

Ruckus Wireless[™] SmartCell Insight[™] Installation Guide

Supporting SmartCell Insight[™] 3.6.0

Copyright Notice and Proprietary Information

Copyright © 2018 Ruckus Networks, an ARRIS company. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Ruckus Networks ("Ruckus"). Ruckus reserves the right to revise or change this content from time to time without obligation on the part of Ruckus to provide notification of such revision or change.

Destination Control Statement

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, RUCKUS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. Ruckus does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. Ruckus does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to Ruckus that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL RUCKUS, ARRIS, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIES, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF RUCKUS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS.

If you are dissatisfied with the Materials or with the associated terms of use, your sole and exclusive remedy is to discontinue their use.

Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

The Ruckus, Ruckus Wireless, Ruckus logo, Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, Xclaim, and ZoneFlex and trademarks are registered in the U.S. and other countries. Ruckus Networks, Dynamic PSK, MediaFlex, FlexMaster, Simply Better Wireless, SmartCast, SmartCell, SmartMesh, SpeedFlex, Unleashed, ZoneDirector and ZoneFlex are Ruckus trademarks worldwide. Other names and brands mentioned in these materials may be claimed as the property of others.

Wi-Fi Alliance®, Wi-Fi®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access® (WPA), the Wi-Fi Protected Setup logo, and WMM® are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance.

Contents

About This Document.....	7
Overview.....	7
Document Conventions.....	7
Related Documentation.....	8
Documentation Feedback.....	8
Before You Begin.....	9
System Requirements.....	9
Minimum Hardware Requirements.....	9
Guidelines for Setting Up Data Nodes.....	10
Requirements.....	11
Bandwidth Requirements.....	11
Minimum Software Requirements.....	11
DHCP Server Requirements.....	11
NTP Server Requirements.....	12
Compatibility Matrix.....	13
Compatibility Matrix.....	13
Installing SCI.....	15
Installation Overview.....	15
Setting Up the Virtual Machine Using VMware ESXi.....	16
Setting Up the Virtual Machine Using AWS.....	18
Setting Up the Virtual Machine Using a Static IP Address.....	20
Setting Up the Virtual Machine Using KVM QCOW2	23
Setting Up the Virtual Machine Using GCE.....	24
Installing the Azure VM Image.....	25
Installing the Hyper-V VM Image.....	25
Setting Up the Nodes.....	29
Firewall Rules.....	31
Installing Custom SSL Certificate.....	32
Secure Shell Access to SCI.....	32
Configuring SMTP.....	35
SMTP Overview.....	35
SMTP Configuration Steps.....	36
Sending a Test Email.....	37
Adding Controllers to Both the SCI and Controller User Interfaces.....	39
Overview of Adding Controllers to SCI.....	39
Adding a SmartZone Controller Version 3.5 or Greater.....	40
Adding a SmartZone Version 3.5 or Later in the SCI User Interface.....	40
Configuring SmartZone Version 3.5 or Later to Send Data to SCI	42
Adding a SmartZone Controller Version Prior to 3.5.....	42
Adding a SmartZone Version Prior to 3.5 on the SCI UI.....	42
Configuring SmartZone Version Prior to 3.5 to Send Data to SCI	43
Enabling AP SCI Statistics Delivery on SmartZone 3.4 Controllers.....	44
Enabling AP SCI Statistics Delivery on SmartZone 3.2 Controllers.....	45
Adding a Zone Director Controller: Push Method.....	46

Adding Zone Director (Push Method) on the SCI UI.....	46
Configuring Zone Director (Push Method) to Send Data to SCI.....	47
Adding a Zone Director Controller: Poll Method.....	48
Adding Zone Director (Poll Method) on the SCI UI.....	48
Configuring Zone Director (Poll Method) to Send Data to SCI.....	49
Important Setting on the ZoneDirector UI.....	50
Editing Controllers in the SCI User Interface.....	50
Updating the SCI Software.....	53
Updating the Software from the Cloud.....	53
Updating the Software Package by Downloading it.....	53
Managing Licenses.....	55
Trial License.....	55
Upgrading to the SCI License.....	55
Migration from SCI 1.x.....	57
Prerequisites.....	57
Migration Procedure.....	58
Monitor the Migration Process.....	59

About This Document

- Overview..... 7
- Document Conventions..... 7
- Related Documentation..... 8
- Documentation Feedback..... 8

Overview

This *SmartCell Insight Installation Guide* provides instructions for installing and the initial setup of the Ruckus Wireless™ SmartCell Insight (SCI) application.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Wi-Fi networks. It assumes basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE

Refer to the release notes shipped with your product to be aware of certain challenges when upgrading to this release.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at <https://support.ruckuswireless.com/contact-us>.



Document Conventions

[Document Conventions](#) and [Document Conventions](#) list the text and notice conventions that are used throughout this guide.

TABLE 1 Text conventions

Convention	Description	Example
message phrase	Represents messages displayed in response to a command or a status	[Device Name] >
user input	Represents information that you enter	[Device Name] > set ipaddr 10.0.0.12
user interface controls	Keyboard keys, software buttons, and field names	Click Create New
Start > All Programs	Represents a series of commands, or menus and submenus	Select Start > All Programs
ctrl+V	Represents keyboard keys pressed in combination	Press ctrl+V to paste the text from the clipboard.
screen or page names		Click Advanced Settings . The Advanced Settings page appears.
command name	Represents CLI commands	
parameter name	Represents a parameter in a CLI command or UI feature	
variable name	Represents variable data	{ZoneDirectorID}
filepath	Represents file names or URI strings	http://ruckuswireless.com

TABLE 2 Notice conventions

Notice type	Description
NOTE	Information that describes important features or instructions
 CAUTION	Information that alerts you to potential loss of data or potential damage to an application, system, or device
 WARNING	Information that alerts you to potential personal injury

Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus Wireless at: docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

Before You Begin

- System Requirements..... 9
- DHCP Server Requirements..... 11
- NTP Server Requirements..... 12

SmartCell Insight (SCI) is a massively scalable reporting and analytics engine, designed to collect data from Ruckus network equipment, analyze that data, and then present it using a wide variety of standard and custom reports.

System Requirements

You must be aware of the minimum hardware and software requirements to run SCI.

Minimum Hardware Requirements

To run SCI effectively, you must ensure that the installation environment meets the minimum hardware requirements.

The SCI cluster consists of a Master node or one or many Data nodes. Alternatively, for demo or testing purposes, you can set up SCI as a single Demo node. The cluster can be fully functional with just the Master node. The Data node is optional, as it only helps to scale the processing power and storage capacity of the cluster. The Demo node is a standalone node which cannot be used in a cluster with a Master node or Data node.

The Demo node must only be used for demo or testing purposes. This node has scaling and performance limitations and **should not** be used in a production environment. The Demo node can only support up to 200 APs.

NOTE

To avoid system-performance issues, do not allocate more CPUs than recommended in the following tables.

Following are the minimum hardware requirements for the Master node in the SCI cluster:

TABLE 3 Minimum Hardware Requirements - Master Node

Requirement	Quantity
Number of vCPUs	8
Memory	32 GB
Root HDD (SCSI)	80 GB
Secondary HDD (SCSI)	500 GB

Following are the minimum hardware requirements for the Data node in the SCI cluster:

TABLE 4 Minimum Hardware Requirements - Data Node

Requirement	Quantity
Number of vCPUs	4
Memory	20 GB
Root HDD (SCSI)	80 GB
Secondary HDD (SCSI)	500 GB

Before You Begin

System Requirements

Following are the minimum hardware requirements for the Demo node in the SCI cluster:

TABLE 5 Minimum Hardware Requirements - Demo Node

Requirement	Quantity
Number of vCPUs	4
Memory	16 GB
Root HDD (SCSI)	80 GB
Secondary HDD (SCSI)	100 GB

Guidelines for Setting Up Data Nodes

The controllers that communicate with the SCI cluster can have a number of APs. The amount of data traffic that the cluster must handle depends on the number of APs in the controller. Therefore, you must setup the right number of Data nodes on the cluster to handle the AP traffic.

Following are guidelines to setup Data nodes within the cluster, based on the number of APs in the controller:

TABLE 6 General Guidelines for Hardware Requirements (No. of APs)

Number of Data Nodes	ZD	SZ version 3.4 or earlier <i>or</i> SZ version 3.5 or later with 15-minute granularity	SZ version 3.5 or later with 3-minute granularity
0	3,000	3,000	1,000
1	10,000	10,000	3,000
2	20,000	20,000	6,000
3	30,000	30,000	9,000
4	40,000	40,000	12,000

NOTE

For SmartZone 3.4 or earlier or SmartZone 3.5 or later with 15-minute granularity, add an additional Data node for every additional 10,000 APs. For SmartZone 3.5 or later with three-minute granularity, add an additional Data node for every additional 3,000 APs.

NOTE

Data granularity was increased to three minutes in the SmartZone 3.5 release, depending on the data set. This increased data granularity and new set of data require more processing power and hard disk space. These changes necessitated changes to the number of data nodes needed and scalability of the system.

NOTE

This table is only a guideline and the actual hardware requirements would depend on various factors such as the number of clients, the number of sessions, and the type of server hardware.

Requirements

You must be aware of the storage capacity requirements for each node in order to handle the maximum data traffic per day, for every 1,000 APs.

TABLE 7 Storage Requirements

Storage Requirements	ZD	SZ version 3.4 or earlier, or SZ 3.5 or later with 15-minute granularity	SZ version 3.5 or later with 3-minute granularity
Per day per 1,000 APs	1 GB	1 GB	3 GB

To reduce the resource requirements in SmartZone 3.5 or later by increasing the data granularity to 15 minutes, run the following command in the SmartZone CLI:

```
ap-config-routine-status-interval slowdown
```

Bandwidth Requirements

You should be aware of the bandwidth requirements provided in the following table.

TABLE 8 Bandwidth Requirements

Bandwidth Requirements	ZD	SZ version 3.4 or earlier or SZ version 3.5 or later with 15-minute granularity	SZ version 3.5 or later with 3-minute granularity
Per AP	15 kb per 15 minutes	15 kb per 15 minutes	15 kb per 3 minutes

Minimum Software Requirements

The minimum required virtualization software version is VMware ESXi 5.0 or above.

DHCP Server Requirements

Before the SCI cluster installation, ensure that a static IP address is available to the Master node, Data node and Demo node. A DHCP server must be available to issue an IP address to the SCI virtual machine (VM).

NOTE

The IP address that is assigned to the nodes must be accessible.

To setup a VMware environment, the networking layer of VMware is used, which includes its own virtual routers and the DHCP server. Therefore, a dedicated DHCP server is not necessary.

NOTE

The IP addresses assigned to SCI VMs must not change throughout the lifetime of the deployment.

If you cannot assign an IP address through the VMware or DHCP, see [Setting Up the Virtual Machine Using a Static IP Address](#) on page 20 for more information.

NTP Server Requirements

SCI must keep the correct time in order to report accurate statistics.

As an analytics system, SCI must make sure that all its statistics are reported with the correct time. Therefore, you must ensure that NTP servers are reachable by all elements of the ecosystem: APs, SZ's, ZoneDirectors, and SCI.

NOTE

In addition to ensuring access to an NTP server, you must also ensure that the time and date are correct. If you change the time after SCI is installed, it will cause serious issues within the SCI system. For example, when APs reboot, they would lose all measurements and aggregated statistics as the AP re-initializes its real-time clock through the NTP server.

Ensure that the system time is correct on the SCI VM and on the host. **Please do not change the timezone on the SCI VMs. SCI expects the VM to keep UTC time. Changing to a timezone other than UTC on the SCI VM can cause SCI to stop working.**

If the SCI VM is unable to access the internet for NTP updates, it must be configured with a local NTP server. Modify the chrony configuration file at `/etc/chrony.conf` with the NTP server information.

For more information about using SSH to connect to SCI, see [Secure Shell Access to SCI](#) on page 32

Login to the SCI VM (master and data nodes) and add the following line to the chrony configuration file `sudo vi /etc/chrony.conf` .

```
server <ntp-server-ip> prefer
```

After editing the NTP server information, it is recommended that you reboot your system so that the time can correct itself immediately.

```
sudo reboot
```

Follow the same steps to update NTP server information for the Demo node.

Compatibility Matrix

- Compatibility Matrix..... 13

Compatibility Matrix

The following is the compatibility matrix between SCI and the SmartZone and ZoneDirector controllers.

TABLE 9 Compatibility Matrix

SCI Release	SmartZone (controller) Release		ZoneDirector (controller) Release
Version	Version 3.4 or lower	Version 3.5 or higher	<ul style="list-style-type: none">• Branch 9.5.3.0, build 45 and above• All branches starting from 9.7.0.0 and above
1.x	Yes	No	Yes
2.x (Up to 2.4)	Yes	No	Yes
2.5 and above	Yes	Yes	Yes

If you have a ZoneDirector 9.13 or lower version, the only option available to bring data into SCI is the polling mechanism, meaning that once the ZoneDirector is added to SCI, SCI regularly polls the ZoneDirector for data.

If you have Zone Director version 9.13 - MR1 or higher, version, you can choose the polling option or the ZoneDirector push mechanism, meaning that ZoneDirector will push data to the SCI.

Ensure that you use only one of the methods (poll or push) to avoid duplicate data.

NOTE

The ZoneDirector "push" model usually does not require firewall changes, whereas the "pull" model may need firewall changes.

Installing SCI

- Installation Overview..... 15
- Setting Up the Virtual Machine Using VMware ESXi..... 16
- Setting Up the Virtual Machine Using AWS..... 18
- Setting Up the Virtual Machine Using a Static IP Address..... 20
- Setting Up the Virtual Machine Using KVM QCOW2 23
- Setting Up the Virtual Machine Using GCE..... 24
- Installing the Azure VM Image..... 25
- Installing the Hyper-V VM Image..... 25
- Setting Up the Nodes..... 29
- Secure Shell Access to SCI..... 32

SCI can be installed as a virtualized cluster using VMware's vSphere Web Client, KVM or Amazon Web Services (AWS). The cluster is made up of Master and Data nodes as virtual machines (VMs).

Installation Overview

You must install SCI as a VM cluster. Setup and activate the Master nodes and Data node(s) (optional) within the cluster after installation is complete.

Ensure that you have identified an IP address for the Master and Data nodes that you are about to create (VMs).

NOTE

IPv6 is currently not supported, therefore IP addressing must only be in the IPv4 format.



