SOFTWARE INSTALLATION GUIDE

Ruckus Wireless™ SmartCell Insight™ Installation Guide

Supporting SmartCell Insight™ 3.1.0

Part Number: 800-71650-001
Publication Date: 21 July 2017

Copyright Notice and Proprietary Information

Copyright 2017. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. (“Ruckus”), or as expressly provided by under license from Ruckus.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Document....5
Overview....5
Document Conventions....5
Related Documentation....6
Documentation Feedback....6
Before You Begin....7
System Requirements....7
Minimum Hardware Requirements....7
Guidelines for Setting Up Data Nodes....8
Storage Requirements....8
Minimum Software Requirements....9
DHCP Server Requirements....9
NTP Server Requirements....9
Compatibility Matrix....11
Compatibility Matrix....11
Installing SCI....13
Installation Overview....13
Setting Up the Virtual Machine Using VMware ESXi....14
Setting Up the Virtual Machine Using AWS....16
Setting Up the Virtual Machine Using a Static IP Address....18
Setting Up the Virtual Machine Using KVM QCOW2....21
Setting Up the Virtual Machine Using GCE....22
Setting Up the Nodes....23
Firewall Rules....25
Web API Setup....25
Installing Custom SSL Certificate....26
Secure Shell Access to SCI....26
Configuring SCI....29
Configuring SMTP....29
Managing Controllers....30
Editing Controllers....34
Enabling AP SCI Statistics Delivery on SmartZone 3.2 Controllers....36
Enabling AP SCI Statistics Delivery on SmartZone 3.4 Controllers....36
Configuring the Controller....39
Configuring Controllers from the Web UI....39
Configuring SCI Settings for:....39
Updating the SCI Software....43
Updating the Software from the Cloud....43
Updating the Software Package by Downloading it....43
Managing Licenses....45
Trial License....45
Upgrading to the SCI License....45

Migration from SCI 1.x....47
Prerequisites....47
Migration Procedure....48
Monitor the Migration Process....49

About This Document

- Overview 5
- Document Conventions 5
- Related Documentation 6
- Documentation Feedback 6

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..... 7
- DHCP Server Requirements..... 9
- NTP Server Requirements..... 9

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.

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

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	Number of Master Nodes	ZD / SZ version 3.4 or lesser	SZ version 3.5 or later
0	1	3,000	1,000
1	1	10,000	3,000
2	1	20,000	6,000
3	1	30,000	9,000
4	1	40,000	12,000

NOTE
For SmartZone 3.4 and below, add an additional Data node for every additional 10,000 APs. For SmartZone 3.5 and above, add an additional Data node for every additional 3,000 APs.

NOTE
Data granularity has been increased by up to 90-sec 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.

Storage 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 lesser	SZ version 3.5 or later
per day per 1,000 APs	1 GB	3 GB

The storage requirements in SCI release 2.5 have increased due to the increase (5 times) in KPIs and data granularity to 5 min versus 15 min in previous SCI releases. However, if you want to control the storage and fallback to a data granularity of 15 min like releases prior to SCI 2.5, you must issue the CLI command:

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

By using this command, you can modify the rate at which APs display their status reports. To slow down the rate set to a maximum of 900 seconds, and to speedup set to a minimum of180 seconds.

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 of DHCP, see Setting Up the Virtual Machine Using a Static IP Address on page 18 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 26

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.....11

Compatibility Matrix

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

TABLE 8 Compatibility Matrix

SCI Release	SmartZone (controller) Release		ZoneDirector (controller) Release
Version	Version 3.4 or lower	Version 3.5 or higher	• 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

Installing SCI

- Installation Overview....13
- Setting Up the Virtual Machine Using VMware ESXi....14
- Setting Up the Virtual Machine Using AWS....16
- Setting Up the Virtual Machine Using a Static IP Address....18
- Setting Up the Virtual Machine Using KVM QCOW2 21
- Setting Up the Virtual Machine Using GCE....22
- Setting Up the Nodes....23
- Secure Shell Access to SCI....26

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 7. 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 14 or Setting Up the Virtual Machine Using AWS on page 16.

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 14 or Setting Up the Virtual Machine Using AWS on page 16.

   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 23.

4. Activate the Master node.

   For more information, see Setting Up the Nodes on page 23.

5. Set up the Data node.

   For more information, see Setting Up the Nodes on page 23.

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.

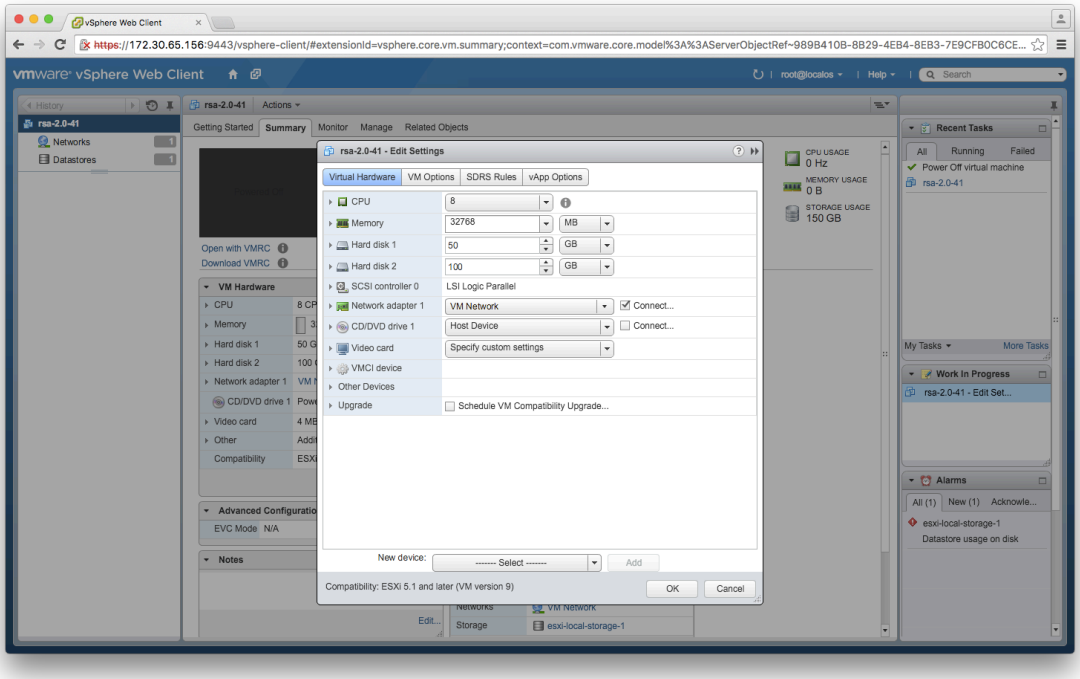
Follow these steps to install and configure the VM:

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

2. 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 7.

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 18 for more information.

3. 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.

