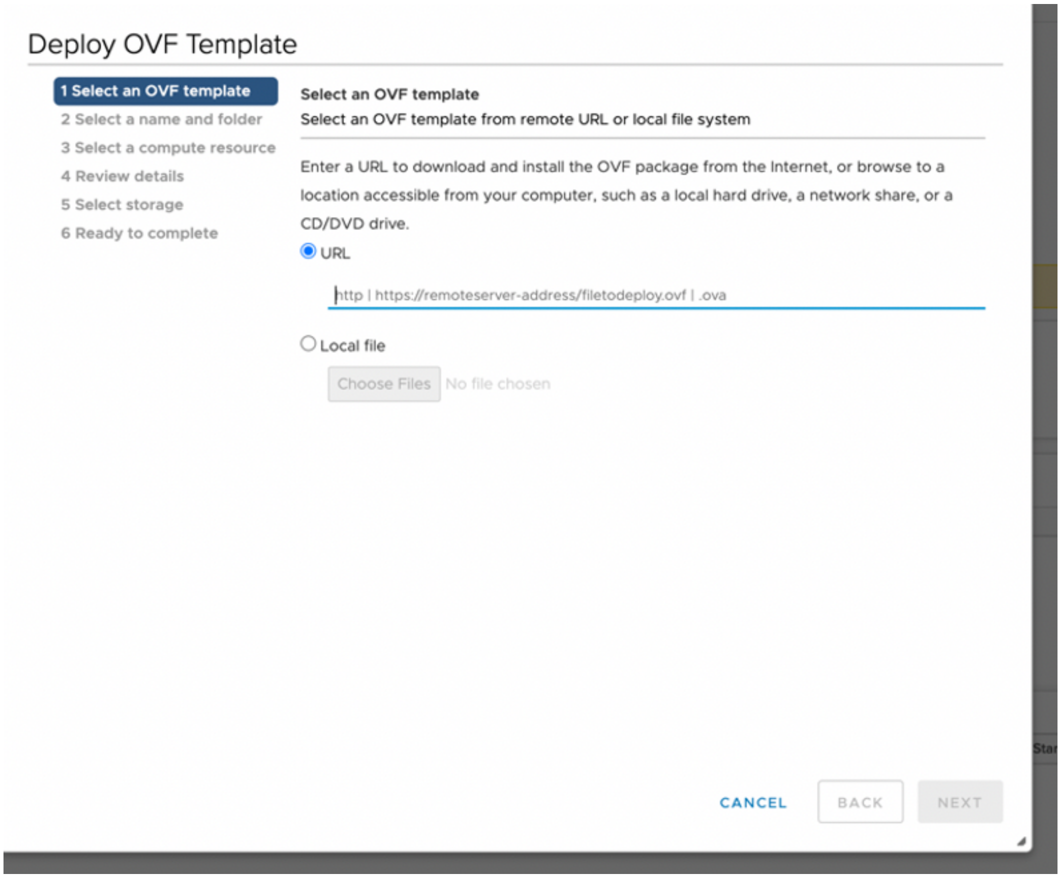
1. Download the Security Director Insights Cloud - Collector VM OVA image from the Juniper Networks software download page.

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

2. Launch the vSphere Client that is connected to the ESXi server, where the Security Director Cloud Insights VM is to be deployed.
3. Select **File** > **Deploy OVF Template**.

   The Deploy OVF Template page appears, as shown in Figure 2 on page 6.

Figure 2: Select an OVF Template Page



Deploy OVF Template

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

● URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

○ Local file

4. In the Select an OVF template page, 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 appears.

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

   The Select a compute resource page appears.