WARNING

- Ensure that uninterrupted power supply is available for SCI. Abnormal shutdowns due to power outage may cause file system corruption and could disrupt SCI operation after restart.
- Do not power off the SCI instance during or after setup as this could corrupt the file system and disrupt SCI operation after reboot. If you want to restart the system, you must perform a "sudo reboot" from the CLI.
- Do not "yum update" on the SCI instances.

NOTE

Ensure that the VM is setup based on the hardware specifications available at [Minimum Hardware Requirements](#) on page 9. In addition, ensure that there is provision for a secondary data volume (must be a unformatted disk) hard disk drive as well.

NOTE

This document assumes that the reader has working knowledge of VMware ESXi and/or AWS.

The following steps outline the installation process:

1. Create a VM for the Master node.

For more information about how to setup the VM, see [Setting Up the Virtual Machine Using VMware ESXi](#) on page 16 or [Setting Up the Virtual Machine Using AWS](#) on page 18.

Installing SCI

Setting Up the Virtual Machine Using VMware ESXi

2. Create a VM for the Data node.

For more information about how to setup the VM, see [Setting Up the Virtual Machine Using VMware ESXi](#) on page 16 or [Setting Up the Virtual Machine Using AWS](#) on page 18.

After the VMs are created, an IP address must be assigned to them.

NOTE

Ensure that you indicate the IP address to VMware ESXi or the VM manager software when starting up the VM. The network stack on the running VM is automatically set to get an IP address from the DHCP server, but it expects the DHCP server to always assign it the same IP address during its lifetime.

NOTE

Ensure that the IP address is accessible to the nodes within the SCI cluster.

3. Set up the Master node.

For more information, see [Setting Up the Nodes](#) on page 29.

4. Activate the Master node.

For more information, see [Setting Up the Nodes](#) on page 29.

5. Set up the Data node.

For more information, see [Setting Up the Nodes](#) on page 29.

6. Activate the Data node.

7. Enter the login credentials to access the web UI.

You will see the Master and Data nodes you created in the **Admin > Status & Update** page.

8. Configure the controllers that you want to add to the cluster.

This completes the SCI installation as a VM.

Setting Up the Virtual Machine Using VMware ESXi

VMware ESXi is an enterprise-class hypervisor used for deploying and serving virtual computers.

Follow these steps to install and configure the VM:

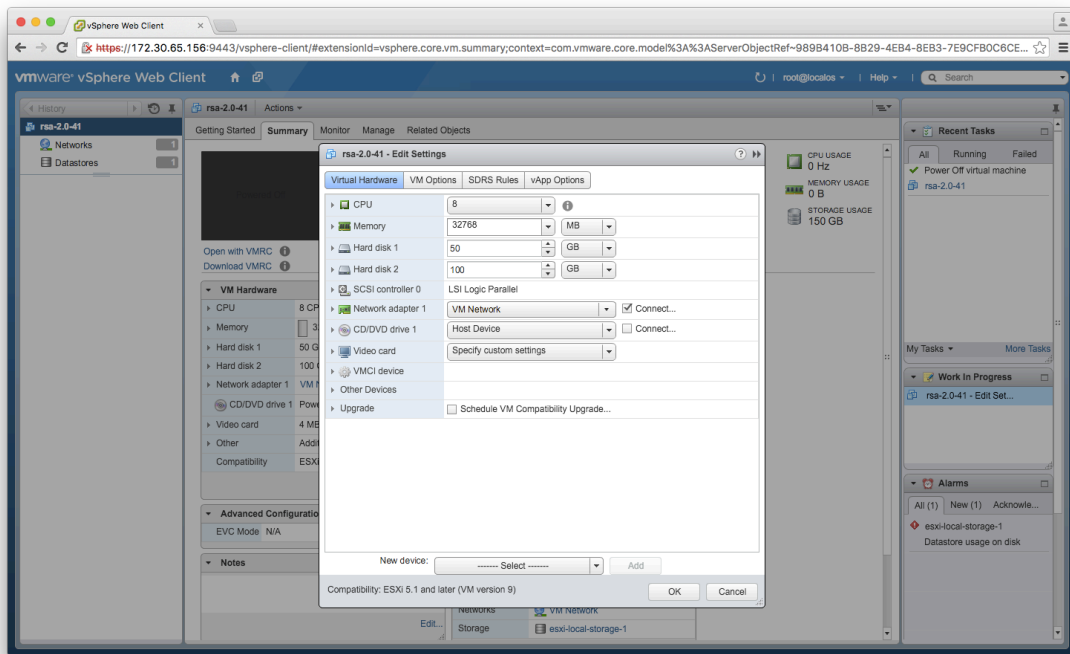
1. Download the VMware ESXi software and ensure that it is running on a suitable server with proper network configuration.

- From the VMware vSphere Web Client, set up and configure the VM.

NOTE

Ensure that the VM is setup based on the hardware specifications available at [Minimum Hardware Requirements](#) on page 9.

FIGURE 1 VMware vSphere Web Client



NOTE

The OVA file does not specify the minimum hardware requirements. Therefore, ensure that the hardware requirements are configured correctly.

NOTE

Ensure that the root and data volumes are set up as the **first** and **second** SCSI devices respectively, on the first SCSI controller of the VM, in order to be detected correctly.

NOTE

The network stack on the VM is automatically set to get an IP address from the DHCP server, but the VM always expects the DHCP server to assign the same IP address during its lifetime. Therefore, provision the VM with a **fixed** IPv4 address. The VMware vSphere Web Client requires this information when the VM is started.

If DHCP is not available, it is possible to set up the VM using a static IP address. See [Setting Up the Virtual Machine Using a Static IP Address](#) on page 20 for more information.

Installing SCI Setting Up the Virtual Machine Using AWS

- From the VMware vSphere Web Client, start the VM.

It could take up to 30 minutes for the VM to boot, depending on the VM resources.

You can press the **Esc** key when the VM is booting, to view the boot logs and troubleshoot failures, if any.

NOTE

You can use the same VM image to provision a Master node, Data node or a Demo node.

Setting Up the Virtual Machine Using AWS

Amazon Elastic Compute Cloud (Amazon EC2) is an Amazon Web Services (AWS) that allows you to create and run virtual machines in the cloud.

Contact Ruckus Wireless customer support and provide your AWS account ID, so that the company can share the SCI private AMI (Amazon Machine Image) number with you. For more information regarding AWS accounts IDs, see <http://docs.aws.amazon.com/general/latest/gr/acct-identifiers.html>.

Follow these steps to install and configure the VM:

- Based on the instructions in <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingsharedamis-finding.html>, find the AMI and launch a VM instance.
- Choose the type of instance you want to create. A good example is **m4.2xlarge**.

NOTE

The AMI will be located in **US West (Oregon)**.

FIGURE 2 Choosing the type of instance

The screenshot shows the AWS Management Console interface for selecting an instance type. The page title is 'Step 2: Choose an Instance Type'. Below the title, it says 'Currently selected: m4.2xlarge (26 ECUs, 8 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 32 GiB memory, EBS only)'. A table lists various instance types with columns for Family, Type, vCPUs, Memory (GiB), Instance Storage (GB), EBS-Optimized Available, and Network Performance. The 'm4.2xlarge' instance type is highlighted with a blue selection bar. At the bottom of the table, there are buttons for 'Cancel', 'Previous', 'Review and Launch', and 'Next: Configure Instance Details'.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High
<input checked="" type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
<input type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate

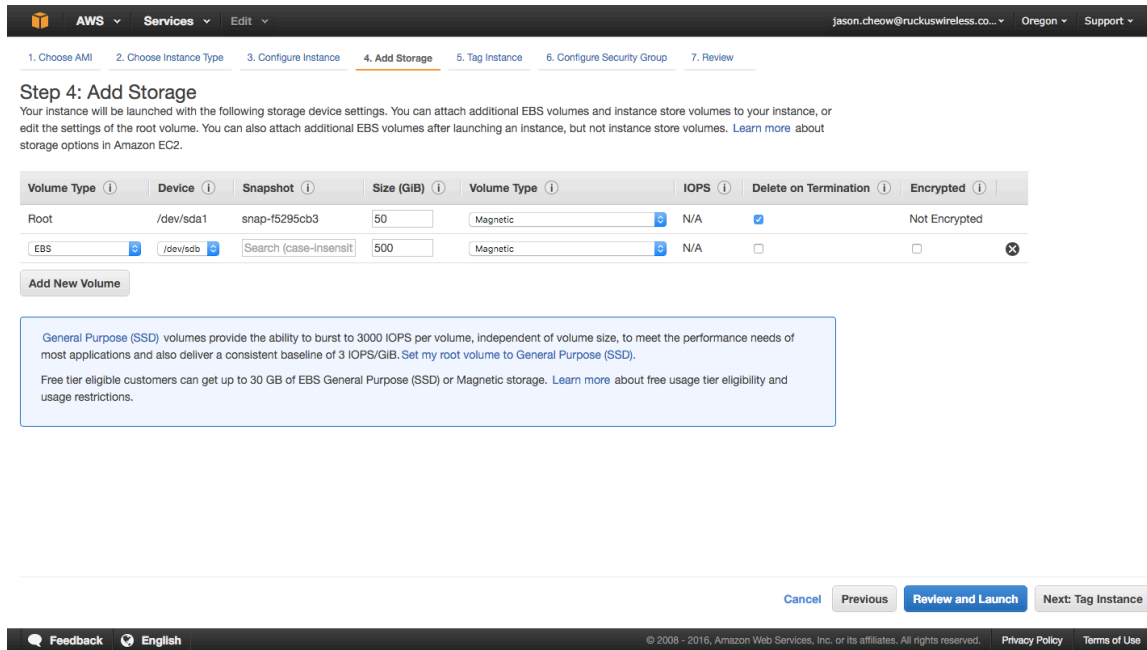
- Configure the instance you have chosen based on your requirements.

4. Add storage to the instance.

Following are the minimum requirements to configure the instance:

- Hard disk 1 (Root volume): 50 GB
- Hard disk 2 (Data volume): 500 GB (choose `/dev/sdb` for **Device**).

FIGURE 3 Adding storage to the instance



5. Tag the instance to manage it.
6. Configure the security group so that traffic to and from the instance is secure.
Review the instance and ensure all the configuration details are final.
7. Launch the instance.
It could take up to 30 minutes for the instance to boot.

You have successfully created a VM instance.

Setting Up the Virtual Machine Using a Static IP Address

If you are unable to use DHCP, you can use a static IP address for the VM.

NOTE

The static IP can be set only when you set up a VM. Once the VM is set up, there is no option to change the IP address.

1. From the console, power on the instance (or reboot).

The following screen appears.

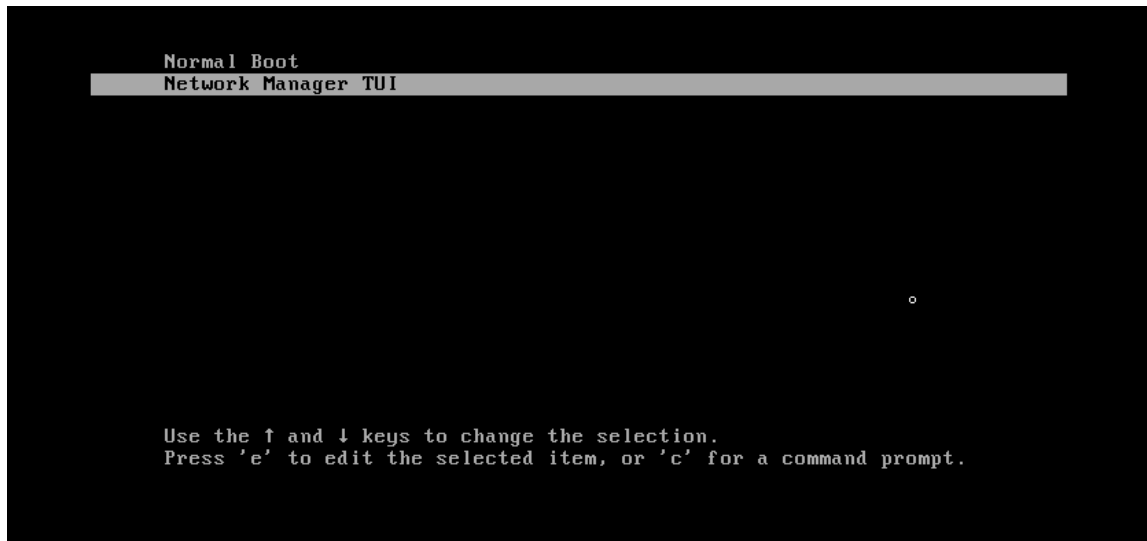


IMPORTANT

If you power on the machine, you will only have 10 seconds to open the console before the screen on the next page disappears. Therefore, it is recommended that you edit your VM boot options to *boot to BIOS*, and then exit the BIOS screen and select your option from the menu on the next page.

If you enable *boot to BIOS*, ensure you turn it off after you set the static IP address, otherwise SCI automatically boots after a power outage.

FIGURE 4 Console



Select **Network Manager TUI** to set the static IP address, and **Normal Boot** to start SCI.

2. Select **Network Manager TUI**.

The **Network Manager TUI** screen appears.

FIGURE 5 Network Manager TUI screen

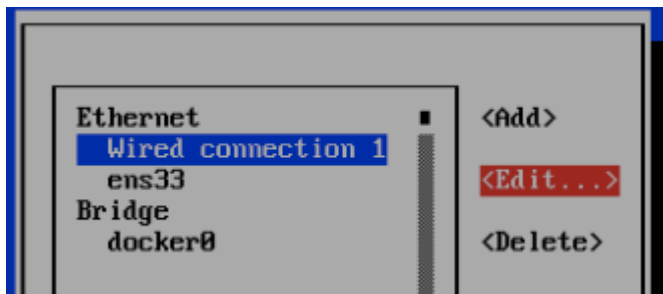


3. Select **Edit a connection**.

4. Press **Enter**.

The following screen appears.

