SmartCell Insight Release 2.1

Installation Guide

Contents

5 Managing Licenses

Copyright Notice and Proprietary Information

About This Guide

This *SmartCell Insight 2.1 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

Table 1: Text conventions on page 6 and Table 2: Notice conventions on page 6 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

Notice type	Description
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

1

In this chapter:

- System Requirements
- DHCP Server Requirements
- NTP Server Requirements

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 and one or many Data nodes. 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.

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 (Root Volume)	80 GB
Secondary HDD (Data Volume)	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 (Root Volume)	80 GB
Secondary HDD (Data Volume)	500 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 5: Guidelines to Setup Data Nodes

Number of Data Nodes	Number of APs
0	Up to 3,000
1	Up to 10,000
2	Up to 20,000
3	Up to 30,000

NOTE: Add an additional Data node for every additional 10,000 APs

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

The node must have a storage capacity to handle at least 1 GB of data per day, for every 1,000 APs.

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 assigned to the Master node and Data 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.

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.

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.

Login to the SCI VM (master and data nodes) and add the following line to the chrony configuration file.

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

For more information about using SSH to connect to SCI, see Secure Shell Access to SCI on page 23

Installing SCI

2

In this chapter:

SCI 2.1 can be installed as a virtualized cluster using VMware's vSphere Web Client 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:

* 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: 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 it's 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 20.

4. Activate the Master node.

   For more information, see Setting Up the Nodes on page 20.

5. Set up the Data node.

   For more information, see Setting Up the Nodes on page 20.

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 host 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 10.

Figure 1: VMware vSphere Web Client
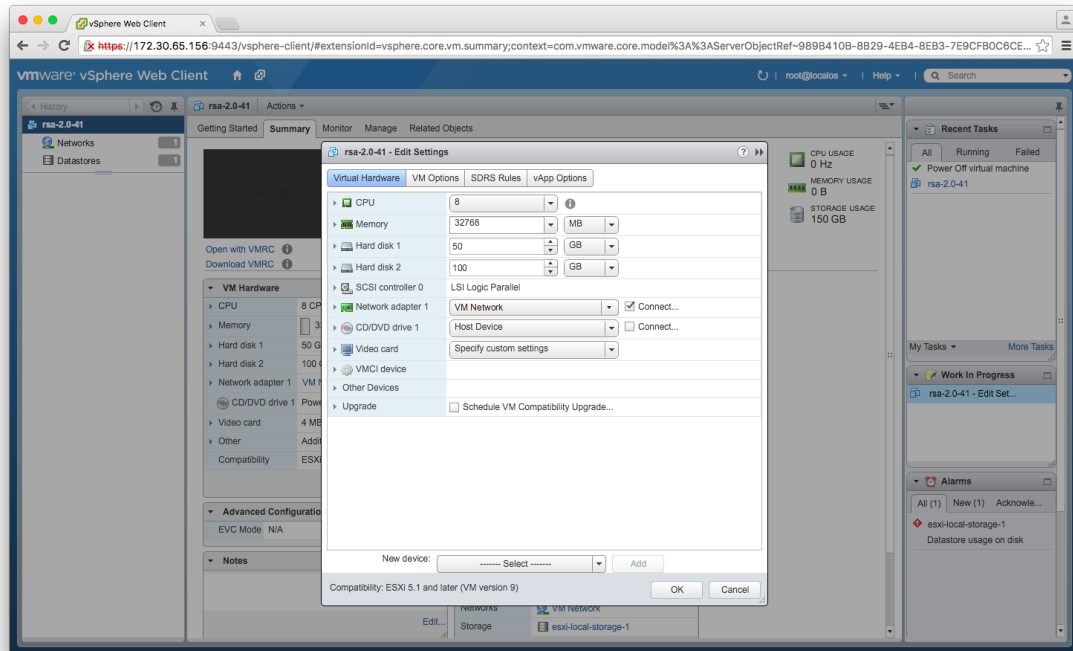
NOTE: The OVA file does not specify the minimum hardware requirements. Therefore, ensure that the hardware requirements are configured correctly.

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 17 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 and Data 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)**.