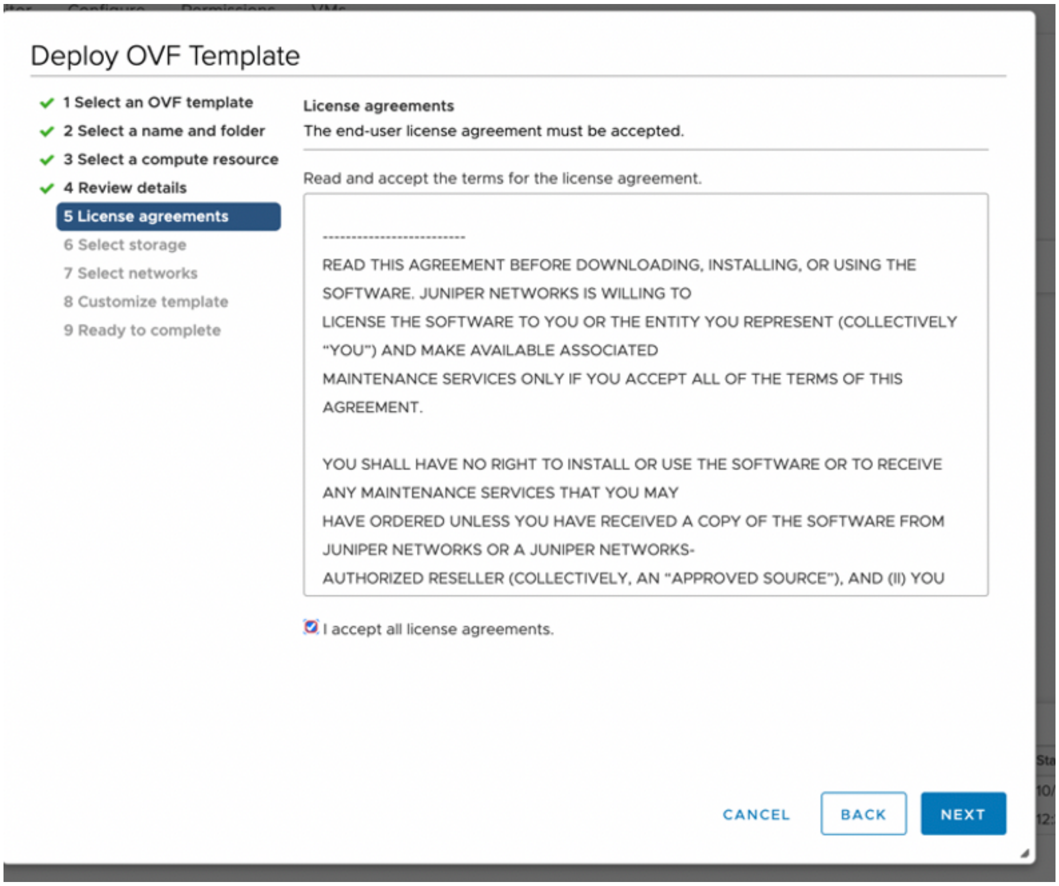
7. Select the destination compute resource for the VM, and click **Next**.

   The Review details page appears.

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

   The License agreements page appears, as shown in Figure 3 on page 7.

Figure 3: License Agreement Page



License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

READ THIS AGREEMENT BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. JUNIPER NETWORKS IS WILLING TO LICENSE THE SOFTWARE TO YOU OR THE ENTITY YOU REPRESENT (COLLECTIVELY "YOU") AND MAKE AVAILABLE ASSOCIATED MAINTENANCE SERVICES ONLY IF YOU ACCEPT ALL OF THE TERMS OF THIS AGREEMENT.

YOU SHALL HAVE NO RIGHT TO INSTALL OR USE THE SOFTWARE OR TO RECEIVE ANY MAINTENANCE SERVICES THAT YOU MAY HAVE ORDERED UNLESS YOU HAVE RECEIVED A COPY OF THE SOFTWARE FROM JUNIPER NETWORKS OR A JUNIPER NETWORKS-AUTHORIZED RESELLER (COLLECTIVELY, AN "APPROVED SOURCE"), AND (II) YOU

☑ I accept all license agreements.

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

   The Select storage page appears.

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 appears.

11. Select the network interfaces for the VM.

    Configure IP allocation for DHCP or Static addressing. We recommend using Static IP Allocation Policy.

    Click **Next**. The Customize template page appears. For DHCP instructions, see Step 13.

12. For IP allocation as Static, configure the following parameters for the VM:

    - IP address—Enter the Security Director Cloud Insights VM IP address.