FIGURE 6 Selecting a wired connection



5. Select **Wired Connection 1**, or the default wired connection.

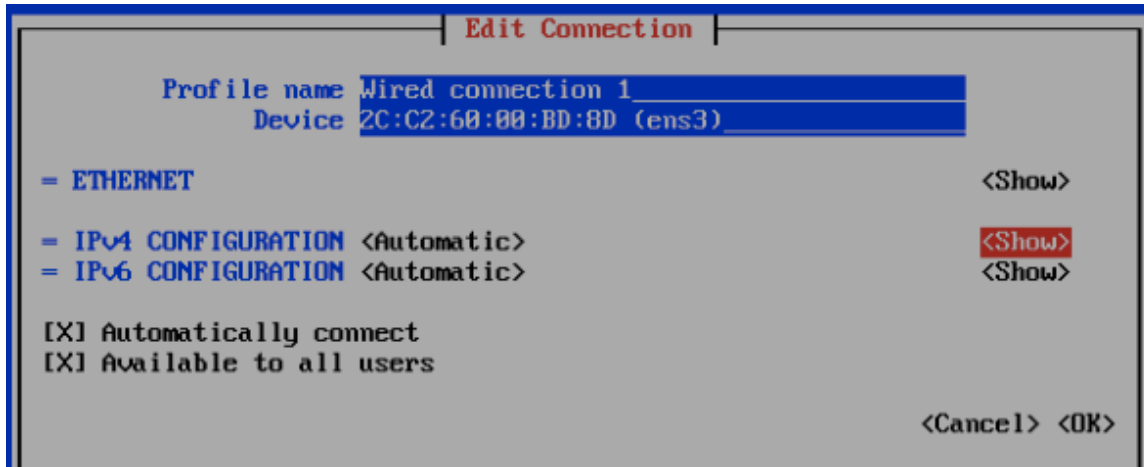
Installing SCI

Setting Up the Virtual Machine Using a Static IP Address

6. Select **Edit**.

The **Edit Connection** screen is displayed.

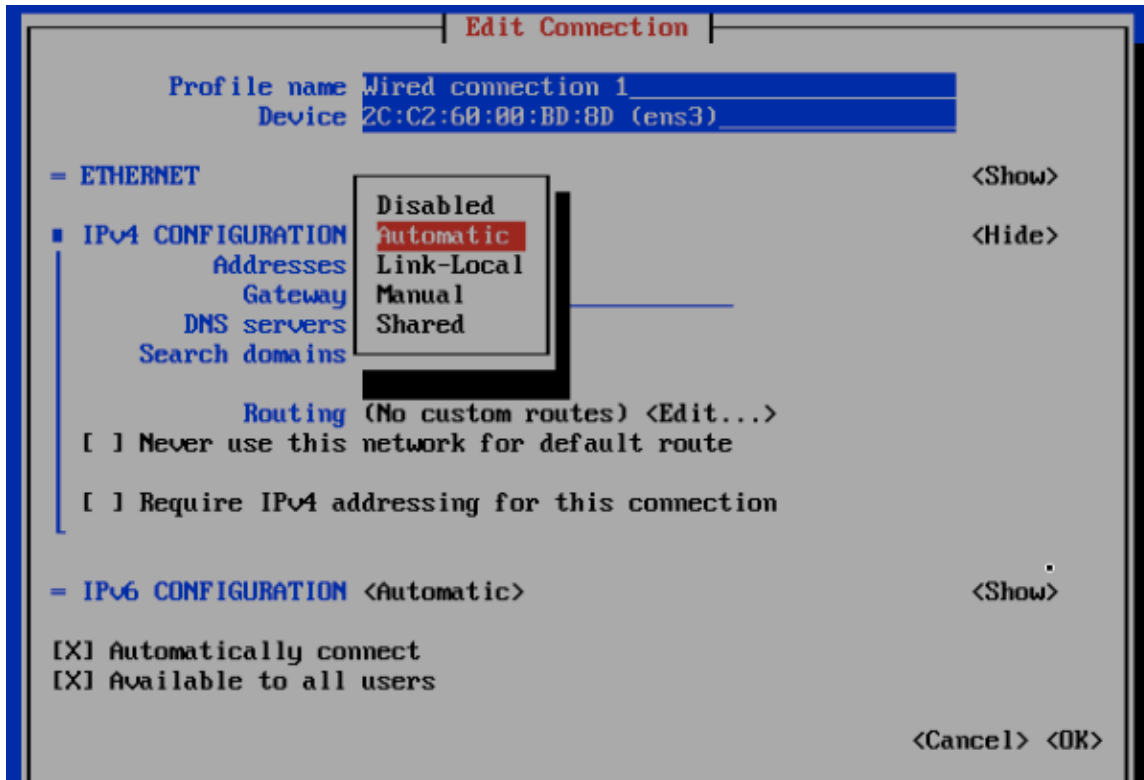
FIGURE 7 Edit connection



7. Select **Show** against the IPv4 configuration.

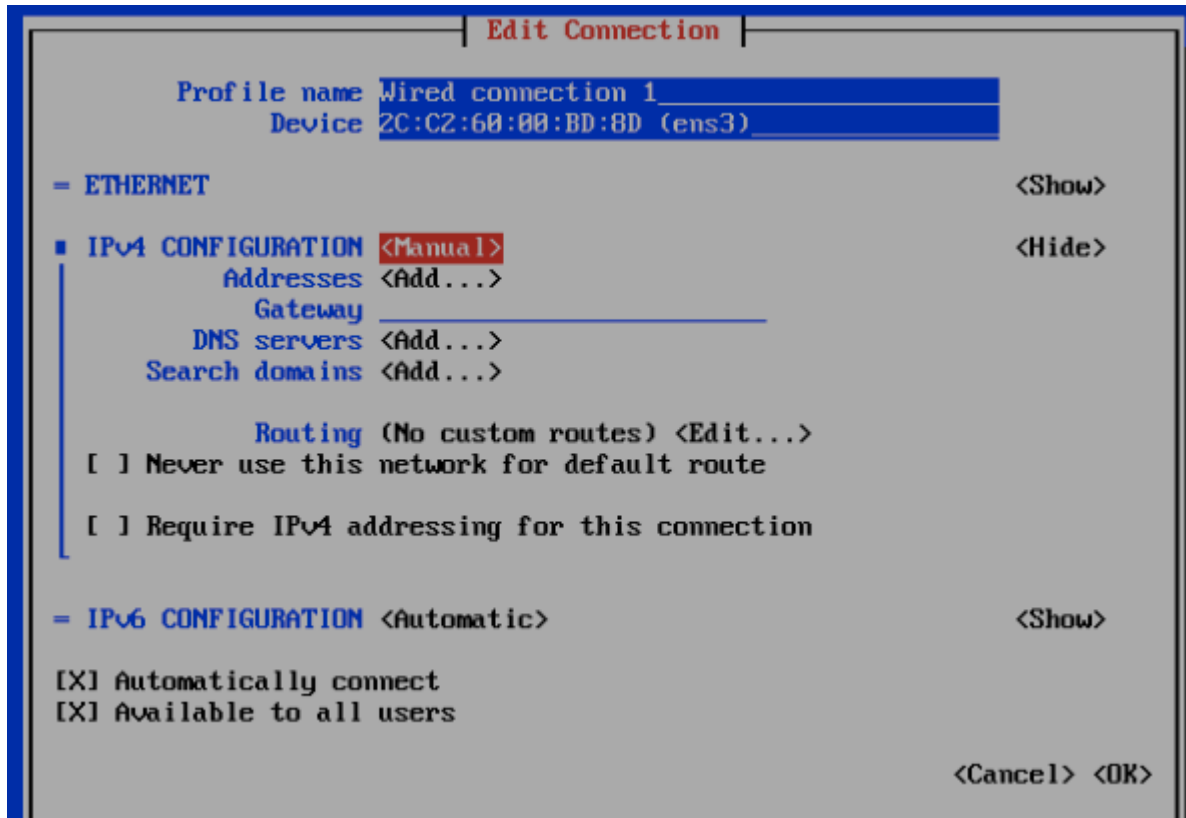
The following screen appears.

FIGURE 8 Changing the connection



8. Change the connection type for the IPv4 Address to **Manual**.

FIGURE 9 Manual IPv4 connection selected



NOTE

If you enabled “boot to bios”, you must turn that off after configuring the static IP address.

9. Fill up all the required details as per the network environment and select **OK**.
10. Select **OK**.

This should reboot the instance and continue to **Normal Boot**.

Setting Up the Virtual Machine Using KVM QCOW2

Kernel-based Virtual Machine (KVM) is an open source virtualization infrastructure that can run Linux and Windows in a virtual machine.

NOTE

The following instructions assume that KVM is installed and set up properly. Installing, setting up and using KVM is beyond the scope of this guide.

Ensure the KVM host is running on a suitable server with proper network configuration.

You must have a KVM virtualization environment that is suitably installed and configured before you can start a guest VM from a provided QCOW2 image.

Installing SCl

Setting Up the Virtual Machine Using GCE

Before you start and stop a RSA VM ensure that:

- The CPU, HDD and memory requirements under the [Minimum Hardware Requirements](#) on page 9 are met.
 - Both Root and Data volumes are set up as SCSI hard disk drives (not IDE). If you receive an error message such as "boot device not found" or similar while starting the VM, it's probably because the hard disk drives have not been set up as SCSI devices.
1. The instructions here have been verified to work on a plain-vanilla CentOS 7 installation, using distro provided command line based libvirt tools (virsh and virt-install) and distro supplied default settings. Please refer to the *Virtulazation Deployment and Administration Guide* at https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/, for useful reference on how to install KVM on RedHat/CentOS 7. Install the necessary libvirt packages and start the libvirtd service:

1.

```
sudo yum -y install bridge-utils libvirt qemu-img qemu-kvm virt-install
```
2.

```
sudo systemctl start libvirtd
```
3.

```
sudo systemctl enable libvirtd
```

2. Download and unpack the RSA QCOW2 VM image, and place the `rsa.qcow2` file in the standard libvirt image library directory: `/var/lib/libvirt/images`. Run the following command to install and start the RSA VM:

```
sudo virt-install --name rsa --vcpus 8 --ram 32768 --controller type=scsi,model=virtio-scsi --disk /var/lib/libvirt/images/rsa.qcow2,bus=scsi,size=80 --import --disk size=500,bus=scsi --graphics vnc --noautoconsole --network bridge=br0
```

3. Adjust the CPU, memory and disk parameters as necessary while meeting the requirements under the [Minimum Hardware Requirements](#) on page 9.

Depending on your network topology, you may or may not need a to use a bridge. This example uses a network bridge called "br0".

Adjust the name of the network bridge device to match the one on your system. On most systems, this is called "br0" or "virbr0". The bridge is used to facilitate network communication between the host VM and the guest VM.

4. Once the guest VM is installed, run the following **virsh** command to start, terminate or monitor the VM (assuming it is named `rsa`):

1.

```
sudo virsh list
```
2.

```
sudo virsh start rsa
```
3.

```
sudo virsh shutdown rsa
```

5. Use a suitable VNC viewer to access the console. Run the following command to obtain the VNC connection number to use:

```
sudo virsh vncdisplay rsa
```

Setting Up the Virtual Machine Using GCE

You can set up a virtual machine using the Google Compute Engine (GCE).

Follow these steps to setup the VM:

1. Contact Ruckus Wireless support for the RSA GCE VM image. You will receive this URL for the VM image in addition to the necessary launch permission: <https://www.googleapis.com/compute/v1/projects/ruckusgdc-rsa-builder/global/images/rsa-v2-3-0-1>
2. Use Google Cloud SDK to create the RSA VM instance running the RSA VM image. Refer to <https://cloud.google.com/sdk/> for instructions on how to install and use the SDK.

3. Create a suitable storage disk by running the following command `gcloud compute disks create my-rsa-instance-storage --project my-project --size 1TB --type pd-standard --zone us-central1-a`. This disk is used as the VM instance's data storage volume.
4. Enter the `gcloud compute instances create my-rsa-instance --disk name=my-rsa-instance-storage --image https://www.googleapis.com/compute/v1/projects/ruckusgdc-rsa-builder/global/images/rsa-v2-3-0-1 --machine-type n1-highmem-8 --project my-project --zone us-central1-a` command to create the VM instance using the disk you created in the previous step.
5. Configure firewall rules for the network and ensure that the VM has access to the required inbound and outbound ports.

Installing the Azure VM Image

Follow these steps to install the Azure VM image for SCI.

1. Sign-in to your account at <https://portal.azure.com>
2. Contact Ruckus Support to obtain access to the RSA Azure VM image. You will be provided with the URL for the VM image in the following format:

```
https://abc.s3.amazonaws.com/packages/file/rsa-v3-6-0-beta-1-vhd-31636606.zip?  
AWSAccessKeyId=ABCD&Expires=154641111&Signature=ABCD%3D
```

3. Provide a username. Make sure that you do not use *rsa* or *root* as the user name. Any other name is ok.
4. Select a VM size (master is 8 CPUs and 32 GB RAM; data is 4 CPUs and 20 GB RAM).
 - Ensure the VM is set up with the specifications listed in [Minimum Hardware Requirements](#) on page 9.
 - vCPUs: 8
 - Memory: 32 GB
 - Hard disk 1 (Root volume): 80 GB
 - Hard disk 2 (Data volume): 500 GB
 - The root and data volumes need to be set up as the first and second SCSI devices, respectively, on the first SCSI controller of the VM, to be detected.
5. Set network firewall rules to ensure that the VM instance has access to the required inbound and outbound ports.
6. In the newly created VM page, go to "Disks" (the page may not appear immediately).
7. Create a data disk.
8. Continue with the setup.

Installing the Hyper-V VM Image

Follow these steps to install the Hyper-V VM Image for SCI.