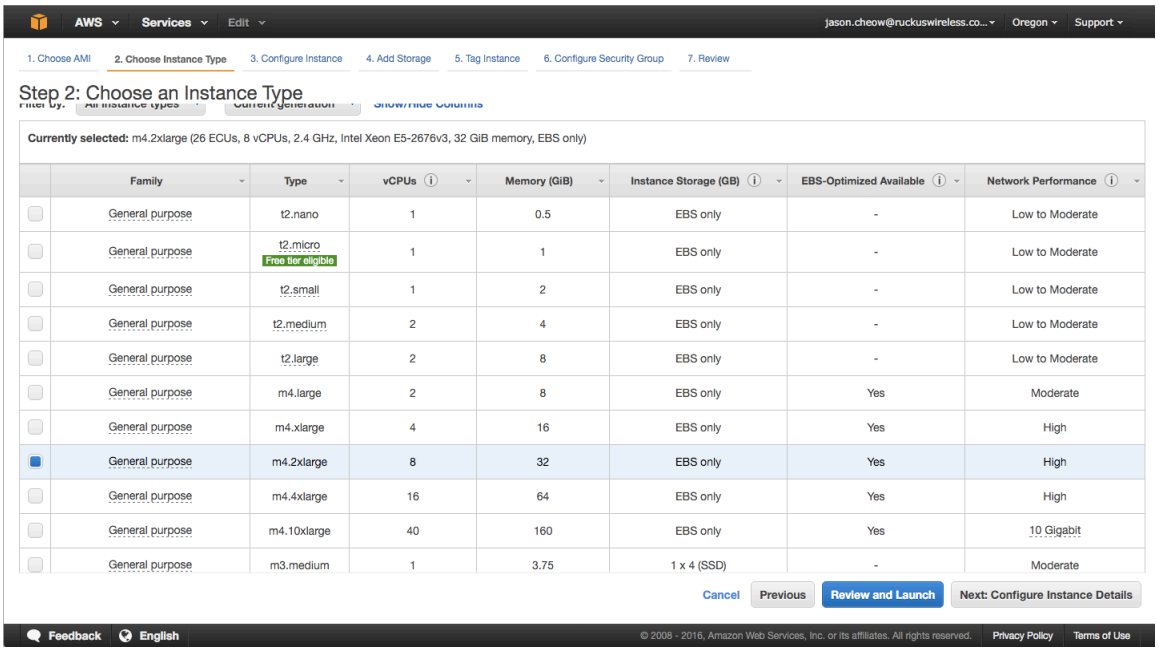
Contact Ruckus Wireless customer support and provide your AWS account ID, so that the company can share the SCI private AMI (Amazon Machine Image) number with you. For more information regarding AWS accounts IDs, see http://docs.aws.amazon.com/general/latest/gr/acct-identifiers.html.

Follow these steps to install and configure the VM:

1. Based on the instructions in http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingsharedamis-finding.html, find the AMI and launch a VM instance.
2. 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



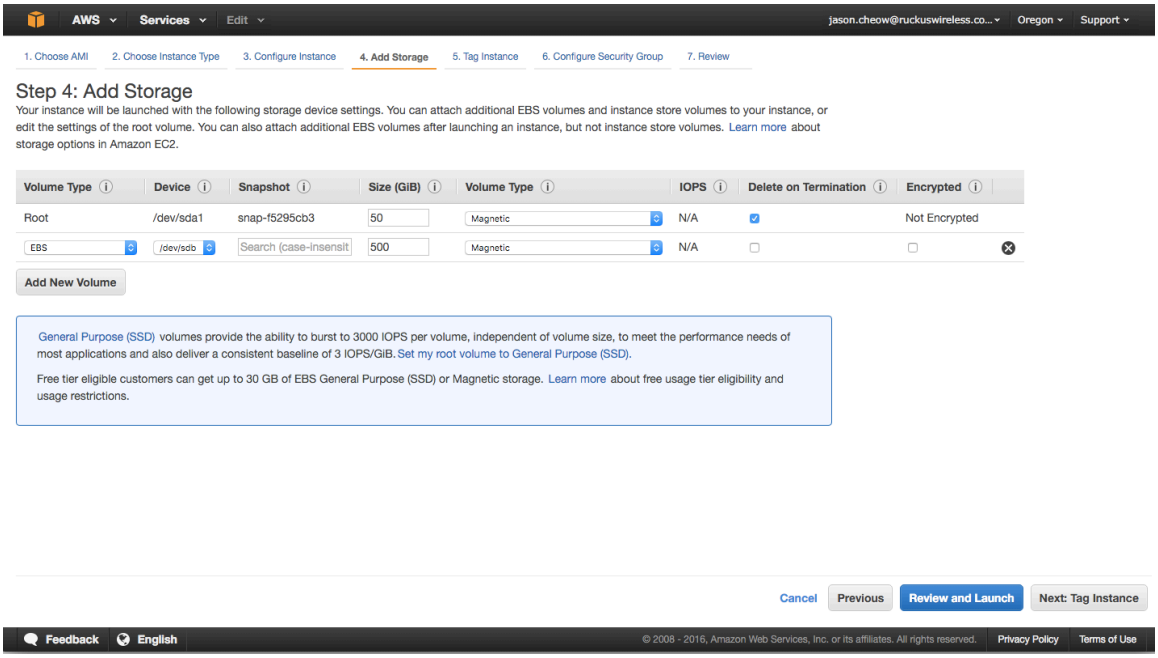
3. Configure the instance you have chosen based on your requirements.

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 the set the static IP address, and **Normal Boot** to start SCI.

2. Select **Network Manager TUI**.

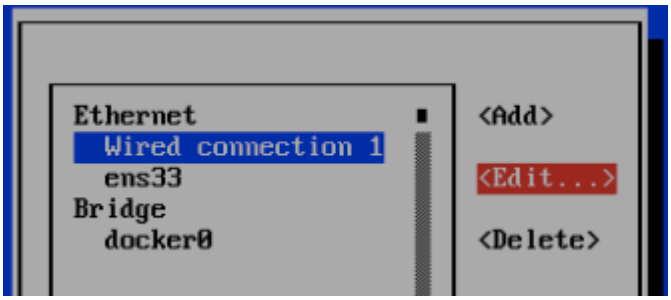
   The **Network Manager TUI** screen appears.

FIGURE 5 Network Manager TUI screen

3. Select **Edit a connection**.
4. Press **Enter**.

   The following screen appears.

FIGURE 6 Selecting a wired connection

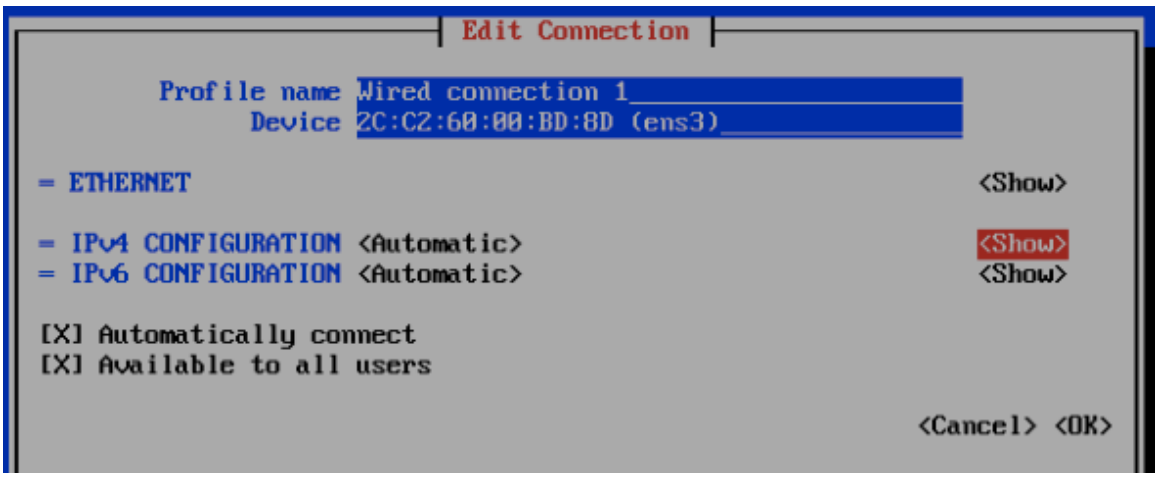


5. Select **Wired Connection 1**, or the default wired connection.

6. Select **Edit**.

   The **Edit Connection** screen is displayed.