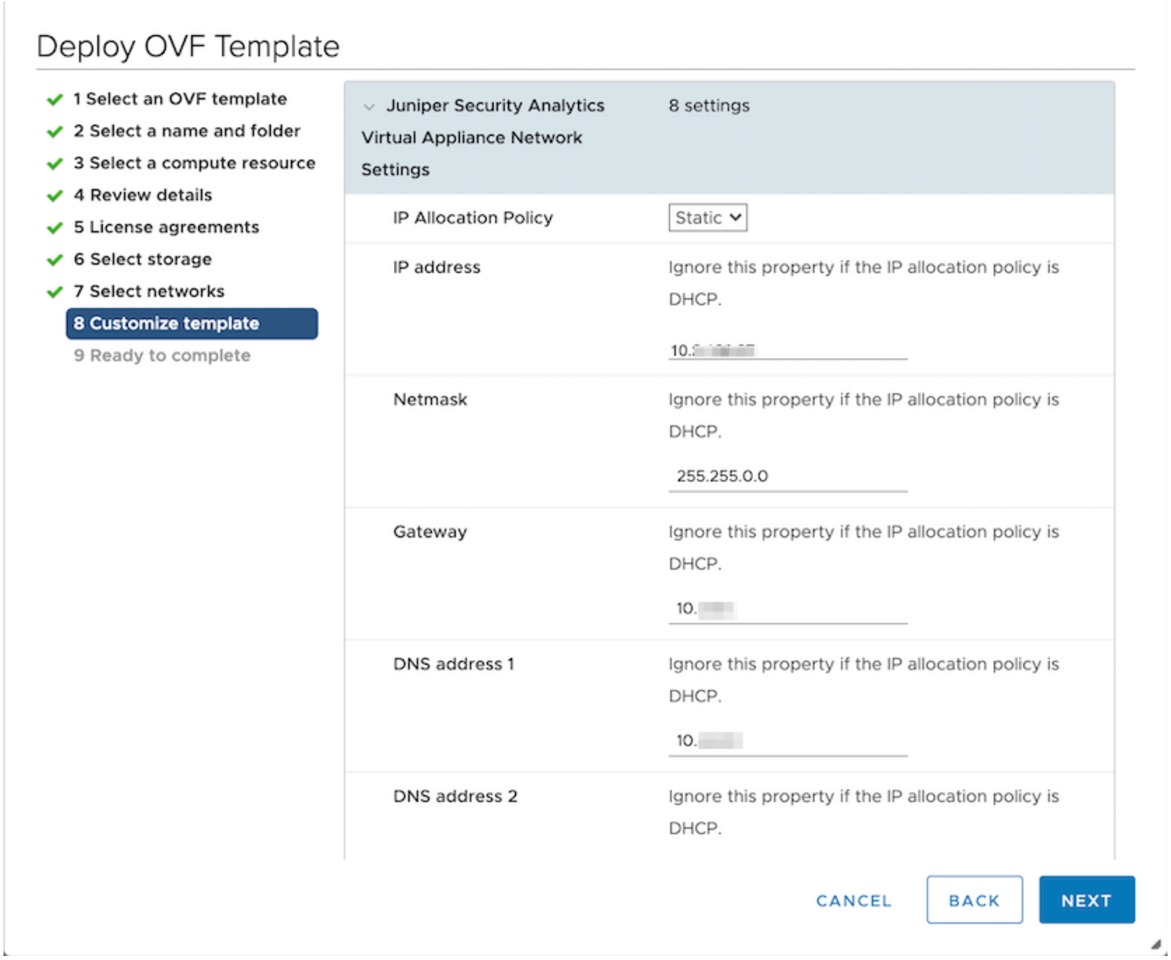
    - Netmask—Enter the netmask.

    - Gateway—Enter the gateway address.

    - DNS Address 1—Enter the primary DNS address.

- DNS Address 2—Enter the secondary DNS address.

Figure 4: Customize Template Page



Deploy OVF Template

Juniper Security Analytics Virtual Appliance Network Settings — 8 settings

IP Allocation Policy: Static

IP address: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

Netmask: Ignore this property if the IP allocation policy is DHCP.
255.255.0.0

Gateway: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

DNS address 1: Ignore this property if the IP allocation policy is DHCP.
10.[redacted]