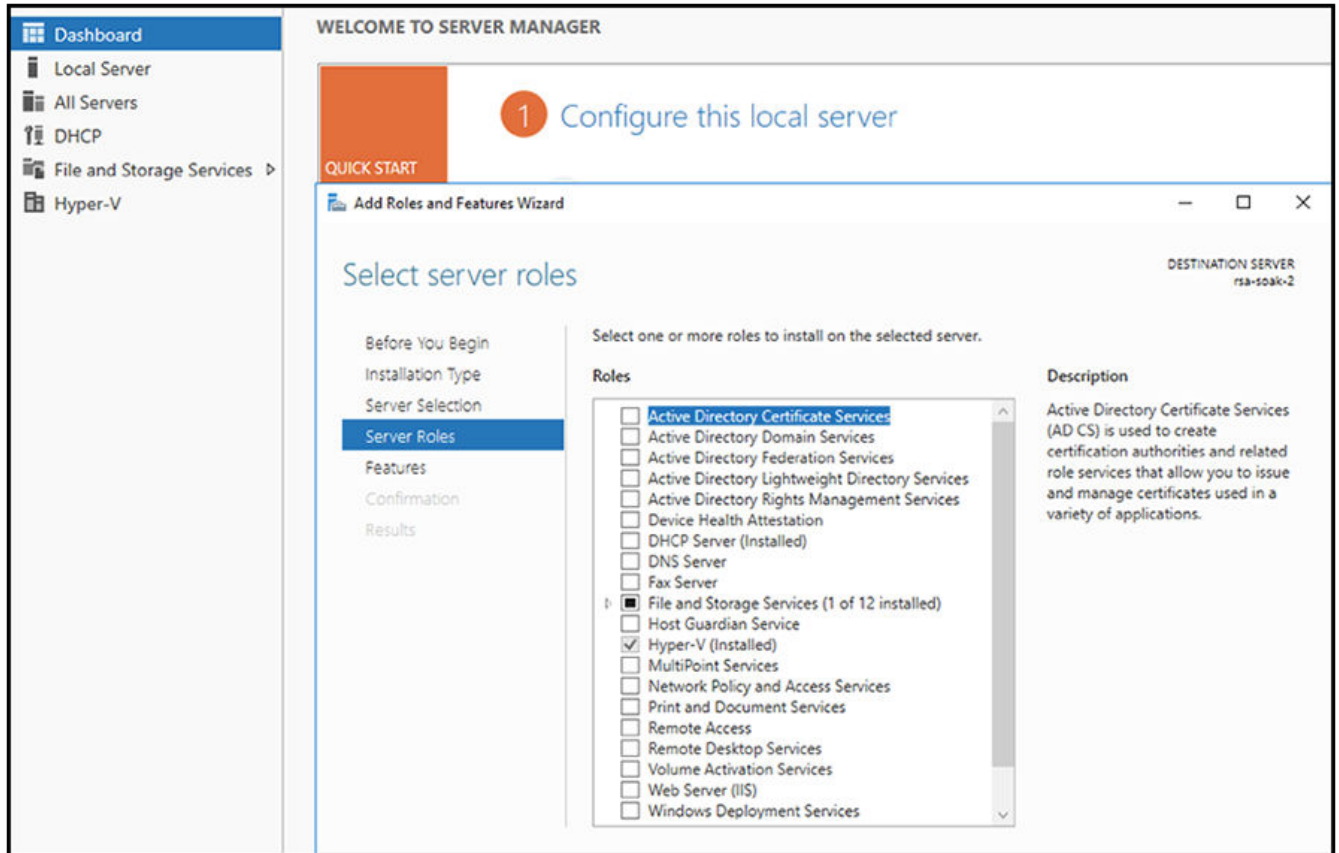
1. Download the Hyper-V image from the Ruckus support website.

Installing SCI

Installing the Hyper-V VM Image

2. Log in to the windows machine and enable the Hyper-V feature on the Windows server, as shown below:

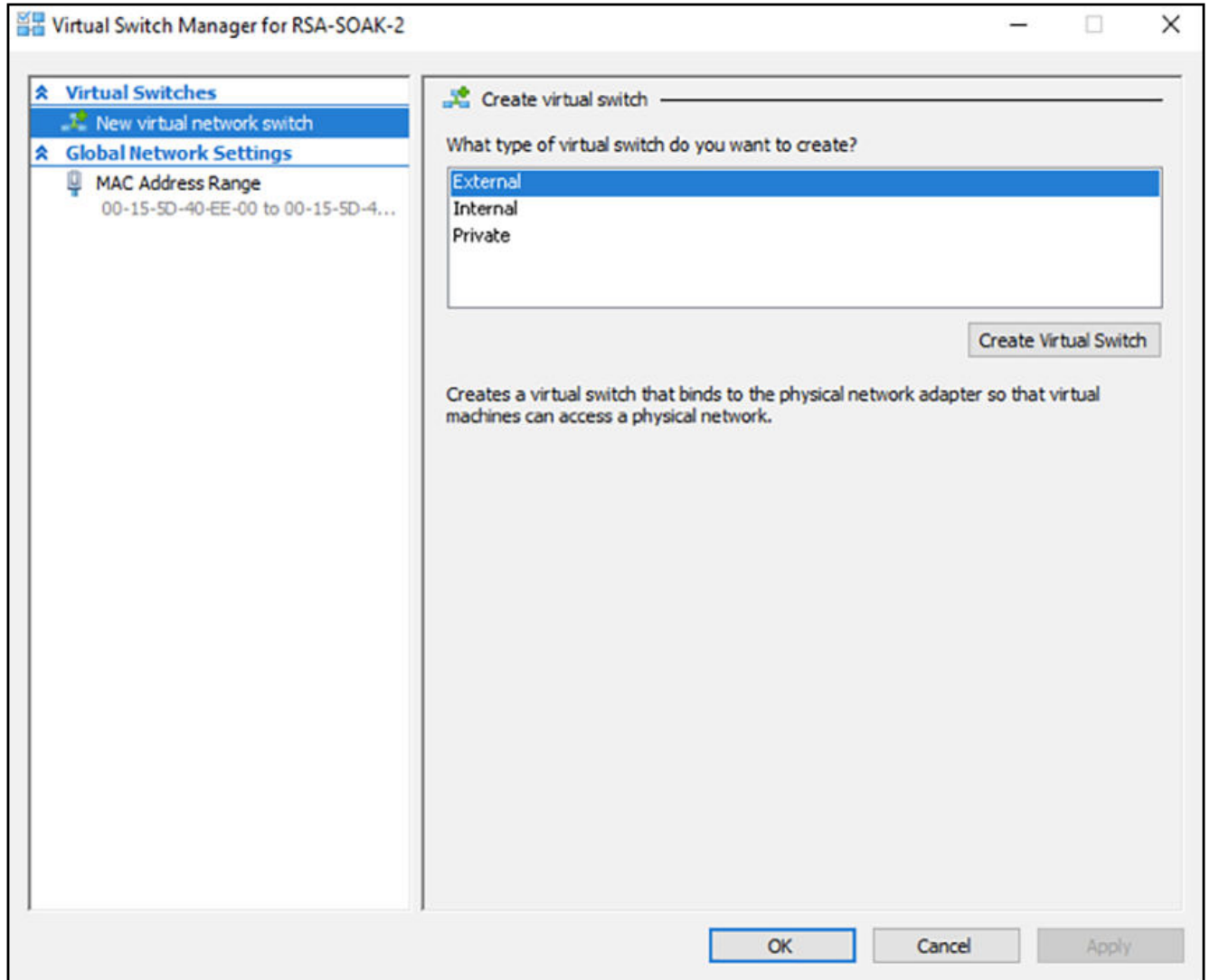
FIGURE 10 Enabling Hyper-V on the Windows Server



3. Enabling this feature will require your server to be restarted. Restart the server, then proceed with the remaining steps.

4. Create a virtual switch from the Virtual Switch Manager by selecting **New virtual network switch** under the Actions sidebar.

FIGURE 11 Creating a New Virtual Switch



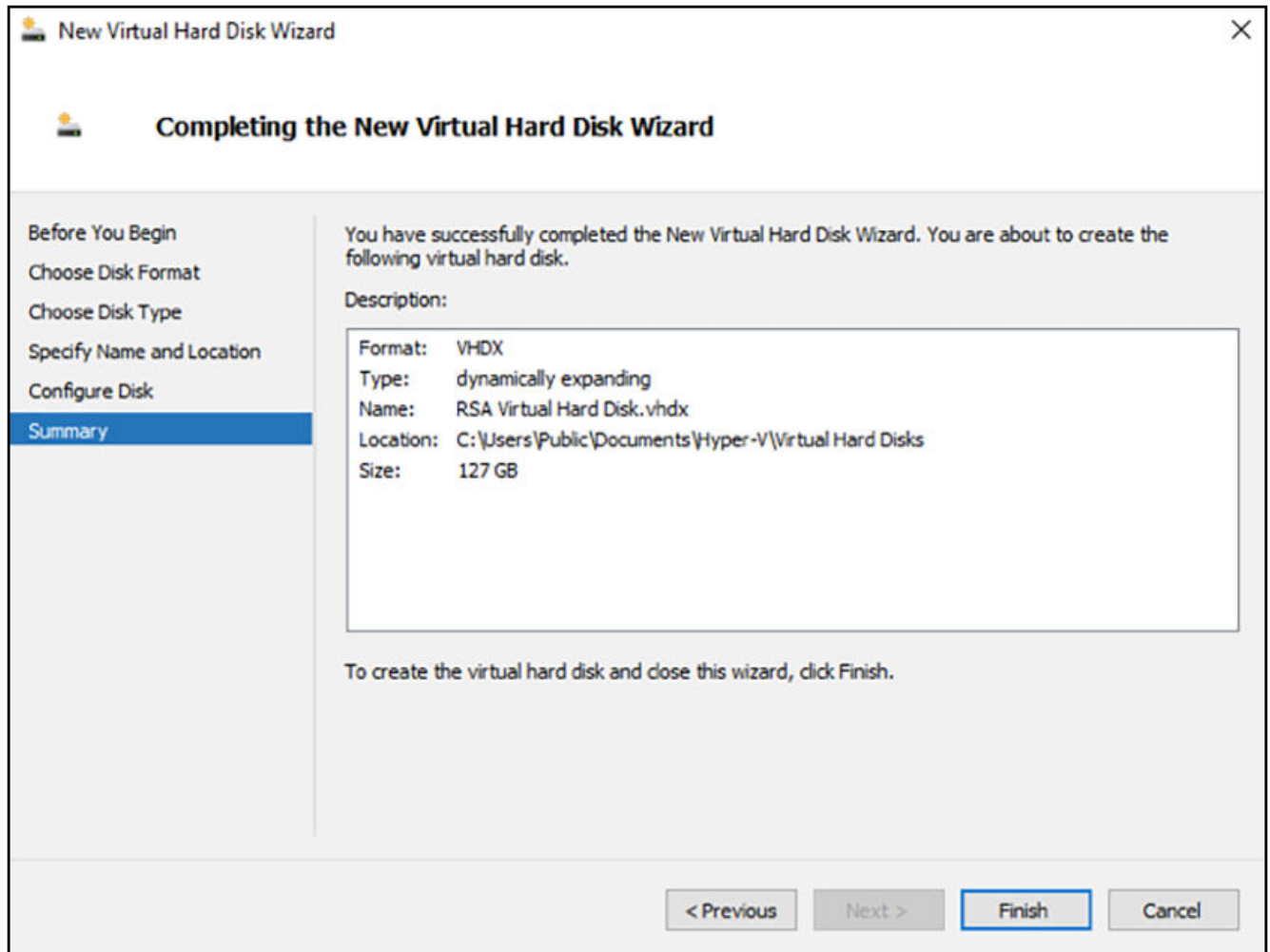
- a) Choose an **Internal** switch.
- b) You can name the internal switch "local" or any other desired name. This name will be used to attach the virtual switch to the virtual machine.

Installing SCI

Installing the Hyper-V VM Image

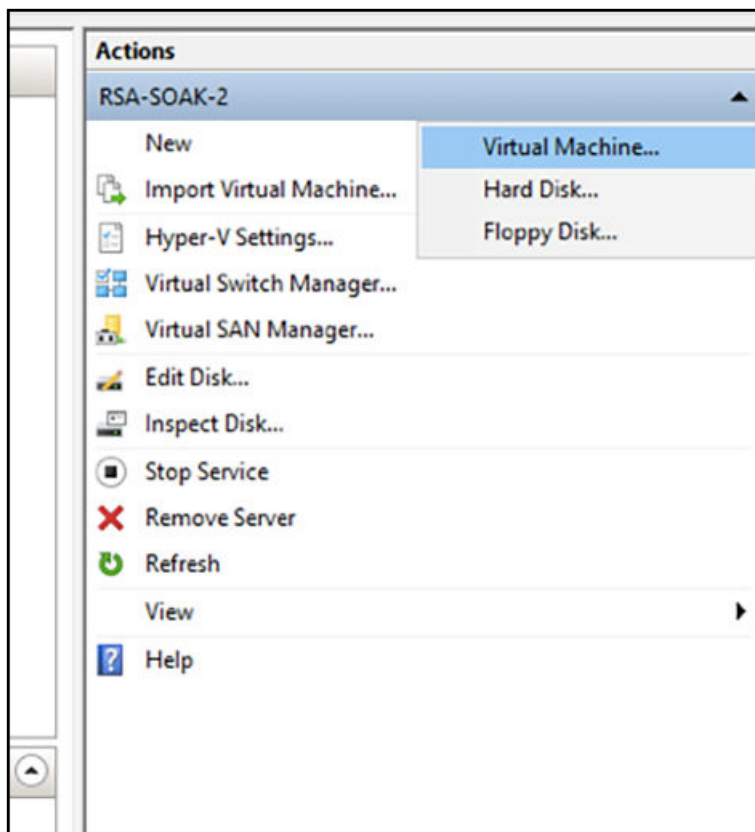
5. On your Windows machine, go to the Network and Sharing Center, then allow the network created above to have access to the default network by following these steps:
 - a) Locate the default network that has internet connectivity. Click on that network to invoke a pop-up window.
 - b) On the pop-up window, click the **Properties** button to bring up a second pop-up window.
 - c) On the second pop-up window, select the **Sharing** tab.
 - d) Select the first checkbox to allow this network to be shared.
 - e) Select the local network from the drop down. This is the same network that you created above for the internal switch.
 - f) Close the two pop-up windows.
6. Create a new hard disk drive with the required specifications that are listed in [Minimum Hardware Requirements](#) on page 9, including:
 - Hard disk 1 (Root volume): 80 GB
 - Hard disk 2 (Data volume): 500 GB

FIGURE 12 Creating a New Hard Drive Disk



7. Open the application called *Hyper-V Manager*.
8. Create a VM (master is 8 CPUs and 32 GB RAM; data is 4 CPUs and 20 GB RAM) from the Actions sidebar, under **New > Virtual Machine**.

FIGURE 13 Creating a New VM



- a) Attach the Virtual Network Switch to the VM.
 - b) The root and data volumes need to be set up as the first and second SCSI devices, respectively, on the first SCSI controller of the VM to be detected.
9. Set network firewall rules to ensure that the VM instance has access to the required inbound and outbound ports.
 10. Click on the newly created VM, and click on the **Start** button under the Actions sidebar.
 11. Once the VM launches, proceed with the setup.

Refer also to [Setting Up the Virtual Machine Using a Static IP Address](#) on page 20.