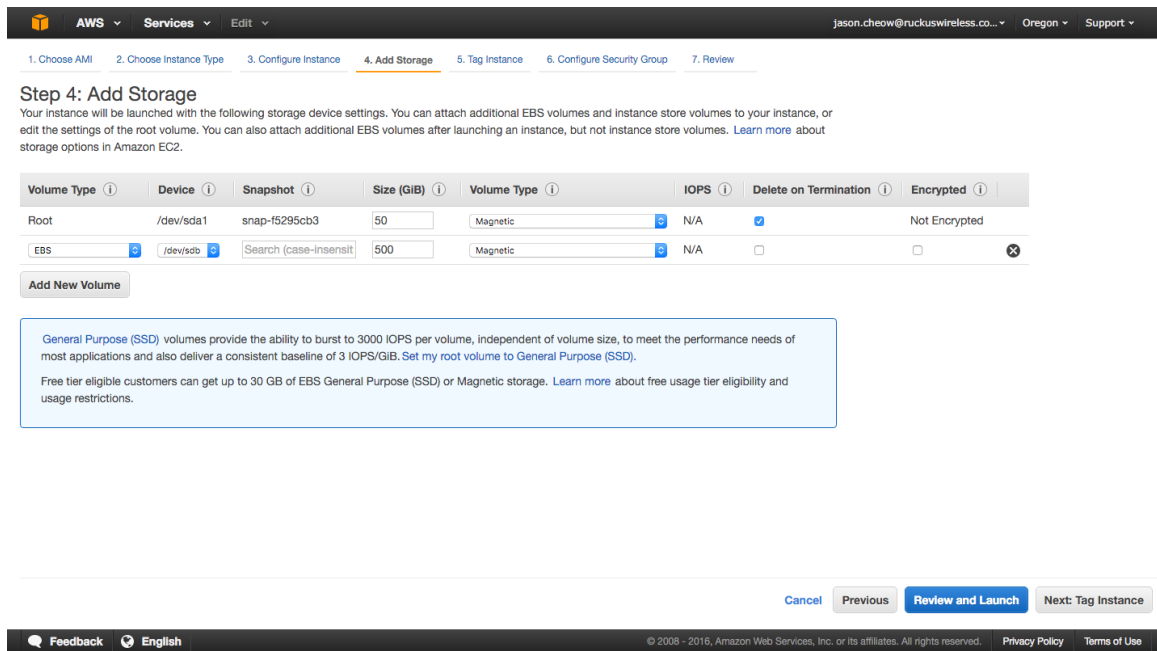   **Figure 2: Choosing the type of instance**

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.

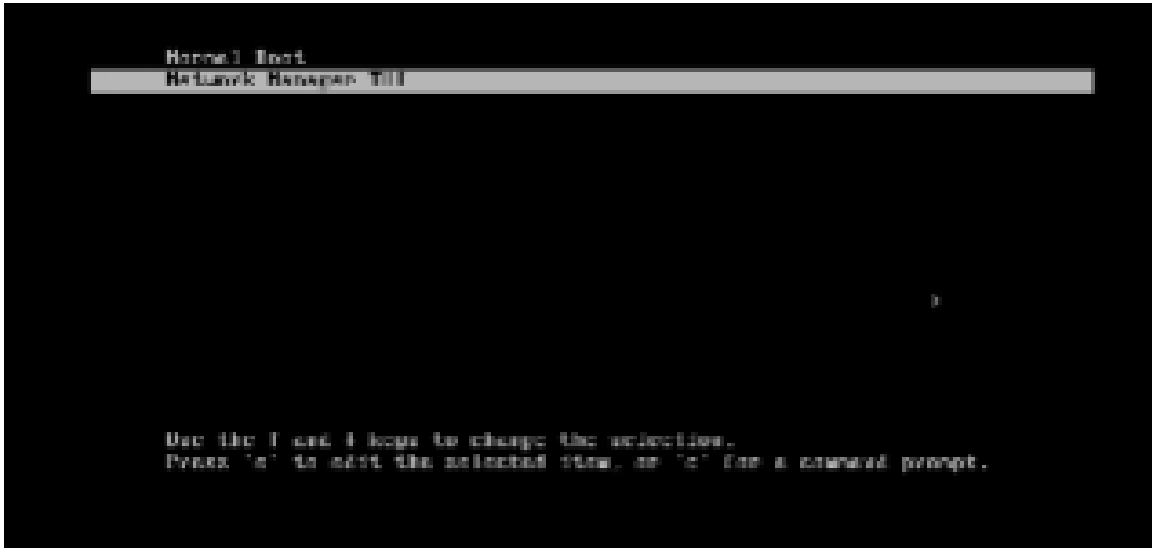# Setting Up the Virtual Machine Using a Static IP Address

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.