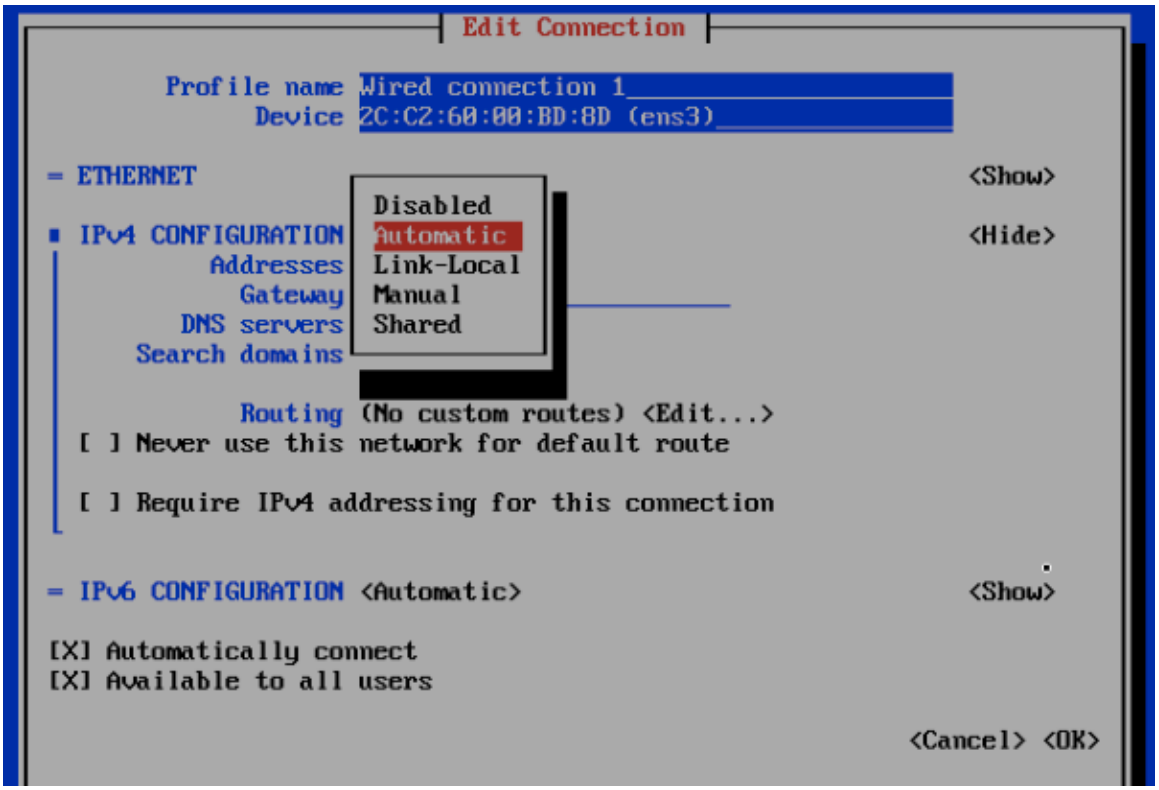
FIGURE 7 Edit connection



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

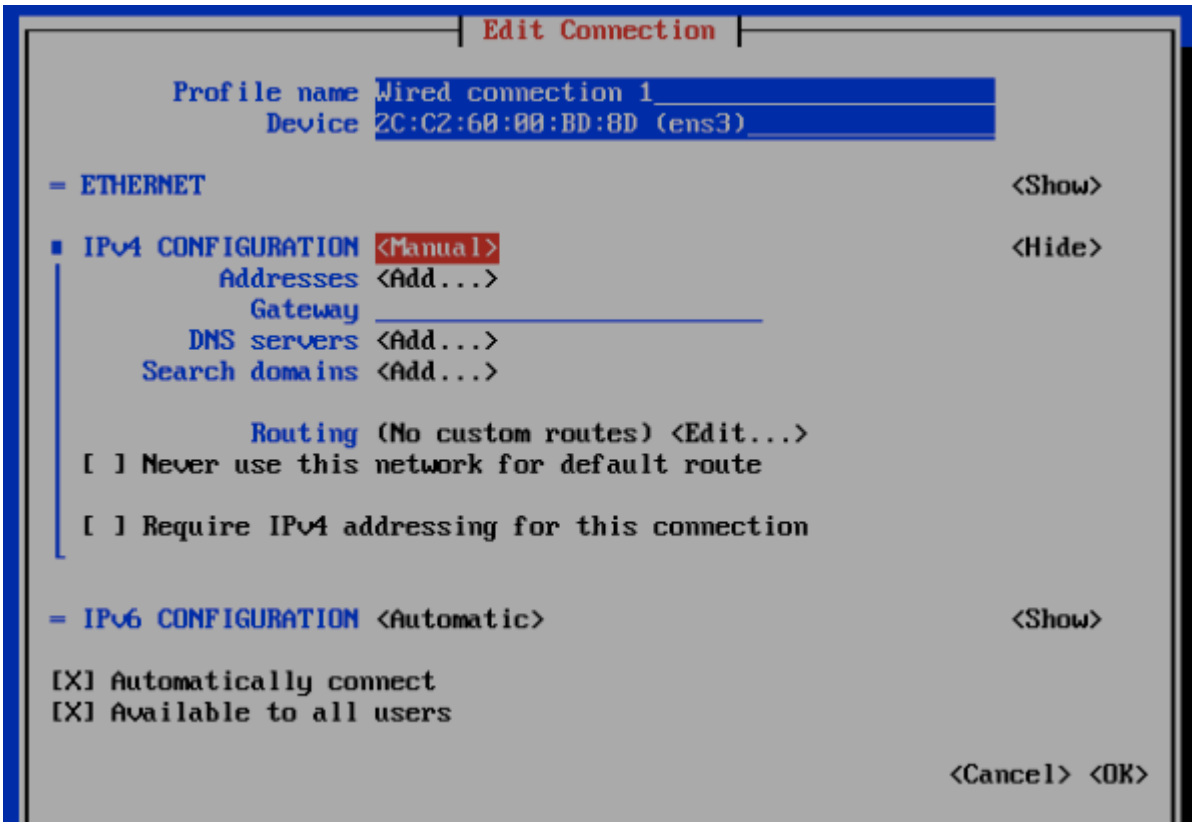
   The following screen appears.

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.

Before you start and stop a RSA VM ensure that:

- The CPU, HDD and memory requirements under the Minimum Hardware Requirements on page 7 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 *Virtulaization 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 7.

   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 **vrish** 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/ruckussgdc-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/ruckussgdc-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.

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:

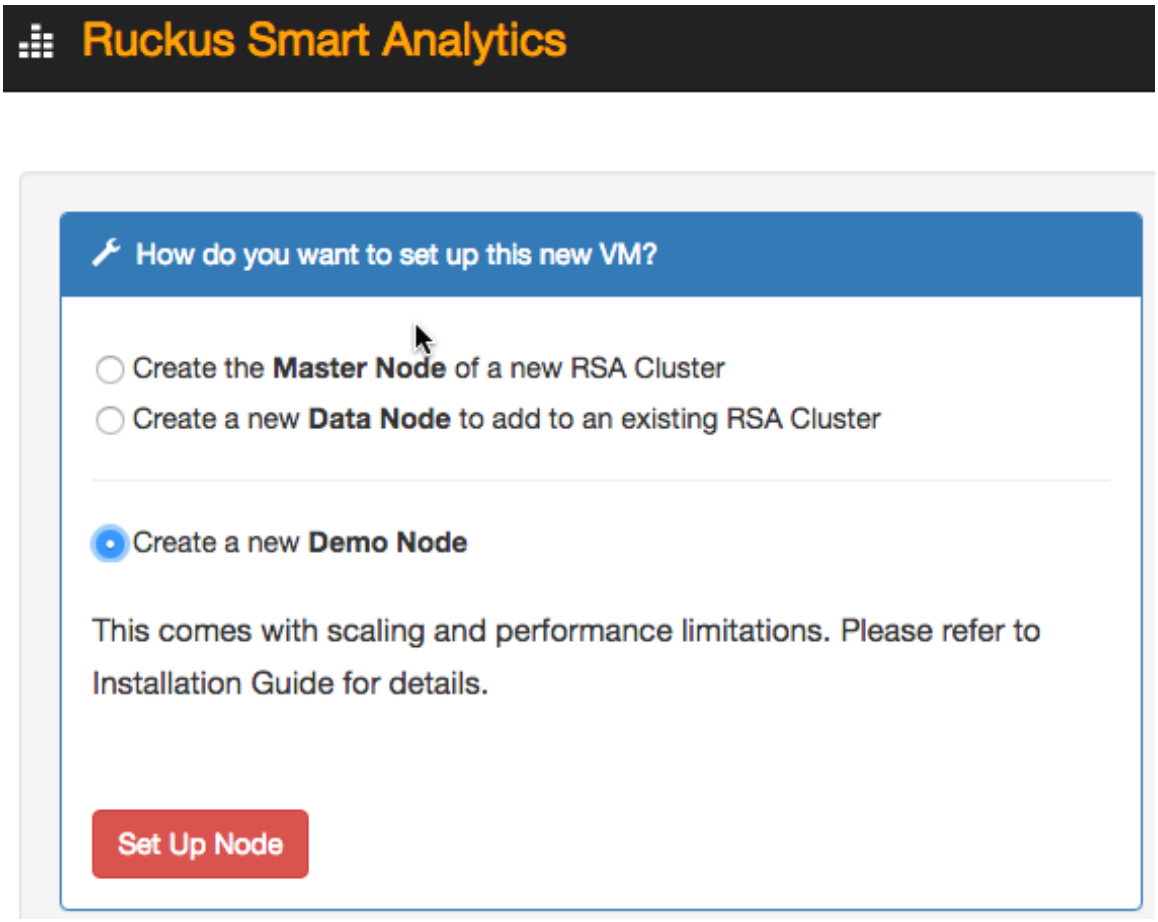
1. Launch a web browser and browse to the SCI set up page (https://<SCI IP address or domain name>).