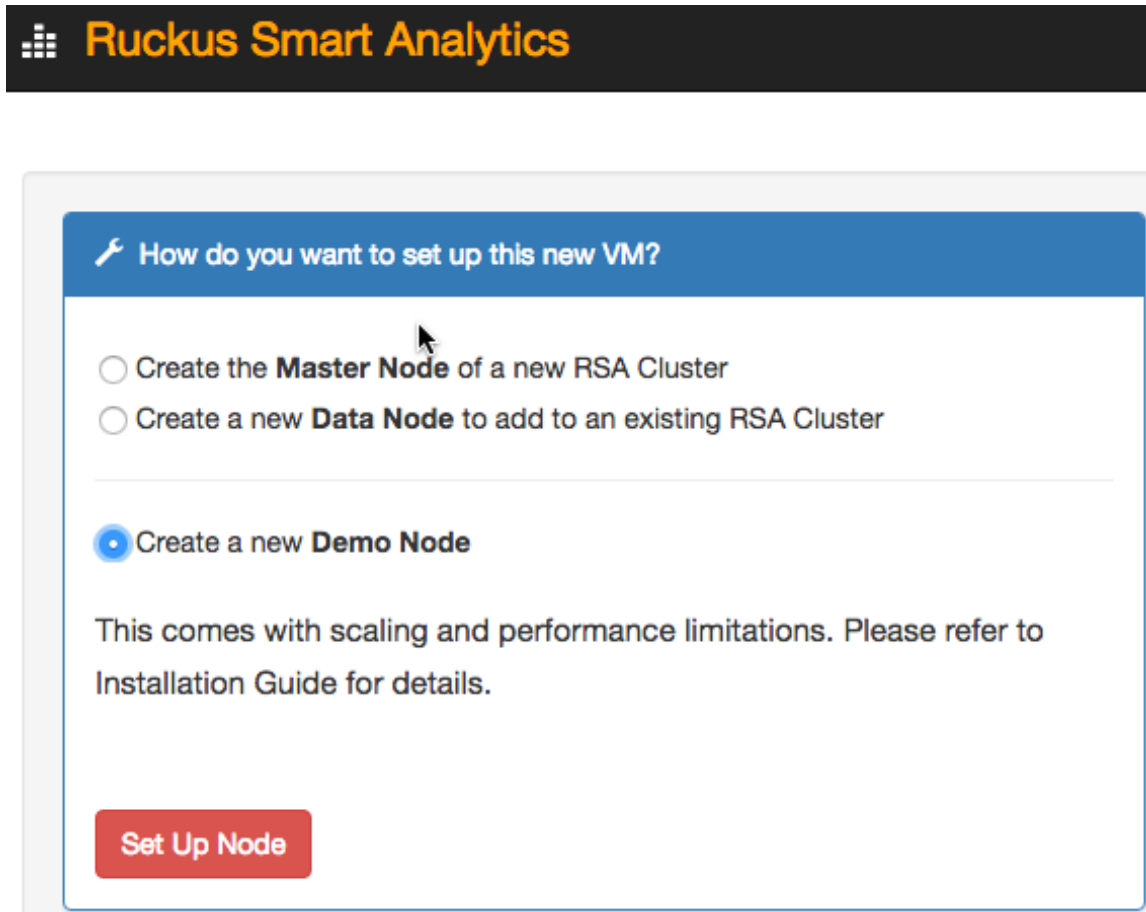
Setting Up the Nodes

You must setup the VM image created, as a Master node or a Data node so that the SCI cluster can be created.

Follow these steps to setup and activate the nodes:

1. Launch a web browser and browse to the SCI set up page (https://<SCI IP address or domain name>).
The **Ruckus Smart Access** page appears.
The Ruckus Smart Access portal uses a self-signed SSL certificate, so you will receive an invalid certificate warning from your browser.
2. You can set up the new VM as a Master Node, or a Data Node, or as a Demo Node.

FIGURE 14 Ruckus Smart Access page



3. From Ruckus Smart Analytics, select the **Create the Master Node of a new RSA cluster**, **Create a Data Node to add to an existing RSA Cluster** or **Create a new Demo Node** as appropriate.
4. Click **Set Up Node**.

The setup process takes a few minutes. When set up is complete, an acknowledgment page appears with the Node IP and Node Token numbers.

NOTE

Remember to record the IP address and token number of the Master node as you will require this information to setup the Data node, and scale the cluster at a later time.

This information is also available in the **Admin > Status & Update** page, within the **Ruckus Smart Access** interface.

You can login to the newly created user portal with the system default username: admin and password: admin.

- Click **Activate Master Node**, **Activate Data Node** or **Activate Demo Node** as appropriate, to activate the nodes.

NOTE

Ensure that no ports are blocked by the firewall between all the nodes within the SCI cluster. For more information, see [Firewall Rules](#) on page 31

- After activation is completed, the **Ruckus Smart Analytics** page appears. Login with user credentials to access the portal.

Firewall Rules

Firewall rules control incoming and outgoing data traffic between the SCI cluster and the controller interface.

The following firewall rules are observed for user access, controller access and NTP access.

TABLE 10 Firewall rules for User Access

	Main Portal	SSH	Cloud Updapter	Diagnostics
From	User IP	User IP	SCI Master Node IP and Data Node IPs	User IP
To	SCI Master Node IP	SCI Master Node IP and Data Node IPs	Internet (Static IP)	SCI Master Node IP
Port Number	443, 53000, 59090	22	443	55070, 58090, 58081, 58080
Protocol	HTTPS	SSH	HTTPS	HTTPS
Traffic Direction	Incoming traffic to SCI	Incoming traffic to SCI	Outgoing traffic from SCI	Incoming traffic to SCI

TABLE 11 Firewall rules for Controller Access

	SmartZone AP Stats (JSON) (for SmartZone 3.4.x and below)	SmartZone Application Data (for SmartZone 3.4.x and below)	SmartZone Data (for SmartZone 3.5 and above)	ZoneDirector Pull (XML)	ZoneDirector Push (XML) ZD 9.13 and above
From	SCI Master Node IP and Data Node IPs	SmartZone Management IP	SmartZone Management IP	ZoneDirector IP	SCI Master Node IP and Data Node IPs
To	SmartZone Management IP	SCI Master Node IP and Data Node IPs	SCI Master Node IP and Data Node IPs	SCI Master Node IP and Data Node IPs	ZoneDirector IP
Port Number	8443	1883	8883	443	443
Protocol	HTTPS	MQTT	MQTT	HTTPS	HTTPS
Traffic Direction	Outgoing traffic from SCI	Incoming traffic to SCI	Incoming traffic to SCI	Outgoing traffic from SCI	Incoming traffic to SCI

NOTE

Ensure that SCI runs within a secure network protected by a firewall. If SCI is exposed to the public internet, ensure that only the ports listed in the preceding tables are opened, and that the rest of the ports are closed by the firewall.

TABLE 12 Firewall rules for NTP Access

	SmartZone AP Stats (JSON)
From	SCI Master Node IP and Data Node IPs
To	NTP server IP
Port Number	123
Protocol	NTP
Traffic Direction	Outgoing traffic from SCI

Installing Custom SSL Certificate

Please ensure that this custom SSL certificate does not require the user to input a username and password to get authorized.

Be sure that you have the following files:

- A server certificate. For more information, refer to: http://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_certificate.
- A private key. For more information, refer to: http://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_certificate_key.

1. Copy these files to the SCI, as shown in the following example:

```
scp server.* rsa@54.149.124.136:.
```

2. Perform an SSH to the SCI.
3. Replace the default server certificate and private key files with the custom files, as shown in the following example:

```
sudo docker cp server.crt rsa-gateway:/etc/ssl/certs/server.crt  
sudo docker cp server.key rsa-gateway:/etc/ssl/private/server.key
```

NOTE

Whenever you update the SCI, the SSL certificate gets replaced by the default certificate, which requires you to replace the default with the custom certificate.

4. Restart the RSA gateway, as shown in the following example:

```
sudo docker restart rsa-gateway
```

Secure Shell Access to SCI

You can use Secure Shell (SSH) to login to a node.

Follow these steps to use SSH to configure the node (VM):

1. Open the VM console.

The IP address and token number of the node are displayed.

This information is also available in the **Admin > Status & Update** page, within the **Ruckus Smart Access** interface.

- Using SSH, login to the node.

ATTENTION

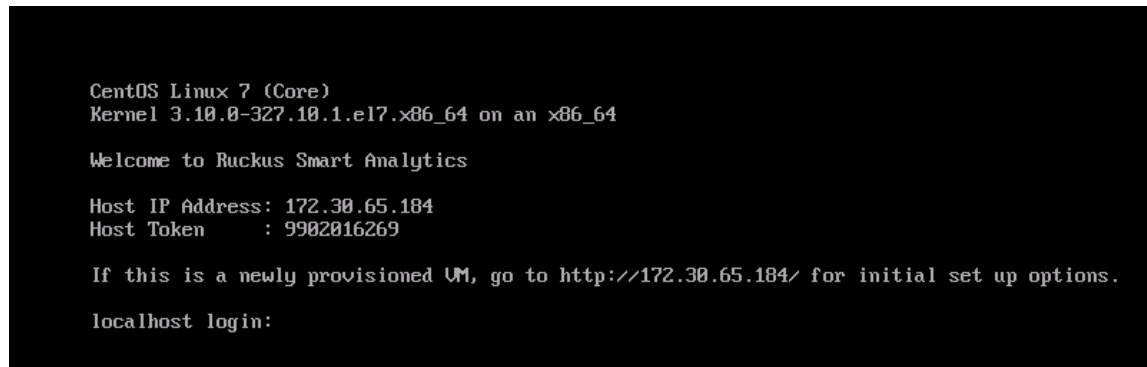
Login with the following credentials:

Username: rsa

Password: Node token

The node is now accessible and you can make the necessary configuration changes.

FIGURE 15 Sample SSH screen



```
CentOS Linux 7 (Core)
Kernel 3.10.0-327.10.1.el7.x86_64 on an x86_64

Welcome to Ruckus Smart Analytics

Host IP Address: 172.30.65.184
Host Token      : 9902016269

If this is a newly provisioned UM, go to http://172.30.65.184/ for initial set up options.

localhost login:
```


Configuring SMTP

- SMTP Overview.....35
- SMTP Configuration Steps..... 36
- Sending a Test Email..... 37

SMTP Overview

After the nodes in the SCI cluster are setup and activated, SCI must be configured. You can start by configuring your SMTP mail server to receive scheduled reports from SCI by e-mail.

Configuring the SMTP server is optional. However, If you do not configure the SMTP server, you will not receive any scheduled reports.

After SCI setup, log in to the system using the following default login credentials:

Username: admin

Password: admin

You are then directed to the **Settings page** where you can configure SMTP.

SMTP Configuration Steps

Follow the steps below to configure the SMTP mail server:

1. **Admin > Settings**

The **Settings** screen includes the Outgoing Mail Server (SMTP) section.

FIGURE 16 SMTP configuration

The screenshot shows the 'Outgoing Mail Server (SMTP)' configuration interface. It contains the following fields and values:

- Host:** email-smtp.us-west-2.amazonaws.com
- Port:** 587
- Username:** User123
- Password:** Leave blank to remain unchanged
- Encryption:** STARTTLS
- From Email:** rsa@ruckuslbs.com

At the bottom of the form, there are two buttons: a blue 'Update' button and a white 'Send Test Email' button.

2. You can configure the SMTP mail server to send or receive e-mail messages to or from SCI. The SMTP settings section contains the configuration details:
- **Host:** Enter the name of the host. The system now checks the SMTP connectivity and displays an error if the authentication is not successful.
 - **Port:** Enter the port number.
 - **Username:** Enter the user name required to access the SMTP mail server.
 - **Password:** Enter the password required to access the SMTP mail server.
 - **Encryption:** Select the encryption method from the drop down list. You can also disable the encryption by selecting **Disabled** from the drop down list.
 - **From email:** Enter the email ID that the messages are sent from.
3. To save your changes, click **Update**.

Sending a Test Email

You can test your SMTP settings by sending a test email.

1. After you have configured SMTP and saved your changes, click **Send Test Email**. The following popup appears:

FIGURE 17 Send Test Email Popup



The screenshot shows a modal dialog box titled "Send Test Email" with a close button (X) in the top right corner. Inside the dialog, there is a label "Email:" followed by a text input field containing the email address "ops@ruckuslbs.com". At the bottom right of the dialog, there are two buttons: a blue "Send" button and a white "Cancel" button with a grey border.

2. Click **Send**.
3. Check that you receive an email to confirm that SMTP is working properly. The subject of the email that you receive should be: "Test email from your Ruckus SmartCell Insight." The body of the email should be: " Hi there, this is a test email."

The email will be sent to the email address that is configured in the My Account screen > Profile section, which you open by clicking on the admin icon in the upper right of the SCI user interface, as shown in the following figure:

FIGURE 18 Email Address to Receive SMTP Test Email Reply from Ruckus



The screenshot shows the "My Account" page in a web interface. The page title is "My Account". In the top right corner, there is a user profile icon labeled "admin" with a dropdown menu containing "My Account" and "Logout". The main content area is titled "Profile" and displays the following information: "Username: admin" and "Email: user1@ruckuslbs.com". Below the email field, there is a note: "This email will receive alerts regarding the system". At the bottom of the profile section, there is a blue "Update Profile" button.

Adding Controllers to Both the SCI and Controller User Interfaces

- Overview of Adding Controllers to SCI..... 39
- Adding a SmartZone Controller Version 3.5 or Greater..... 40
- Adding a SmartZone Controller Version Prior to 3.5..... 42
- Adding a Zone Director Controller: Push Method..... 46
- Adding a Zone Director Controller: Poll Method..... 48
- Important Setting on the ZoneDirector UI..... 50
- Editing Controllers in the SCI User Interface..... 50

Overview of Adding Controllers to SCI

You must add controllers to SCI to monitor and manage them. SCI analyzes data from the controller and provides information about the WiFi network performance.

The choices of controllers that you can add are:

- SmartZone version 3.5 or later
- SmartZone versions prior to 3.5
- ZoneDirector (Push, ZD versions 9.13-MR1 and above and ZD10-MR1 and above)
- ZoneDirector (Poll, ALL ZD versions)

In SCI, go to the **Admin > Settings** screen. An example of a listing of already-configured controllers on this screen is shown below.