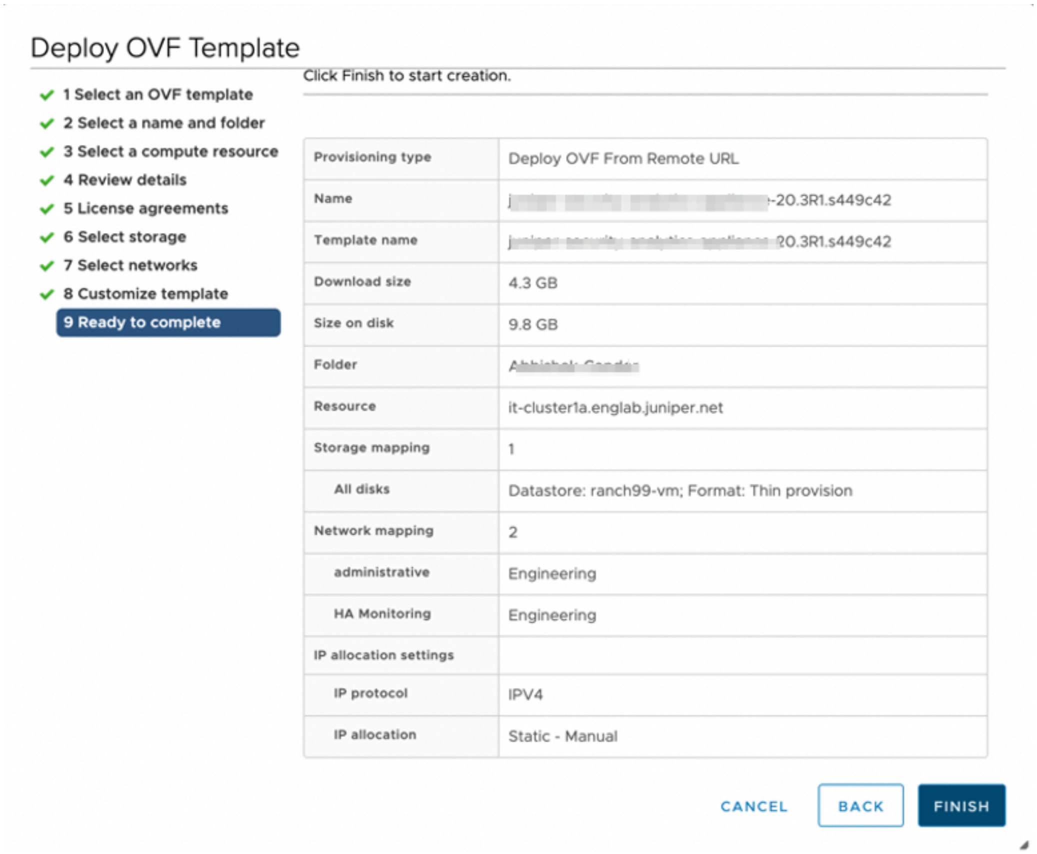
DNS address 2: Ignore this property if the IP allocation policy is DHCP.

13. For IP allocation as DHCP, enter the search domain, hostname, device name, and device description for the VM.

    We recommend this option only for the Proof of Concept type of short-term deployments. Do not use this option.

    Click **Next**. The Ready to complete page appears, as shown in Figure 5 on page 9.

Figure 5: Ready to Complete Page



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

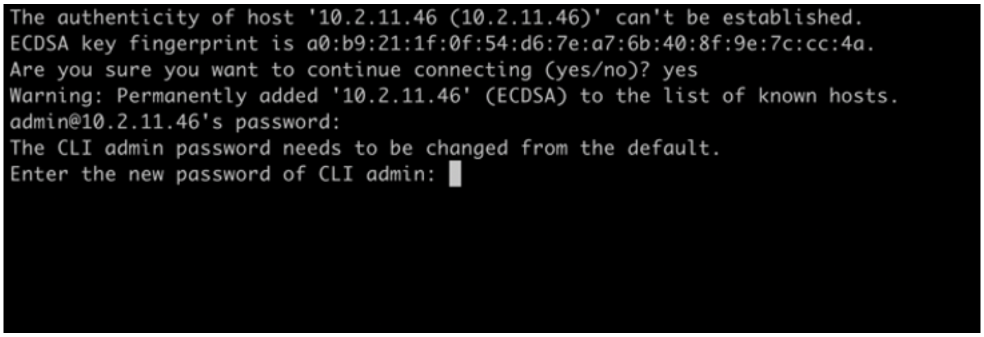
Click Finish to start creation.

Provisioning type	Deploy OVF From Remote URL
Name	j[redacted]-20.3R1.s449c42
Template name	[redacted]20.3R1.s449c42
Download size	4.3 GB
Size on disk	9.8 GB
Folder	[redacted]
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

14. Verify all the details and click **Finish** to begin the OVA installation.
15. After the OVA is installed successfully, power on the VM and wait for the boot-up to complete.
16. After 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, the system prompts you to change the default admin password. Enter a new password to change the default password, as shown in Figure 6 on page 9.

Figure 6: Default Admin Password Reset



```
The authenticity of host '10.2.11.46 (10.2.11.46)' can't be established.
ECDSA key fingerprint is a0:b9:21:1f:0f:54:d6:7e:a7:6b:40:8f:9e:7c:cc:4a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.2.11.46' (ECDSA) to the list of known hosts.
admin@10.2.11.46's password:
The CLI admin password needs to be changed from the default.
Enter the new password of CLI admin: █
```

17. Follow the wizard to configure the network details (hostname, connection and so on) on the cloud.

    After you deploy the Security Director Cloud Insights VM, if you want to change the tenant to which the on-premises collector is connected, then go to the CLI and run the sdic configure command.

    The format of the command is *sdic configure <username> <password> <realm>*.

The Security Director Cloud Insights on-premises collector deployment is now complete.