   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 10 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.

5. 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 25

6. 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 9 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	22	443	53000, 55070, 58090, 58081, 58080, 59090
Protocol	HTTPS	SSH	HTTPS	HTTPS
Traffic Direction	Incoming traffic to SCI	Incoming traffic to SCI	Outgoing traffic from SCI	Incoming traffic to SCI

TABLE 10 Firewall rules for Controller Access

	SmartZone AP Stats (JSON)	SmartZone AVC Data	ZoneDirector Pull (XML)	ZoneDirector Push (XML) ZD 9.13 and above
From	SCI Master Node IP and Data Node IPs	SmartZone IP	ZoneDirector IP	SCI Master Node IP and Data Node IPs
To	SmartZone IP	SCI Master Node IP and Data Node IPs	SCI Master Node IP and Data Node IPs	ZoneDirector IP
Port Number	8443	1883 and 8883	443	443
Protocol	HTTPS	MQTT	HTTPS	HTTPS
Traffic Direction	Outgoing traffic from 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 Table 7 and 8 are opened, and the rest of the ports are closed by the firewall.

TABLE 11 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

Web API Setup

You can setup the nodes using API calls.

You must issue the first API call to set up the VM as a Master node, Data node or Demo node. The response to this call (JSON response) contains information about the node_type, node_ip and node_token.

Issue the second API call to activate the node. There is no response for this call.

> **NOTE**
> As the process of activation shuts down the Set Up web application, you may receive a HTTP read error from the curl request. Ignore this message.

Master Node

- curl -k -H "Content-Type: application/json" -X POST -d '{"node": {"node_type": "master"}}' https://[SCI IP or domain name]/nodes
- curl -ks -X PUT https://[SCI IP or domain name]/nodes/master/activate

Data Node

- curl -k -H "Content-Type: application/json" -X POST -d '{"node": {"node_type": "data", "data_node_master_ip": "[Cluster's Master Node IP]", "data_node_master_token": "[Cluster's Master Node Token]"}}' https://[SCI IP or domain name]/nodes
- curl -k -X PUT https://[SCI IP or domain name]/nodes/data/activate

Demo Node

- curl -k -H "Content-Type: application/json" -X POST -d '{"node": {"node_type": "demo"}}' https://[SCI IP or domain name]/nodes
- curl -ks -X PUT https://[SCI IP or domain name]/nodes/demo/activate

Installing Custom SSL Certificate

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.

Be sure that you have the following files:

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

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.

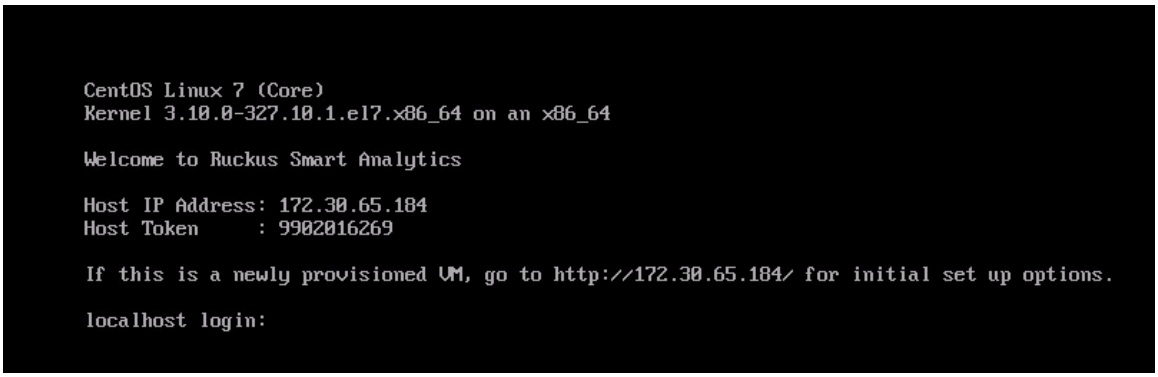
   This information is also available in the **Admin** > **Status & Update** page, within the **Ruckus Smart Access** interface.

2. 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 11 Sample SSH screen



Configuring SCI

- Configuring SMTP..... 29
- Managing Controllers..... 30

After the nodes in the SCI cluster are setup and activated, SCI must be configured. You must add controllers for SCI to monitor and collect data. The SCI dashboard is populated with reports and trends after the controllers are added.

After SCI setup, you can login 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 and controller settings.

Configuring SMTP

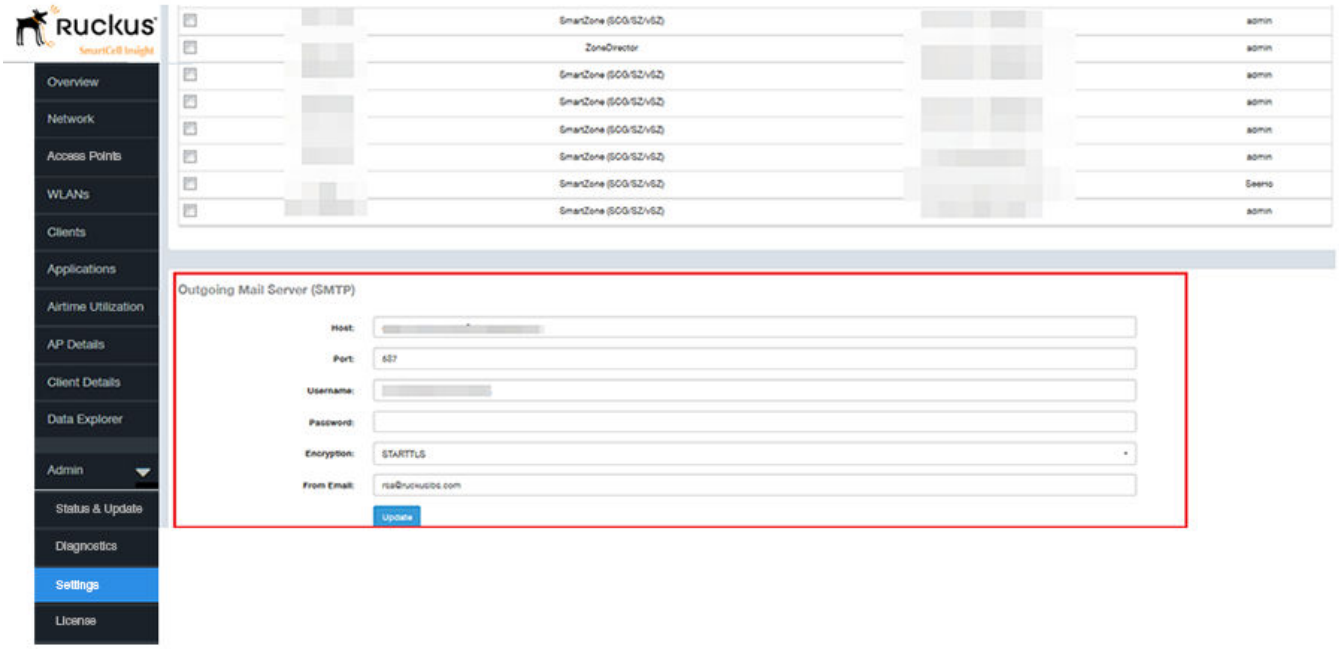
You can configure the SMTP mail server to receive scheduled reports from SCI by e-mail.