FIGURE 19 Adding and deleting controllers

Settings					
Systems					
	System ID	Type	URL	User	Last Seen
<input type="checkbox"/>	SystemID1	SmartZone (SCG/SZ/vSZ < 3.5)	https://192.168.1.112:8443	admin	2 minutes ago
<input type="checkbox"/>	SystemID2	SmartZone (SCG/SZ/vSZ >= 3.5)	https://192.168.1.112:8443	admin	
<input type="checkbox"/>	SystemID3	SmartZone (SCG/SZ/vSZ >= 3.5)	https://192.168.1.112:8443	admin	3 months ago
<input type="checkbox"/>	SystemID4	SmartZone (SCG/SZ/vSZ < 3.5)	https://192.168.1.112:8443	sci_mon	2 minutes ago
<input type="checkbox"/>	SystemID5	SmartZone (SCG/SZ/vSZ < 3.5)	https://192.168.1.112:8443	ruckus.sci	2 minutes ago
<input type="checkbox"/>	SystemID6	SmartZone (SCG/SZ/vSZ < 3.5)	https://192.168.1.112:8443	rsa-agent	2 minutes ago
<input type="checkbox"/>	SystemID7	SmartZone (SCG/SZ/vSZ < 3.5)	https://192.168.1.112:8443	admin	2 minutes ago
<input type="checkbox"/>	SystemID8	ZoneDirector (Poll, all ZD versions)	https://192.168.1.112:8443	admin	3 minutes ago
<input type="checkbox"/>	SystemID9	ZoneDirector (Poll, all ZD versions)	https://192.168.1.112:8443	admin	3 minutes ago
<input type="checkbox"/>	SystemID10	SmartZone (SCG/SZ/vSZ >= 3.5)	https://192.168.1.112:8443	admin	4 minutes ago
<input type="checkbox"/>	SystemID11	SmartZone (SCG/SZ/vSZ < 3.5)	https://192.168.1.112:8443	admin	20 days ago
<input type="checkbox"/>	SystemID12	SmartZone (SCG/SZ/vSZ < 3.5)	https://192.168.1.112:8443	admin	5 months ago

Adding Controllers to Both the SCI and Controller User Interfaces

Adding a SmartZone Controller Version 3.5 or Greater

To add a controller, click **Add** in the upper-right portion of the screen. The following popup appears:

FIGURE 20 Adding a New Controller Popup

The screenshot shows a 'New System' dialog box with the following fields and options:

- System ID:** Text input field.
- Type:** Dropdown menu showing 'SmartZone (SCG/SZ/vSZ < 3.5)'. The dropdown list includes:
 - ZoneDirector (Poll, all ZD versions)
 - ZoneDirector (Push, ZD >= 9.13)
 - SmartZone (SCG/SZ/vSZ < 3.5)
 - SmartZone (SCG/SZ/vSZ >= 3.5)
- URL:** Dropdown menu showing 'ZoneDirector (Poll, all ZD versions)'. The dropdown list includes:
 - ZoneDirector (Push, ZD >= 9.13)
 - SmartZone (SCG/SZ/vSZ < 3.5)
 - SmartZone (SCG/SZ/vSZ >= 3.5)
- Backup URL:** Dropdown menu showing 'SmartZone (SCG/SZ/vSZ < 3.5)'. The dropdown list includes:
 - SmartZone (SCG/SZ/vSZ >= 3.5)
- Username:** Text input field.
- Password:** Text input field.

Buttons: **Create** (blue), **Cancel** (white).

The following sections describe how to add each type of controller.

Adding a SmartZone Controller Version 3.5 or Greater

Use the procedures shown to add a SmartZone Controller version 3.5 or greater to both the SCI and Controller web user interfaces.

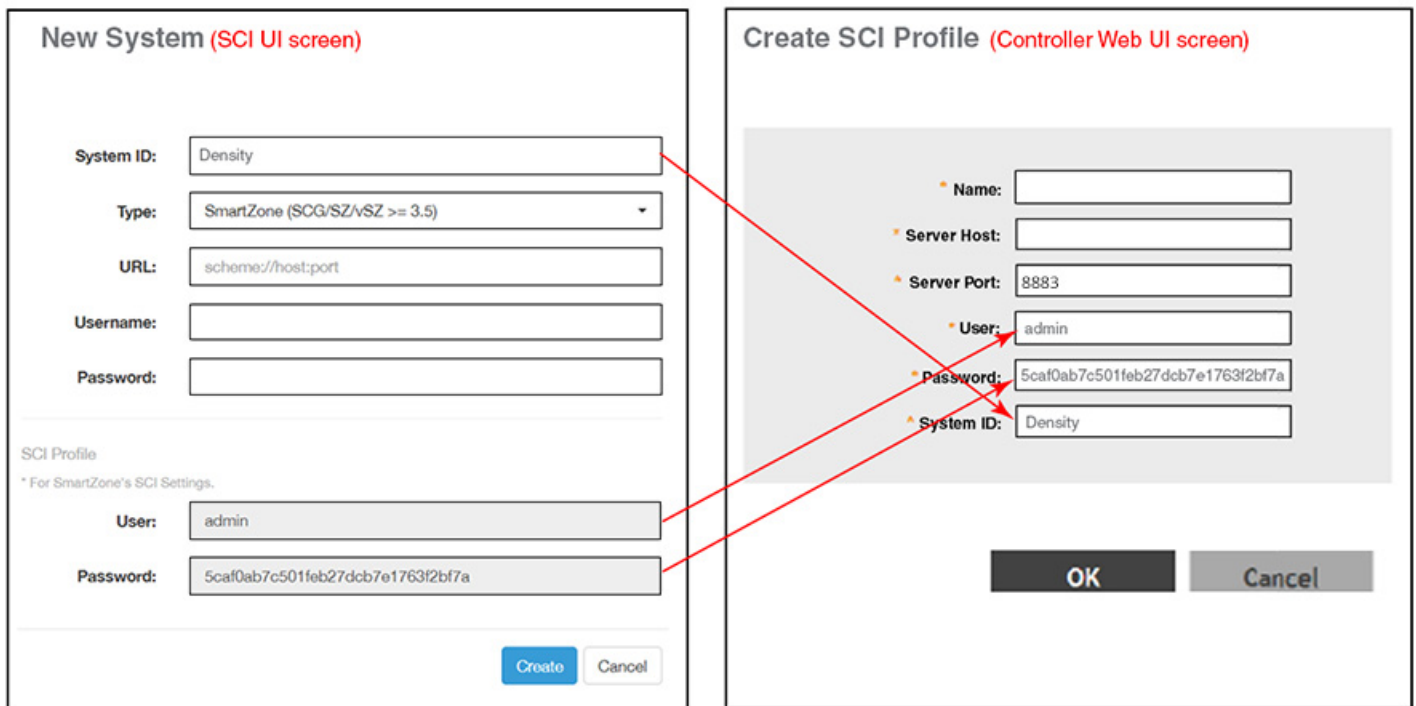
Adding a SmartZone Version 3.5 or Later in the SCI User Interface

If you choose SmartZone version 3.5 or later from the popup, the New System screen, shown on the left-hand side of the figure below, appears.

NOTE

The figure below shows **two** screens: 1) the New System screen, which is on the SCI user interface, and 2) the Create SCI Profile screen, which is on the Controller Web UI at **Systems > General Settings > SCI**. There are three fields in the New System screen whose values must be entered **identically** in the Create SCI Profile screen. The three fields that must match are indicated with arrows in the figure below.

FIGURE 21 Adding a SmartZone Version 3.5 or Later



The following is a complete list all the fields that you must configure in the SCI New System screen when adding a SmartZone 3.5 controller:

- System ID: This is the unique name of the controller that you want to add to SCI. As shown in the figure above, this field must be identical between the SCI New System screen and the Create SCI Profile screen of the Controller Web UI.

NOTE

The system ID cannot be changed once it has been configured in the SCI Add System screen.

- Type: This is the controller type you have already selected from the drop-down menu.
- URL: URL of the controller.
- Username: The administrator username to access the controller.
- Password: The administrator password to access the controller.
- **SCI Profile:** Enter the **User** and **Password** login credentials to access the SCI profile. These login credentials are different from the administrator credentials listed in the two preceding bullet items. As shown in the figure above, the two SCI Profile fields must be identical between the SCI New System screen and the Create SCI Profile screen of the Controller Web UI.

NOTE

Do not add each controller of the cluster as a separate controller in the SCI.

Click **Create** to add the new controller.

The new controller should be listed in the Settings screen, and a confirmation message should be displayed.

Configuring SmartZone Version 3.5 or Later to Send Data to SCI

Follow these steps to configure the SCI settings in the controller web UI:

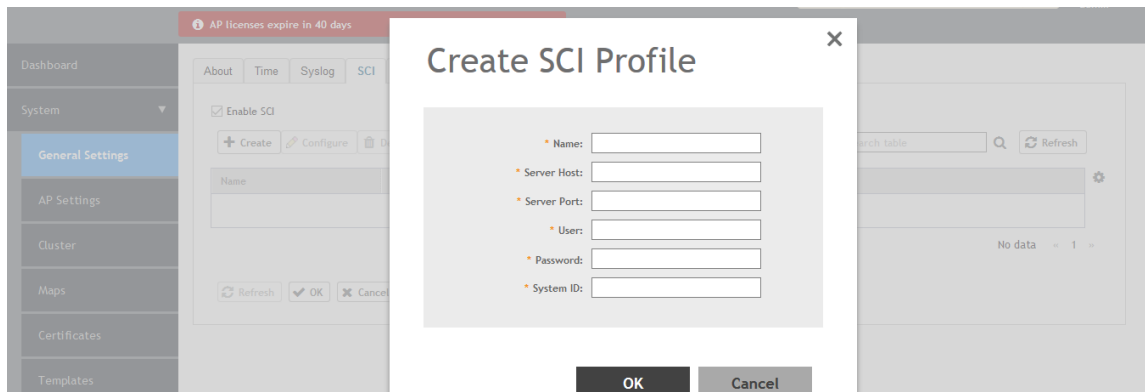
NOTE

This procedure is applicable for all controllers running SmartZone 3.5 and above.

1. In the controller web UI, click **System > General Settings > SCI**.

The **SCI Setting** page appears.

FIGURE 22 SmartZone 3.5 SCI Setting page



2. Select the **Enable SCI** check-box. This enables SmartZone application visibility.
3. Click **Create** to create a new SCI profile. The **Create SCI Profile** screen appears.

You can click **Configure** to modify an existing SCI profile.

4. Configure the following SCI settings:
 - Name: Type the name of the SCI profile.
 - Server Host: Type the SCI IP address or the domain name.
 - Server Port: Set to 8883.

NOTE

For the "User," "Password," and "System ID" fields, refer to [Figure 21](#), and be sure that the values match those configured in the SCI User Interface.

5. Click **OK**.

Adding a SmartZone Controller Version Prior to 3.5

Use the procedures shown to add a SmartZone Controller version prior to 3.5 to both the SCI and Controller web user interfaces.

Adding a SmartZone Version Prior to 3.5 on the SCI UI

If you choose SmartZone version less than 3.5 from the popup, the following screen appears:

FIGURE 23 Adding a SmartZone Controller Version Prior to 3.5 in the SCI User Interface

The image shows a 'New System' dialog box with the following fields and options:

- System ID:** A text input field.
- Type:** A dropdown menu with the selected option 'SmartZone (SCG/SZ/vSZ < 3.5)'.
- URL:** A text input field with the placeholder 'scheme://host:port'.
- Backup URL:** A text input field with the placeholder 'scheme://host:port'.
- Username:** A text input field.
- Password:** A text input field.
- Buttons:** 'Create' (blue) and 'Cancel' (white) buttons at the bottom right.

Configure the following controller settings:

- System ID: Name of the controller you want to add to SCI.

NOTE

The controller name should be unique and cannot be changed.

- Type: This is the controller type you have already selected from the drop-down menu.
- URL: URL of the controller.
- Backup URL: URL of the backup controller location.
- Username: The administrator username to access the controller.
- Password: The administrator password to access the controller.

NOTE

The username and password must be *created* in the controller.

Click **Create** to add the new controller.

The new controller should be listed in the Settings screen, and a confirmation message should be displayed.

Configuring SmartZone Version Prior to 3.5 to Send Data to SCI

Follow these steps to configure the SCI settings on the SmartZone controller web UI:

1. In the controller web UI, click **Configuration > System > SCI Setting**.

The **SCI Setting** page appears.

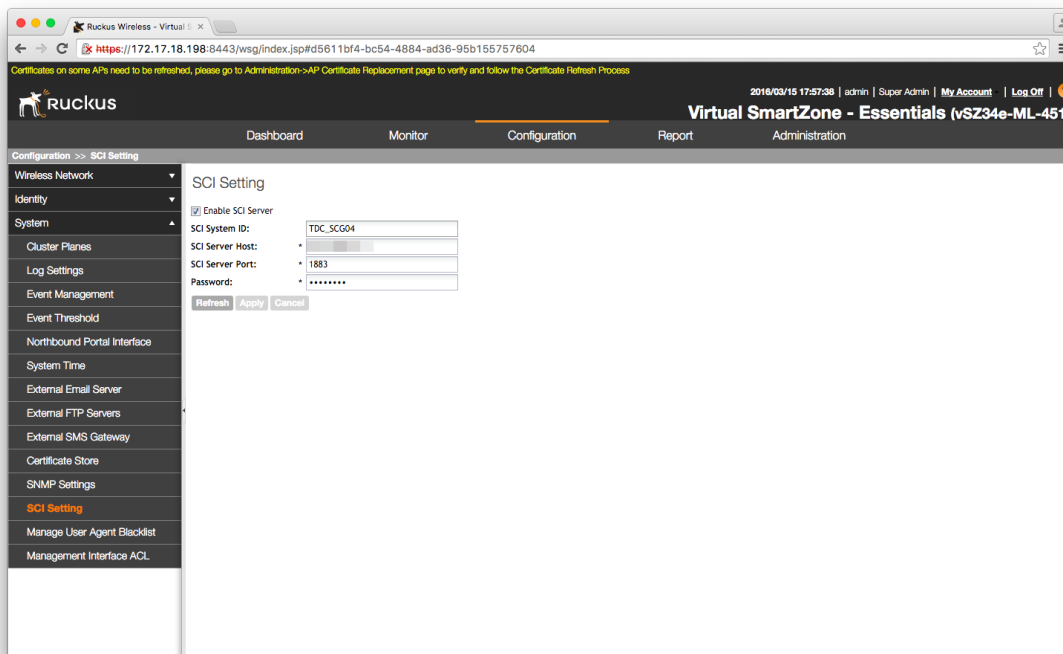
Adding Controllers to Both the SCI and Controller User Interfaces

Adding a SmartZone Controller Version Prior to 3.5

NOTE

This procedure is applicable for all controllers running SmartZone 3.4 and below.

FIGURE 24 SmartZone 3.4 SCI Setting page



2. Select the **Enable SCI Server** check-box. This enables SmartZone application visibility.
3. Configure the following SCI settings:
 - SCI System ID: Type the unique name that was given while adding the controller.
 - SCI Server Host: Type the SCI IP address or the domain name
 - SCI Server Port: Set to 1883.
 - Password: Enter the password to access the SCI server.

You have completed configuring the SCI server settings on the SmartZone 3.4 controller.

NOTE

The Master and Data node IP addresses must be *white-listed* on the controller for SCI to *pull* data from the controllers.

Enabling AP SCI Statistics Delivery on SmartZone 3.4 Controllers

Ruckus Wireless APs do not send statistics that are customized for SCI to SmartZone controllers in order to save network and disk resources. If you add a SmartZone controller as a data source for SCI, you must enable AP SCI statistics delivery on the controller.

Follow these steps to enable AP SCI statistics delivery:

1. Run the following commands to verify if the APs are sending statistics to SCI:

- **SZ> enable**
- **Password: *******
- **SZ# show running-config zone-global ap-sci**
- **AP SCI: Enabled**

After executing these commands, if the output is `AP SCI: Disabled`, follow the next step to enable AP SCI.

2. Run the following commands to enable AP SCI:

- **SZ> enable**
- **Password: *******
- **SZ# config**
- **SZ(config)# ap-sci enable**
- **SZ(config)# exit**
- **SZ#**

Verify that AP SCI is enabled by running the **show running-config zone-global ap-sci** command again.

For SmartZone version 3.2, see [Enabling AP SCI Statistics Delivery on SmartZone 3.2 Controllers](#) on page 45. For other SmartZone versions, refer to the SmartZone documentation for details about how to enable APs to send statistics tailored for SCI to the SmartZone controller.

The SCI Master and Data Node IP Addresses must be whitelisted on the controller for SCI to pull data from the controllers.

Enabling AP SCI Statistics Delivery on SmartZone 3.2 Controllers

Ruckus Wireless APs do not send statistics that are customized for SCI to SmartZone controllers in order to save network and disk resources. If you add a SmartZone controller as a data source for SCI, you must enable AP SCI statistics delivery on the controller.

Follow these steps to enable AP SCI statistics delivery:

1. Run the following commands to verify if the APs are sending statistics to SCI:

- **SZ> enable**
- **Password: *******
- **SZ# show running-config common-settings ap-sci**
- **AP SCI: Enabled**

After executing these commands, if the output is `AP SCI: Disabled`, follow the next step to enable AP SCI.

2. Run the following commands to enable AP SCI:

- **SZ> enable**
- **Password: *******
- **SZ# config**
- **SZ(config)# ap-sci enable**
- **SZ(config)# exit**
- **SZ#**

Verify that AP SCI is enabled by running the **show running-config common-settings ap-sci** command again.

Adding Controllers to Both the SCI and Controller User Interfaces

Adding a Zone Director Controller: Push Method

For SmartZone version 3.4, see [Enabling AP SCI Statistics Delivery on SmartZone 3.4 Controllers](#) on page 44. For other SmartZone versions, refer to the SmartZone documentation for details about how to enable APs to send statistics tailored for SCI to the SmartZone controller.

The SCI Master and Data Node IP Addresses must be whitelisted on the controller for SCI to pull data from the controllers.

Adding a Zone Director Controller: Push Method

With the push method, ZoneDirector pushes data to SCI.

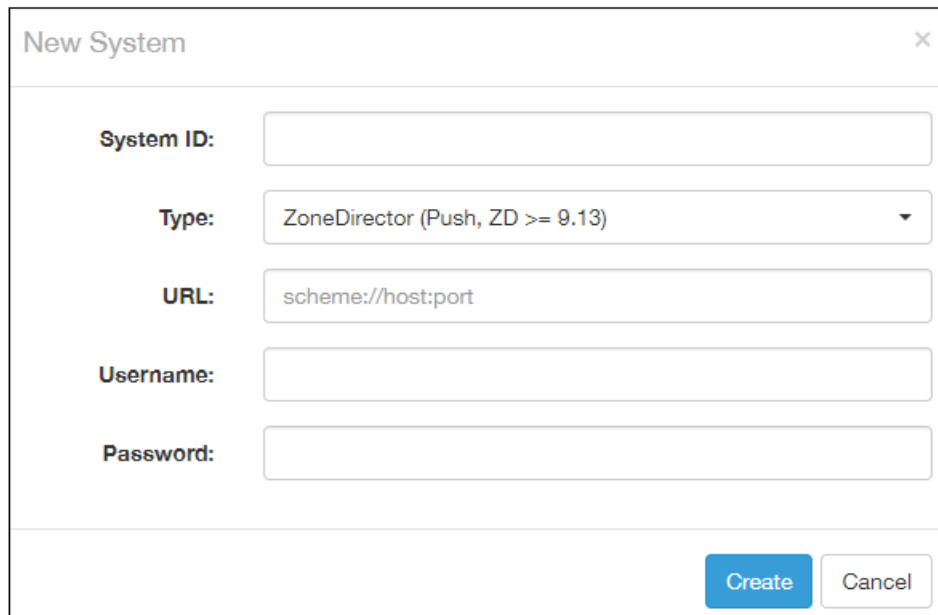
If you have Zone Director version 9.13 - MR1 or higher, version, you have the choice of using the push mechanism or polling option.

Ensure that you use only one of these mechanisms to avoid duplicate data.

Adding Zone Director (Push Method) on the SCI UI

If you choose the push method from the popup, the following screen appears:

FIGURE 25 Adding a ZoneDirector in the SCI User Interface to Use Push Method



The screenshot shows a 'New System' dialog box with the following fields and options:

- System ID:** An empty text input field.
- Type:** A dropdown menu currently set to 'ZoneDirector (Push, ZD >= 9.13)'. A downward arrow is visible on the right side of the dropdown.
- URL:** A text input field containing the placeholder text 'scheme://host:port'.
- Username:** An empty text input field.
- Password:** An empty text input field.

At the bottom right of the dialog, there are two buttons: a blue 'Create' button and a white 'Cancel' button with a grey border.

Configure these settings:

- System ID: Name of the controller you want to add to SCI.

NOTE

The controller name should be unique and cannot be changed.

- Type: This is the controller type you have already selected from the drop-down menu.
- URL: URL of the controller.
- Username: The administrator username to access the controller.

- Password: The administrator password to access the controller.

NOTE

The username and password must be *created* in the controller.

Click **Create** to add the new controller.

The new controller should be listed in the SCI Settings screen, and a confirmation message should be displayed.

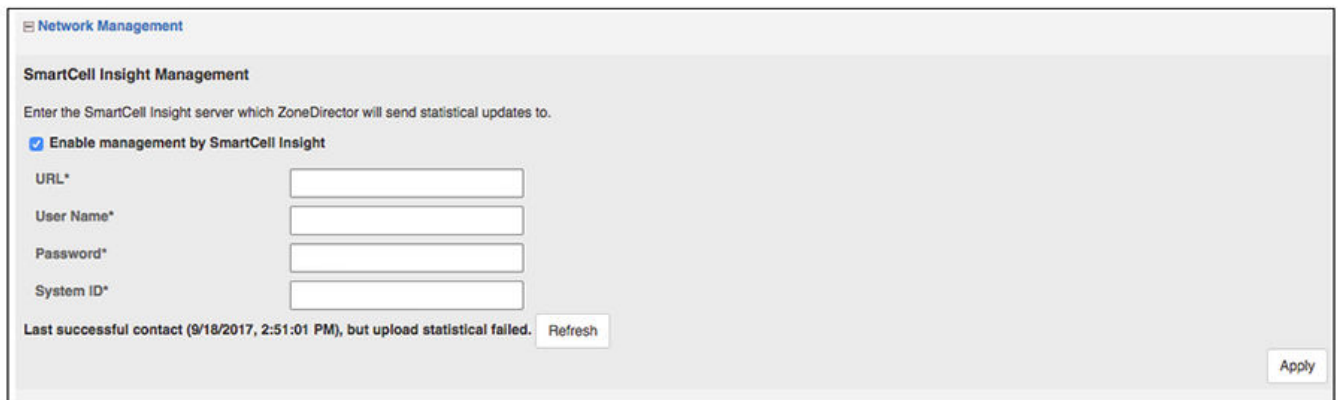
Configuring Zone Director (Push Method) to Send Data to SCI

Follow these steps to configure the SCI settings on the ZoneDirector controller web UI:

1. Navigate to **Configure > System**.
2. Click the **Network Management** option at the bottom of the page.

The SCI management section opens, and you can enter the SCI details:

FIGURE 26 ZoneDirector (Push Method) SCI Settings Page on Controller Web UI



3. Configure the following SCI settings:

- URL: URL of the SCI.

NOTE

The URL must be in the form: **https://[IP_address]** with no slash or port number after the IP address.

- User Name: Login username for SCI.
- Password: Login password for SCI.
- System ID: Set this to the same unique name that was used in the SCI user interface screen for adding a controller.

4. Click **Apply**.

If you are using ZD3000 or ZD5000, setting the above configuration completes the setup required to enable ZoneDirector Push data. However, for ZD1100 and ZD 1200, additional configuration is required to enable Push XML settings. Please follow the steps shown in the following code block if you have a ZD 1100 or ZD 1200:

```
ruckus> en
ruckus# config
You have all rights in this mode.
ruckus(config)# system
```

Adding Controllers to Both the SCI and Controller User Interfaces

Adding a Zone Director Controller: Poll Method

```
ruckus(config-sys)# session-stats-resv
The session statistics function has been enabled.
ruckus(config-sys)# quit
No changes have been saved.
ruckus(config-sys)# show

Session Statistics:
Enable= true
Limited Unauthorized Session= true

ruckus(config)# quit
```

Adding a Zone Director Controller: Poll Method

With the poll method, SCI regularly polls the ZoneDirector for data.

If you have a ZoneDirector 9.13 or lower version, the only option available to bring data into SCI is the polling mechanism

If you have Zone Director version 9.13 - MR1 or higher, version, you have the choice of using the polling option or the push mechanism.

Ensure that you use only one of these mechanisms to avoid duplicate data.

Adding Zone Director (Poll Method) on the SCI UI

If you choose the polling method from the popup, the following screen appears:

FIGURE 27 Adding a ZoneDirector in the SCI User Interface to Use Poll Method

The screenshot shows a 'New System' dialog box with the following fields and options:

- System ID:** An empty text input field.
- Type:** A dropdown menu currently showing 'ZoneDirector (Poll, all ZD versions)'.
- URL:** A text input field with the placeholder text 'scheme://host:port'.
- Username:** An empty text input field.
- Password:** An empty text input field.

At the bottom right of the dialog are two buttons: 'Create' (highlighted in blue) and 'Cancel'.

Configure these settings:

- System ID: Name of the controller you want to add to SCI.

NOTE

The controller name should be unique and cannot be changed.

- Type: This is the controller type you have already selected from the drop-down menu.
- URL: URL of the controller.
- Username: The administrator username to access the controller.
- Password: The administrator password to access the controller.

NOTE

The username and password must be *created* in the controller.

Click **Create** to add the new controller.

The new controller should be listed in the SCI Settings screen, and a confirmation message should be displayed.

Configuring Zone Director (Poll Method) to Send Data to SCI

The only action required on the controller side is to keep port 443 open.

Important Setting on the ZoneDirector UI

When setting up a ZoneDirector from which SCI will retrieve data, please ensure that the **Enable login Warning** box is *not* checked. If it is checked, SCI will have trouble retrieving data from the ZoneDirector.

FIGURE 28 Do Not Enable Login Warnings in ZoneDirector Configuration

The screenshot shows the 'SMS settings' section of the ZoneDirector configuration interface. It features two radio button options: 'twilio account information' (selected) and 'clickatell account information'. The Twilio section includes input fields for 'Account SID', 'Auth Token', and 'From PhoneNumber', with a link to '[register a new twilio account]'. The Clickatell section includes input fields for 'User Name', 'Password', 'API Id', and 'From PhoneNumber', with a link to '[register a new clickatell account]'. Below this is the 'login Warning' section, which contains the text 'Enable login warning to pop up a warning after a user logs into the ZD management GUI and SSH.' and an unchecked checkbox for 'Enable login Warning'. A text area for 'Customize Warning Content:' contains the message: 'Warning, you are logging into device for authorized user only. If you are not an authorized user, please click Quit; otherwise click Continue to login.' At the bottom left, there is a 'Network Management' link.

The path to get to this screen in the ZoneDirector Web UI is **Configure > System**. The **Enable login Warning** box is located in the bottom half of the screen.

Editing Controllers in the SCI User Interface

You can modify information about a controller that you have already added to SCI.

NOTE

You cannot modify the name (System ID) of the controller once it is created.

Follow these steps to edit the controller's information:

- From the SCI dashboards, go to **Admin > Settings**.
 The **Settings** screen appears.

FIGURE 29 List of Controllers on Settings screen

Settings					
Systems ✕ Delete + Add					
<input type="checkbox"/>	System ID	Type	URL	User	Last Seen
<input type="checkbox"/>	SystemID1	SmartZone (SCG/SZ\VSZ < 3.5)	https://192.168.1.111:8443	admin	2 minutes ago
<input type="checkbox"/>	SystemID2	SmartZone (SCG/SZ\VSZ >= 3.5)	https://192.168.1.111:8443	admin	
<input type="checkbox"/>	SystemID3	SmartZone (SCG/SZ\VSZ >= 3.5)	https://192.168.1.111:8443	admin	3 months ago
<input type="checkbox"/>	SystemID4	SmartZone (SCG/SZ\VSZ < 3.5)	https://192.168.1.111:8443	sci_mon	2 minutes ago
<input type="checkbox"/>	SystemID5	SmartZone (SCG/SZ\VSZ < 3.5)	https://192.168.1.111:8443	ruckus.sci	2 minutes ago
<input type="checkbox"/>	SystemID6	SmartZone (SCG/SZ\VSZ < 3.5)	https://192.168.1.111:8443	rsa-agent	2 minutes ago
<input type="checkbox"/>	SystemID7	SmartZone (SCG/SZ\VSZ < 3.5)	https://192.168.1.111:8443	admin	2 minutes ago
<input type="checkbox"/>	SystemID8	ZoneDirector (Poll, all ZD versions)	https://192.168.1.111:8443	admin	3 minutes ago
<input type="checkbox"/>	SystemID9	ZoneDirector (Poll, all ZD versions)	https://192.168.1.111:8443	admin	3 minutes ago
<input type="checkbox"/>	SystemID10	SmartZone (SCG/SZ\VSZ >= 3.5)	https://192.168.1.111:8443	admin	4 minutes ago
<input type="checkbox"/>	SystemID11	SmartZone (SCG/SZ\VSZ < 3.5)	https://192.168.1.111:8443	admin	20 days ago
<input type="checkbox"/>	SystemID12	SmartZone (SCG/SZ\VSZ < 3.5)	https://192.168.1.111:8443	admin	5 months ago

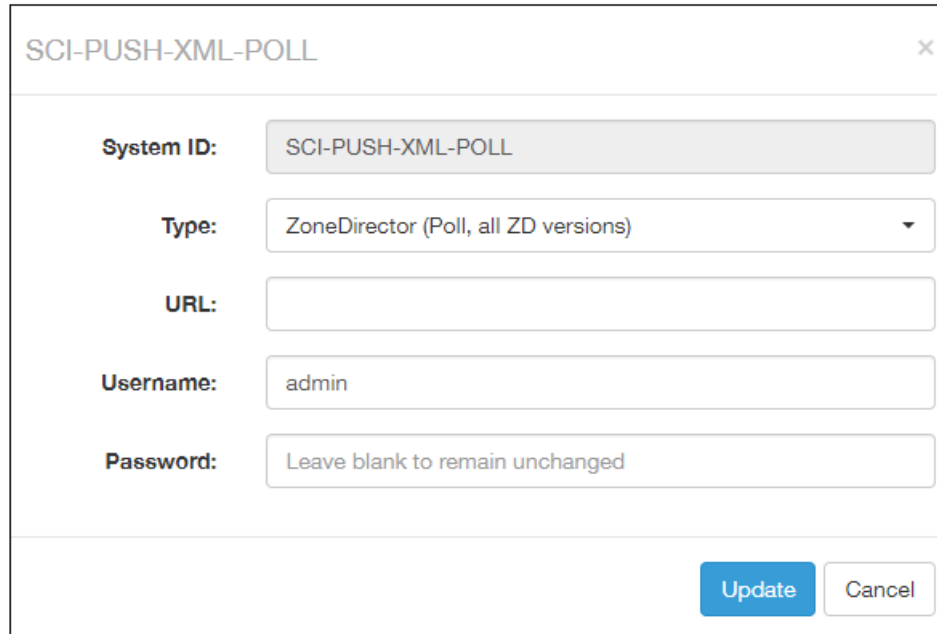
Adding Controllers to Both the SCI and Controller User Interfaces

Editing Controllers in the SCI User Interface

2. Click the controller that you want to edit.

A dialogue box appears with controller information you can modify, as shown. Make necessary changes.