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

1. **Admin** > **Settings**

   The **Settings** page appears with options to configure the SMTP settings.

FIGURE 12 SMTP configuration



2. Configure the following information:
   - Host: type the name/IP address of the host
   - Port: type the port number
   - Username: type the user name to access the SMTP mail server
   - Password: type the password to access the SMTP mail server
   - Encryption: from the drop-down menu, select **Enable** to encrypt the e-mail, and **Disable** if you do not want to encrypt the e-mail.
   - From Email: type the e-mail address from which the e-mail is to be sent
3. Click **Update**.

The SMTP configuration is updated.

Managing Controllers

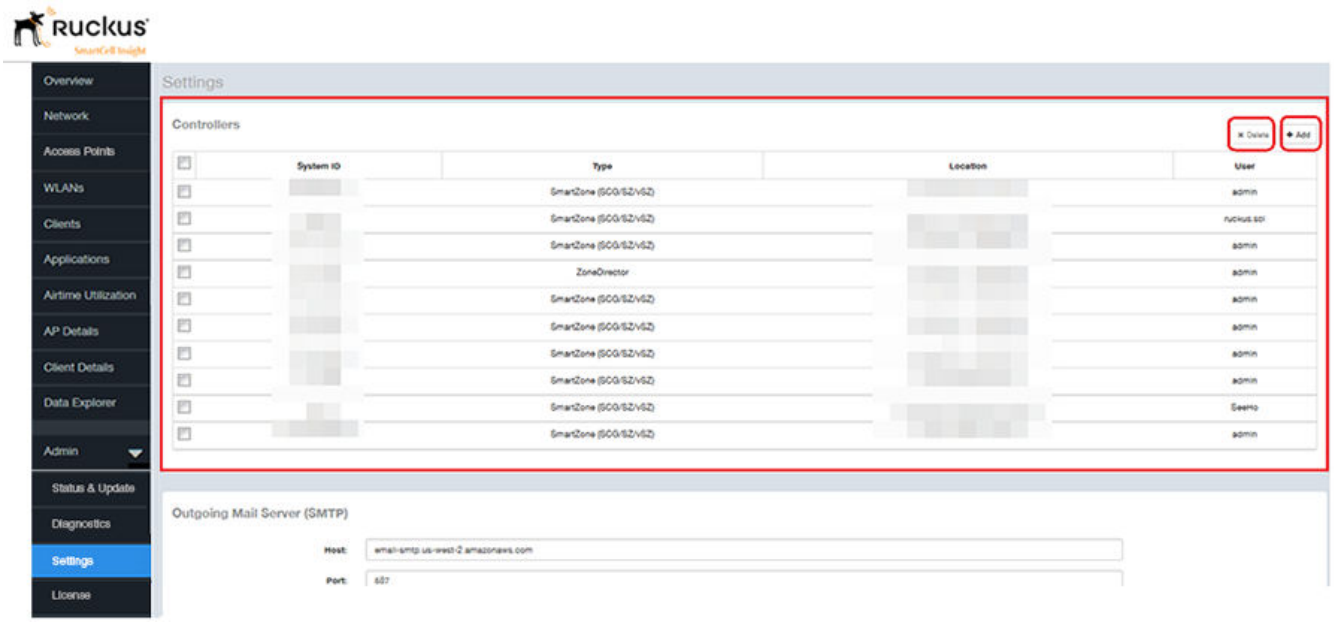
You must add controllers to SCI to monitor and manage them. SCI analyzes data from the controller and provides information about the WiFi network performance.

Follow these steps to add a controller:

1. From the SCI dashboard, click **Admin** > **Settings**.

   The **Settings** page appears with options to manage controllers.

FIGURE 13 Adding and deleting controllers



2. In **Controllers**, click **Add**.

   The **New Controller** dialog box appears.

   For example, you could add a ZoneDirector or SmartZone controller to monitor and manage through SCI. Examples to add ZoneDirector, SmartZone 3.4 and SmartZone 3.5 controllers are shown.

   ATTENTION

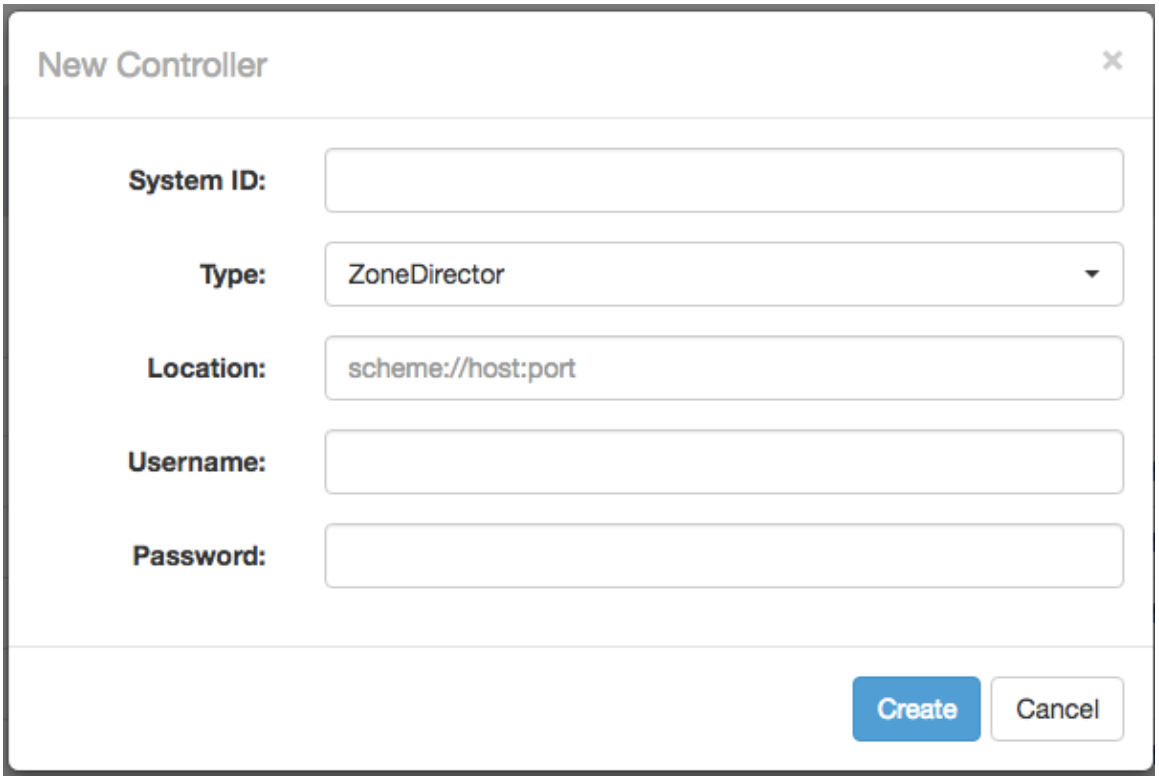
   ZoneDirector uses port 443 and SmartZone controllers use port 8443. For example,

   - ZoneDirector URL: https://myzd.mycompany.com:443 or https://192.168.10.26:443
   - SmartZone controller URL: https://myscg.mycompany.com:8443 or https://192.168.20.45:8443

Adding ZoneDirector

If you add a ZoneDirector, you will see the following screen.

FIGURE 14 New controller information - ZoneDirector

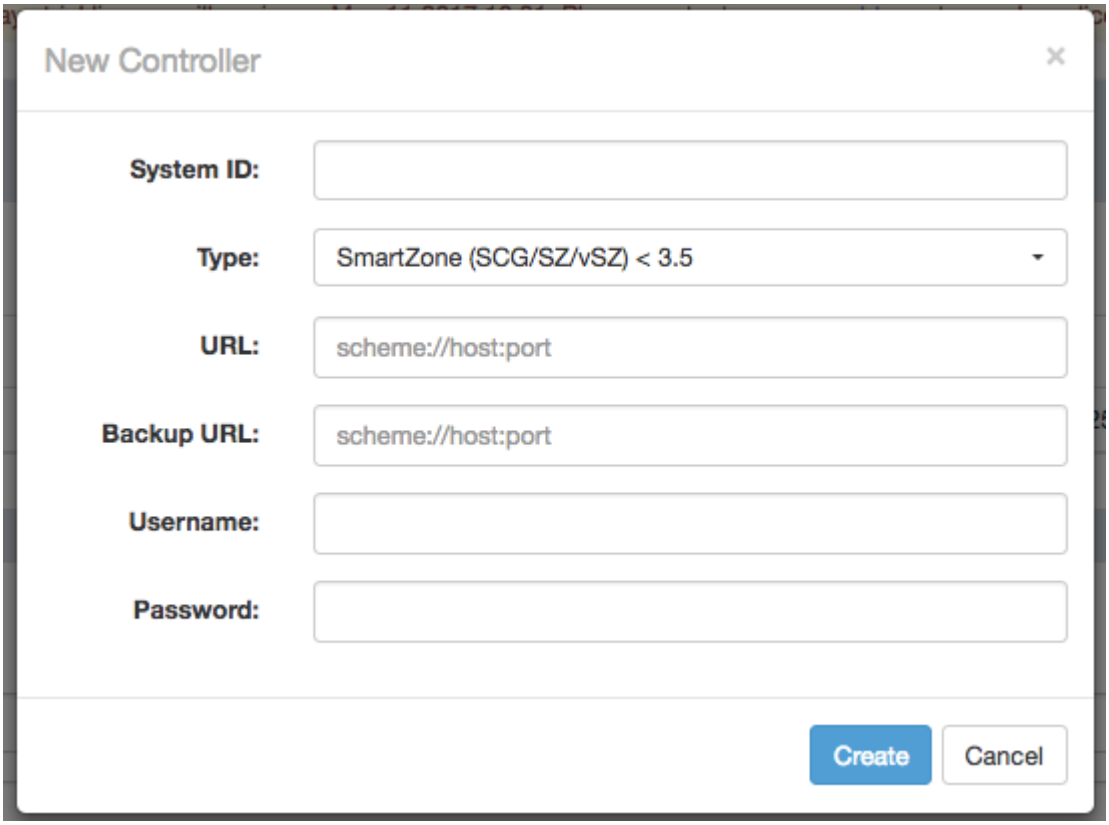


ADDING SmartZone 3.4 CONTROLLER

NOTE

If you add a SmartZone cluster running version 3.4 or below, you will see the following screen. You can provide a backup location for SCI to connect to it if it is not able to connect to the default location.

FIGURE 15 New controller information - SmartZone 3.4 controller



Configure the following controller settings:

- System ID: type the name of the controller you want to add to SCI

  NOTE
  The controller name should be unique and cannot be changed.

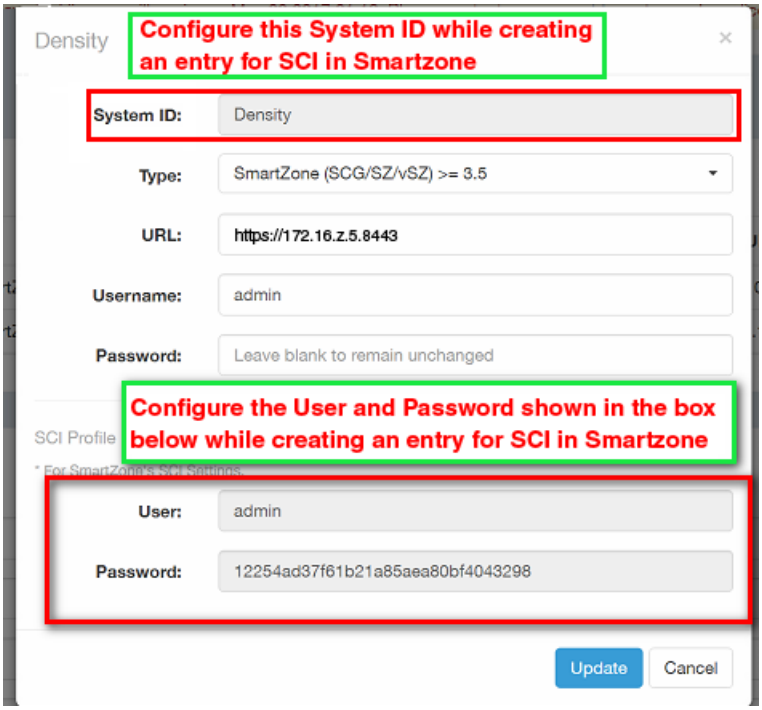
- Type: select the controller type from the drop-down menu
- URL: type the URL of the controller
- Backup URL: type the URL of the backup controller location
- Username: Type the administrator username to access the controller.
- Password: Type the administrator password to access the controller.

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

ADDING SmartZone 3.5 CONTROLLER

NOTE
If you have a SmartZone cluster running version 3.5 or above, you will see the following screen. The figure below includes important information about fields in this screen that must be identical to fields in the Add/Edit SCI Profile screen of the Controller Web UI.

FIGURE 16 New Controller screen - SmartZone 3.5



The System ID field and the two fields under "SCI Profile" (User and Password) in the screen above must be identical to the fields of the same name in the Add (or Edit) Profile screen of the Controller Web UI Systems > General Settings > SCI area, as indicated in the figure below.

See Configuring Controllers from the Web UI on page 39 for more information about configuring controllers from the Web UI.

The following is a complete list all the fields that you must configure in the SCI New Controller 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 two figures above, this field must be identical between the SCI New Controller screen and the Add/Edit SCI Profile of the Controller Web UI.

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

- Type: Select the controller type from the drop-down menu
- URL: Enter the URL of the controller.
- Username: Enter the administrator username to access the controller.

  NOTE
  The Username provided should be the same as the user name used to access the SmartZone UI.

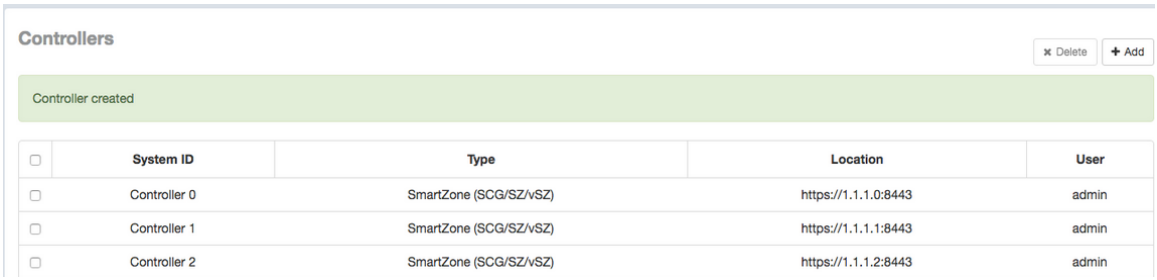
- Password: Enter the administrator password to access the controller.
- **SCI Profile:** Enter the User and Password login credentials to access the SCI profile. These login credentials are different from the administrator credentials above. As shown in the two figures above, the two SCI Profile fields must be identical between the SCI New Controller screen and the Add/Edit SCI Profile of the Controller Web UI.

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

3. Click **Create**.

   The new controller is listed under the **Controllers** section of the **Settings** page, and a confirmation message is displayed.

FIGURE 17 New controller is added



You have successfully added a controller for SCI to monitor.

You can delete a controller by selecting it from the **Controllers** section, and clicking **Delete**.

NOTE
The delete operation is irreversible. However, the controller with the same details can be added again.
Deleting a controller does not remove its data from the reports.

Editing Controllers

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.