FIGURE 30 Editing controller information



The image shows a dialog box titled "SCI-PUSH-XML-POLL" with a close button (X) in the top right corner. The dialog contains the following fields:

- System ID:** A text field containing "SCI-PUSH-XML-POLL".
- Type:** A dropdown menu showing "ZoneDirector (Poll, all ZD versions)".
- URL:** An empty text field.
- Username:** A text field containing "admin".
- Password:** A text field containing "Leave blank to remain unchanged".

At the bottom right of the dialog, there are two buttons: "Update" (a blue button) and "Cancel" (a white button with a grey border).

3. Click **Update**.

You have successfully edited the controller's information.

Updating the SCI Software

- [Updating the Software from the Cloud.....](#)53
- [Updating the Software Package by Downloading it.....](#) 53

You can update your SCI software either from the cloud or by downloading the updated software package.

Updating the Software from the Cloud

You can update the SCI software from the cloud if you are connected to the internet (recommended).

Follow these steps to update the software from the cloud:

NOTE

Because the cloud updater downloads images from Amazon AWS, ensure that the following domains are whitelisted from the SCI VM for both incoming and outgoing traffic:

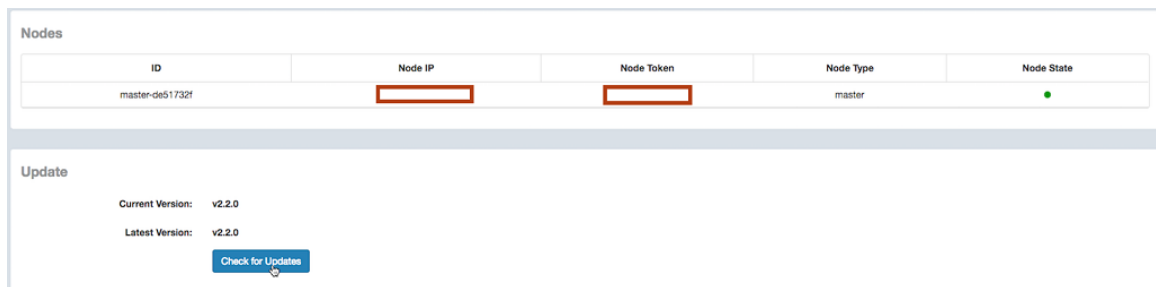
- s3-us-west-2.amazonaws.com
- 484213038011.dkr.ecr.us-west-2.amazonaws.com

1. From the SCI dashboard, click **Admin > Status & Update**.

The **Status & Update** page appears.

2. Click **Check for Updates**.

FIGURE 31 Updating software



It takes up to 10 minutes to update the software package.

Updating the Software Package by Downloading it

You can also update the SCI software by downloading the updated software package if you are not connected to the internet.

Follow these steps to update the software by downloading the software package:

1. Download the updated software package from the Ruckus Wireless support web site.
2. Upload the software package to the Master Node location: /storage/updates directory.

Updating the SCI Software

Updating the Software Package by Downloading it

3. From the Master node, run the command: `sudo docker exec -it rsa-cluster-manager bin/rake rsa_cluster_manager:software_update:from_package[software_update_package_file_name]`, where **software_update_package_file_name** is the name of the updated software package file (without the parent directories) uploaded in the previous step.

It takes up to 10 minutes to exclusively update the software package (not counting the time to upload or download the software).

Managing Licenses

- Trial License..... 55
- Upgrading to the SCI License..... 55

SCI supports a trial license which you can use to familiarize with the product, and also supports a permanent SCI license.

Trial License

SCI is provided with a built-in trial license. You can upgrade to the SCI license before the trial period ends.

- Is valid only for 90 days
- Does not limit the number of controllers or APs supported by SCI
- Must be upgraded to a SCI license within the validity period of the trial license
- Does not allow you to view reports after the validity period ends

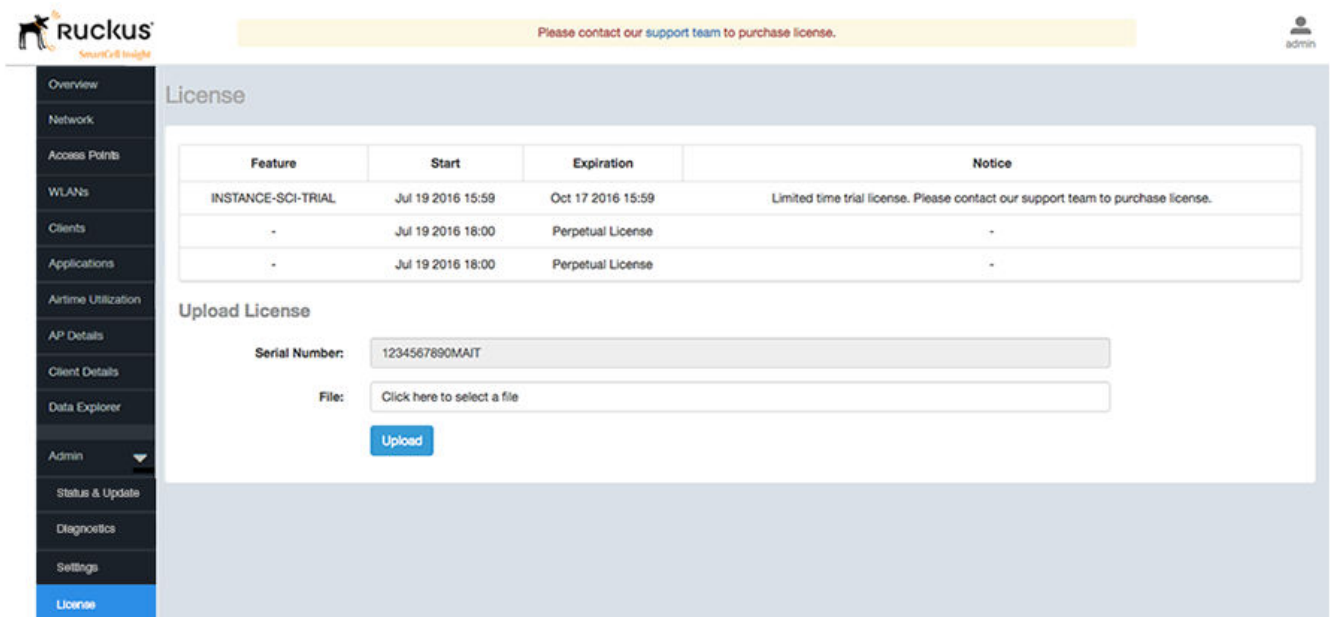
Upgrading to the SCI License

After using SCI with the trial license, make sure that you upgrade to the permanent SCI license in order to benefit from the product.

Follow these steps to upgrade to the SCI license:

1. In the SCI web UI, click **Admin > License**.
The **License** page appears.

FIGURE 32 License page



Managing Licenses

Upgrading to the SCI License

2. Use the Serial Number shown here to activate your license.
3. Click **File**, to upload the license file that you have downloaded from the Ruckus Support website.
4. Click **Upload**.

NOTE

The number of AP licenses uploaded should at least be equal to, or more than the total number of active APs connected to the controllers which are configured in SCI.

Migration from SCI 1.x

- Prerequisites.....57
- Migration Procedure..... 58
- Monitor the Migration Process..... 59

This section describes how you migrate existing data from SCI 1.x to SCI 3.6.0.

As SCI 3.6.0 is built on a different software stack from SCI 1.x series, if there is a need to migrate existing data from SCI 1.x to SCI 3.6.0, a full migration of raw data files with complete re-aggregation of data sources is required. However, do note that data migration is not necessary for the upgrade from SCI 1.x to SCI 3.6.0. Before you start migration, ensure that you have the following pre-requisites and setup.

NOTE

This self-service migration feature has been tested to the best of our ability. However, we may not have covered all cases since it is highly dependent on the environment and SCI 1.x setup . If you have issues during migration, do contact Ruckus Wireless Support at <https://support.ruckuswireless.com/contact-us>.

NOTE

The migration process can take several hours per month of data, based on data volume and time span.

NOTE

Migration of data from SCI 1.4 is currently supported only for Smart Zone(SZ) data.

Prerequisites

Before you start migration, ensure that you have the following prerequisites.

1. SCI 1.4 is installed. Earlier versions of SCI 1.x should first be upgraded to SCI 1.4 before starting the migration process.
2. SCI 3.6.0 is installed.
3. SCI 3.6.0 requires a higher storage capacity - 4 times higher than the raw data in SCI 1.x version in order to be fault tolerant. Adequate storage requirements are necessary before you begin migration.
4. The system for which migration is to be performed is added to the SCI 3.6.0 instance in the **Admin > Settings** section. Ensure that the system name in SCI 3.6.0 matches the name of the system that is being migrated.
5. **Optional:** You can add more data nodes to the SCI 3.6.0 cluster if you want the migration to be faster.

NOTE

- Application report is not supported in SCI 1.x version.
- Migration of ZoneDirector data is not supported.
- Migration can only be performed for one system at a time.
- Time required for migration is dependent on the number of controllers, number of APs, number of days of data to be migrated, and the server resources allocated to the migration cluster.

Migration Procedure

Follow the steps below to successfully migrate from SCI 1.x to SCI 3.6.0.

1. Download the file *migrate.tar.gz* from the support website <https://support.ruckuswireless.com/>. Copy the tar file to the SCI 3.6.0 VM and run the following command: (You can create any directory on the SCI 3.6.0 VM in which to place the tar file; make note of this directory for future reference).

```
tar xvzf migrate.tar.gz
```

This command will create the following scripts in the current directory.

1. step-1-tar.sh
 2. step-2-scp.sh
 3. step-3-list.sh
 4. step-4-migrate.sh
 5. step-5-cleanup.sh
2. Copy the script *step-1-tar.sh* to the SCI 1.4 VM. (You can create any directory on the SCI 1.4 VM in which to place the script; make note of this directory for future reference).
 3. On **SCI 1.4 VM** run the following command to prepare the system data for migration.

```
sudo sh step-1-tar.sh <SCI1.4-System-Name>
```

NOTE

System-Name is the **SCI System Name** as configured in the SCI 1.4 user interface.

This command generates the following tar file, which contains the data for the system in a compressed format.

```
/opt/ruckuswireless/sci/sci1data.tar
```

4. In the SCI 3.6.0 user interface, go to **Admin > Settings**, then configure a controller with a **System ID** that is exactly the same as the *System-Name* that you specified in the previous step.

NOTE

This System ID is the unique identifier for this controller between 1.4 and 3.6.

5. On SCI 3.6.0 VM, run the following command to copy the file from SCI 1.4 VM. If you are prompted for a username and password, provide the credentials for the SCI 1.4 login.

```
sudo sh step-2-scp.sh <SCI1.4-System-Name>
```

6. On SCI 3.6.0 VM, use the following command to list the dates for which data is available.

```
sudo sh step-3-list.sh <SCI1.4-System-Name>
```

7. On completion of the above step, all the dates for which data is available for migration from SCI 1.4 is listed in the file whose absolute path is: */storage/rsa-master/logs/migration/dates.txt*.

Optional: If you wish to migrate data only for a select period, delete the lines from this file for dates which do not have to be migrated. For example, if the system has data from 2014 to 2016 and only 2016 data is required, then all the lines containing */2014/* and */2015/* should be deleted from the file.

NOTE

If you already have a running instance of SCI 2.x, which is collecting data for the system, do delete the overlapping dates from the *dates.txt* file before proceeding with the migration. Otherwise, there will be duplicated data for the overlapping period.

8. Once the *dates.txt* is ready, start the migration process by running the following command on SCI 3.6.0 VM

```
sudo sh step-4-migrate.sh <SCI 3.6.0-System-ID>
```

NOTE

Ensure that the **System ID** in SCI 3.6.0 matches the **System Name** that is being migrated from version 1.4.

9. When the migration is complete, and you have verified that all data is in the new SCI, run this step to clean up all temporary files created by the migration process:

```
sudo sh step-5-cleanup.sh
```

Monitor the Migration Process

To monitor the progress of the migration job, view the log file `/storage/rsa-master/logs/migration/spark.stdout`. Detailed spark logs are available at <https://< SCI 3.6.0 VM IP:58080/> and indexing logs at <https://< SCI 3.6.0 VM IP>:58090>

The migration process can take several hours per month of data, based on data volume and time span.

To verify that the migration has completed successfully, review the following:

- The last line of the log file (`/storage/rsa-master/logs/migration/spark.stdout`) should read as **Completed Migration**.
- Indexing logs have no entries in **Running Tasks**
- Data is available in SCI 3.6.0 reports.



Copyright © 2018 Ruckus Networks, an ARRIS company. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com