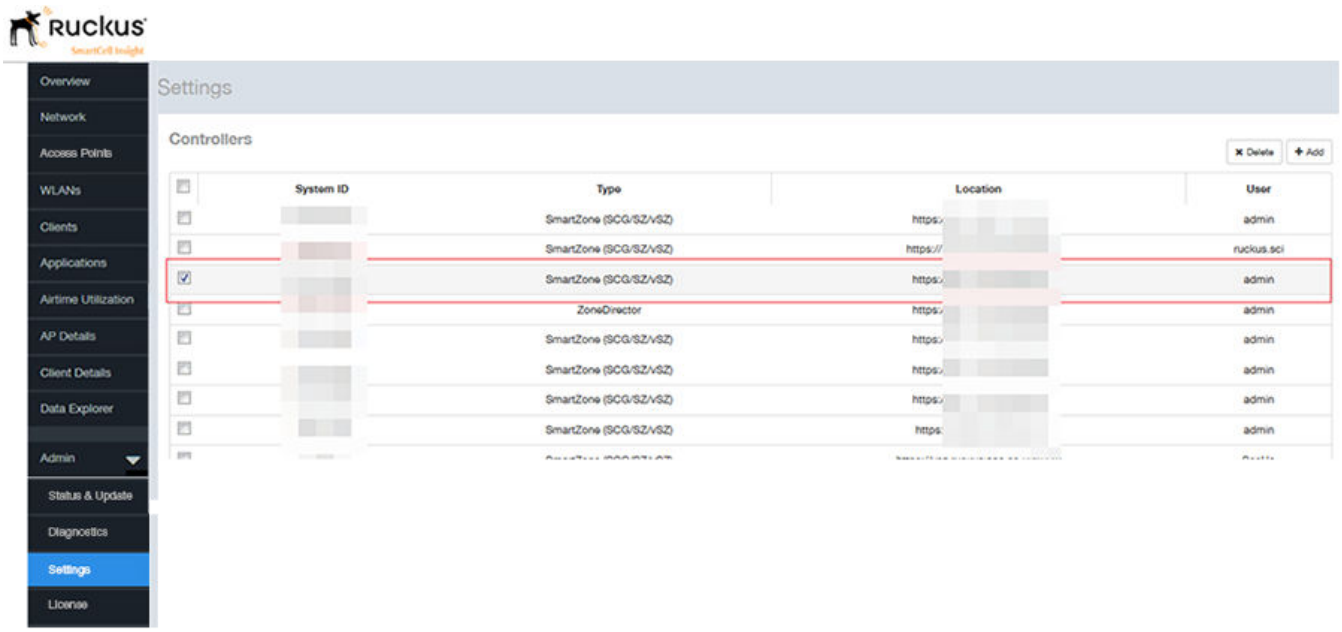
Follow these steps to edit the controller's information:

1. From the SCI dashboard, click **Admin** > **Settings**.

   The **Settings** page appears.

2. Identify the controller that you want to edit, and select the appropriate check-box as shown.

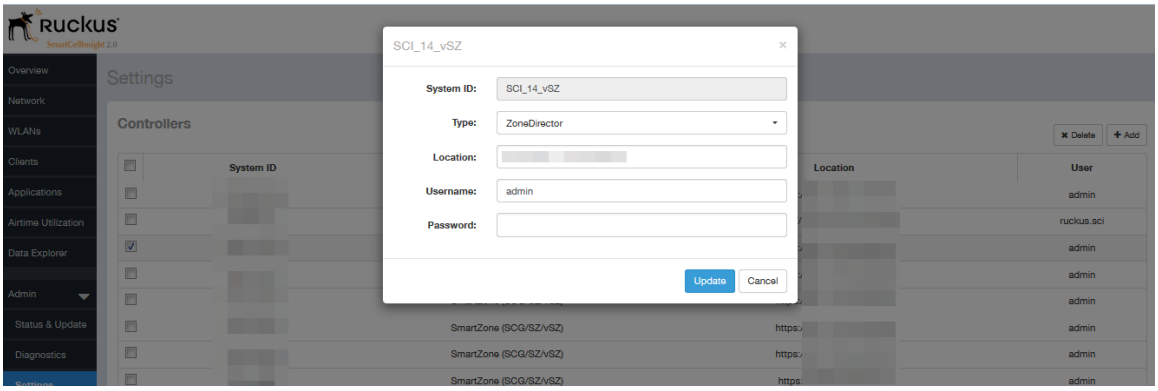
FIGURE 18 Selecting the controller



3. Click the controller row.

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

FIGURE 19 Editing controller information



4. Click **Update**.

You have successfully edited the controller's information.

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.

For SmartZone version 3.4, see Enabling AP SCI Statistics Delivery on SmartZone 3.4 Controllers on page 36. 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 Adresses must be whitelisted 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 36. 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 Adresses must be whitelisted on the controller for SCI to pull data from the controllers.

Configuring the Controller

- Configuring Controllers from the Web UI.....39

To understand the performance trends of a controller, you must add the controller to SCI and configure its SCI settings to monitor it.

Configuring Controllers from the Web UI

After a controller is added to the SCI cluster for monitoring, you must configure the SCI settings of the controller from the controller's web UI.

Configuring SCI Settings for:

SmartZone 3.4 controller

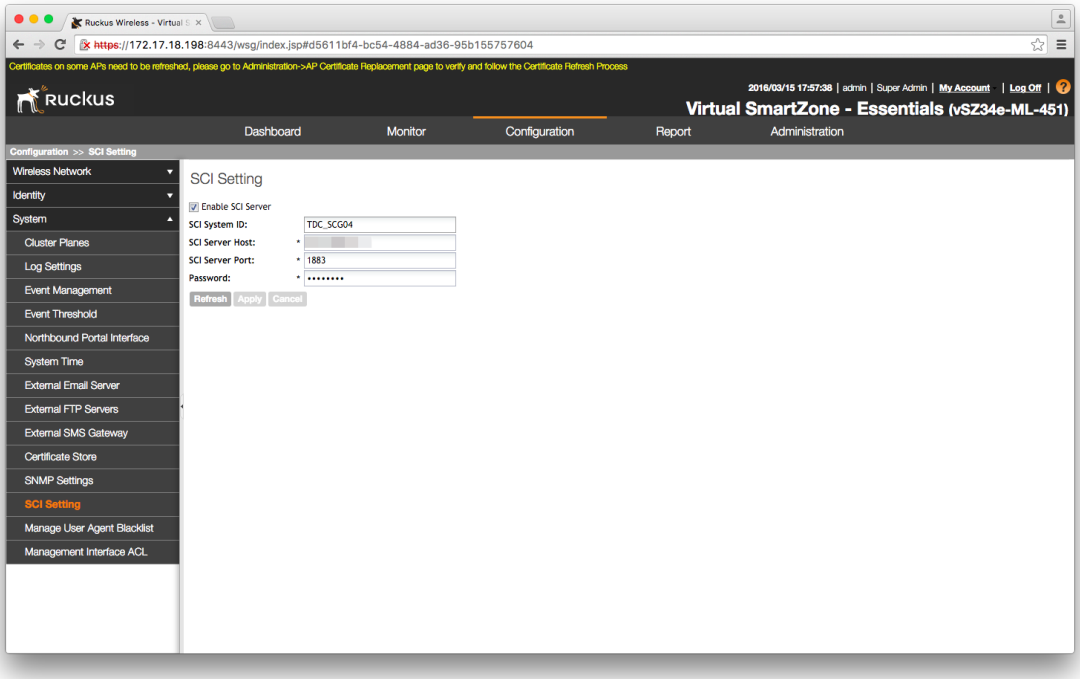
Follow these steps to modify the SCI settings from the controller web UI:

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

   The **SCI Setting** page appears.

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

FIGURE 20 SmartZone 3.4 SCI settings page



2. Select the **Enable SCI Server** check-box.
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.

SmartZone 3.5 controller

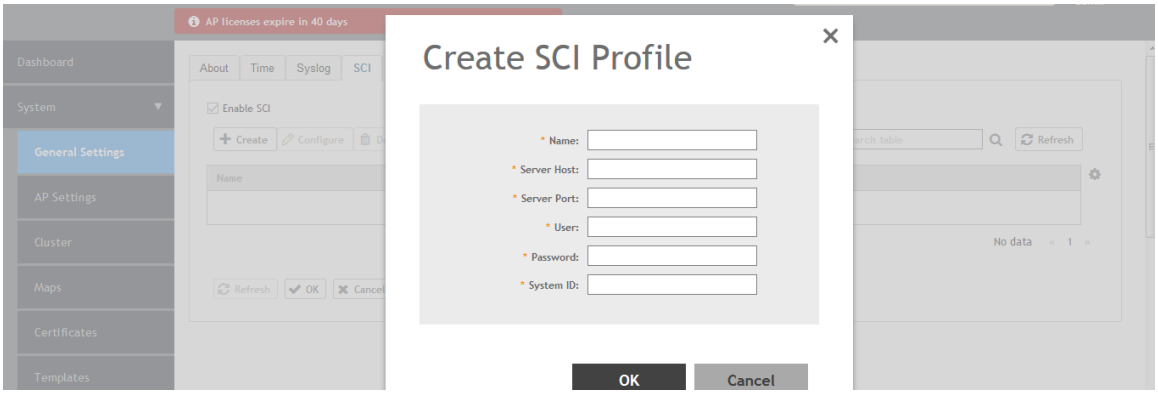
Follow these steps to modify the SCI settings from the controller web UI:

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 21 SmartZone 3.5 SCI settings page



2. Select the **Enable SCI** check-box.
3. Click **Create** to create a new SCI profile.

   The **Create SCI Profile** page 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.
   - SCI Server Host: Type the SCI IP address or the domain name.
   - SCI Server Port: Set to 8883.
   - User: Set this to the "User" field displayed under **SCI Profile** of the **Adding Controllers** section.
   - Password: Set this to the "Password" field displayed under **SCI Profile** of the **Adding Controllers** section.
   - System ID: Set this to the same unique name that was used in the **Adding Controllers** section.
5. Click **OK**.

You have completed configuring the SCI server settings on the SmartZone 3.5 controller.

Updating the SCI Software

- Updating the Software from the Cloud.....43
- Updating the Software Package by Downloading it..... 43

Updating the Software from the Cloud

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

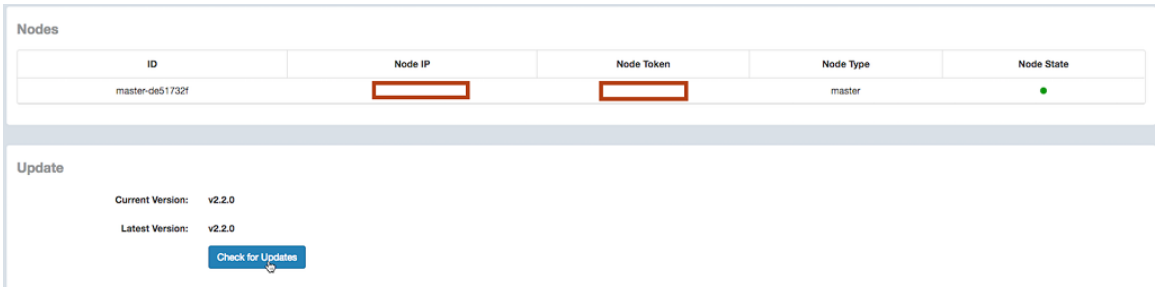
Follow these steps to update the software from the cloud:

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

   The **Status & Update** page appears.

2. Click **Check for Updates**.

FIGURE 22 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.
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..... 45
- Upgrading to the SCI License..... 45

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

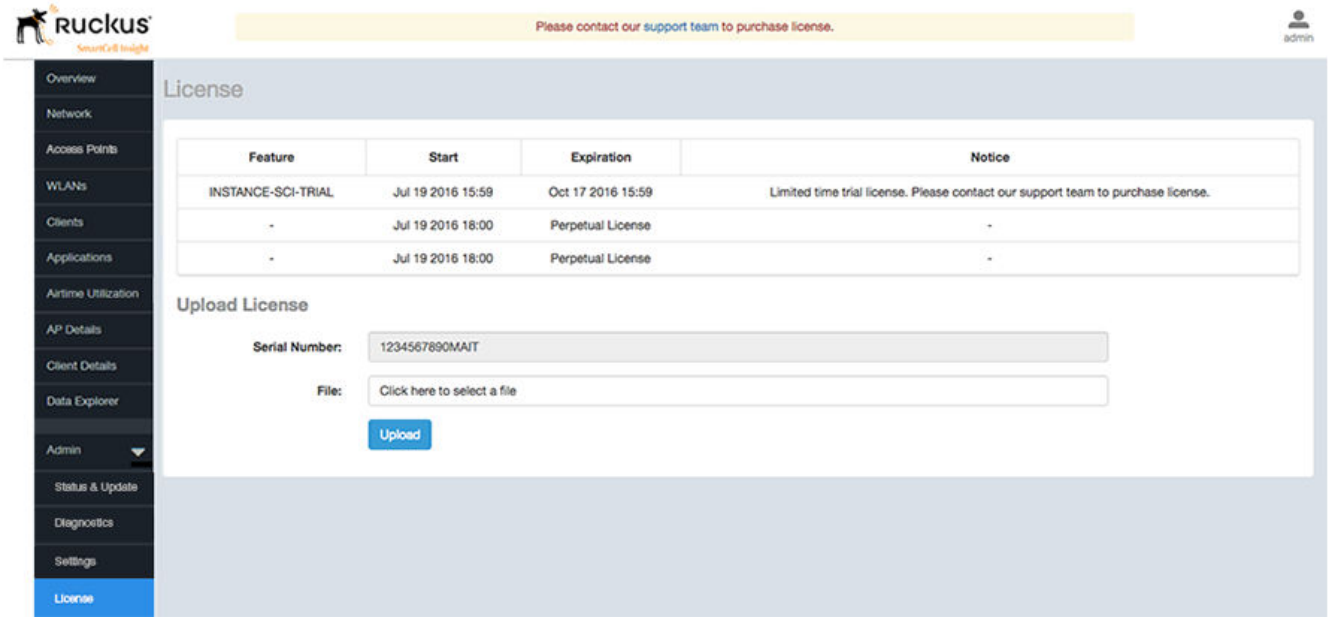
After using SCI with the trial license, make sure that you upgrade to the permanent SCI license in order to benefit from the product.

Follow these steps to upgrade to the SCI license:

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

   The **License** page appears.

FIGURE 23 License page



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....47
- Migration Procedure....48
- Monitor the Migration Process....49

This section describes how you migrate existing data from SCI 1.x to SCI 3.1.0.

As SCI 3.1.0 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 3.1.0, 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 3.1.0. 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 3.1.0 is installed.
3. SCI 3.1.0 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 3.1.0 instance in the **Admin > Settings** section. Ensure that the system name in SCI 3.1.0 matches the name of the system that is being migrated.
5. **Optional**: You can add more data nodes to the SCI 3.1.0 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 3.1.0.

1. Download the file *migrate.tar.gz* from the support website `https://support.ruckuswireless.com/`. Copy the tar file to SCI 3.1.0 VM and run the following command.

   ```
   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.
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>
   ```

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

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

4. On SCI 3.1.0 VM, run the following command to copy the file from SCI 1.4 VM. If you are prompted for a username and password, do provide the credentials for SCI 1.4 login.

   ```
   sudo sh step-2-scp.sh <SCI 1.4 -Hostname>
   ```

5. On SCI 3.1.0 VM, use the following command to list the dates for which data is available.

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

6. 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 */storage/rsa-master/logs/migration/dates.txt* in the form of a data directory URL.

   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.

7. Once the *dates.txt* is ready, start the migration process by running the following command on SCI 3.1.0 VM

   ```
   sudo sh step-4-migrate.sh <SCI 3.1.0-System-Name>
   ```

   > **NOTE**
   > Ensure that the system name in SCI 3.1.0 matches the name of the system that is being migrated from version 1.4.

8. 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 3.1.0 VM IP:58080/** and indexing logs at **https://< SCI 3.1.0 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 3.1.0 reports.

Copyright © 2006-2017. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com