   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.
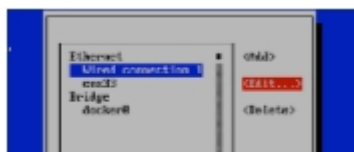
   Figure 5: Network Manager TUI screen

3. Select **Edit a connection**.

4. Press **Enter**.

   The following screen appears.
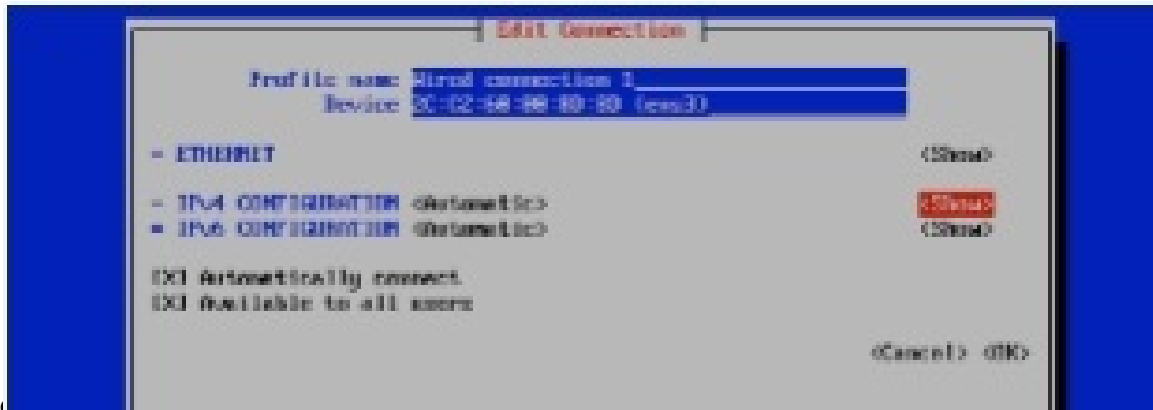
   Figure 6: Selecting a wired connection

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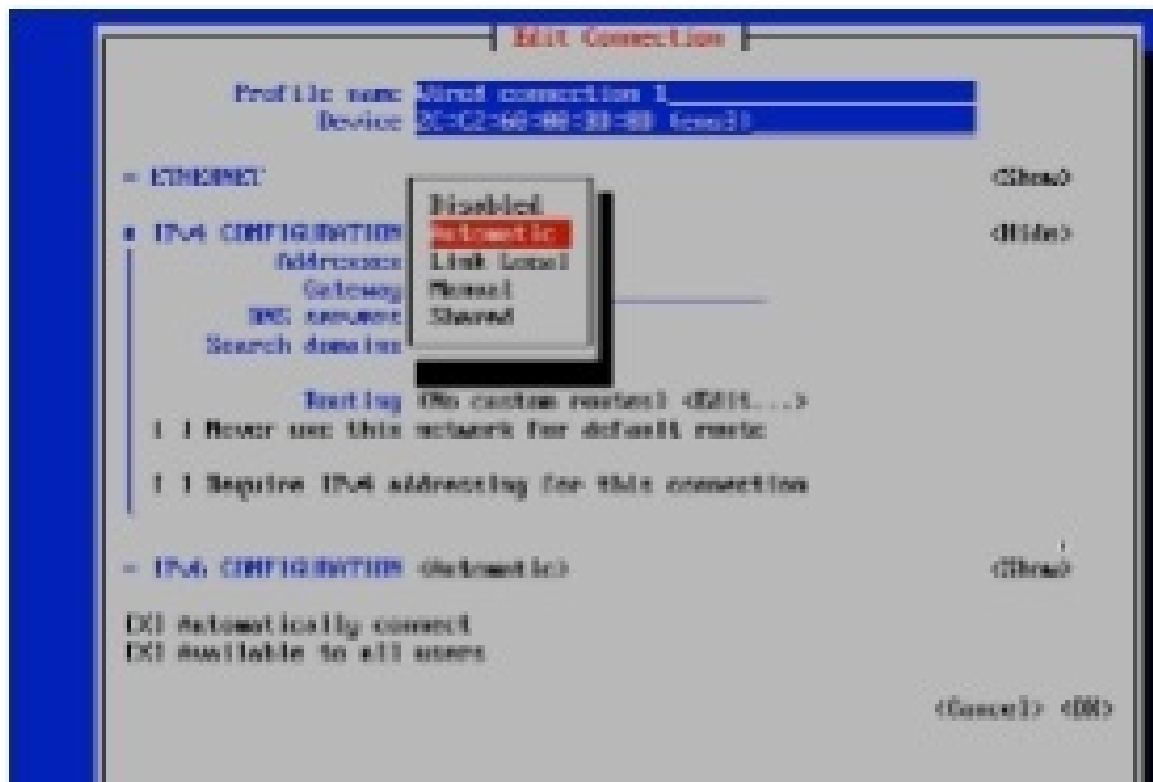
6. Select **Edit**.

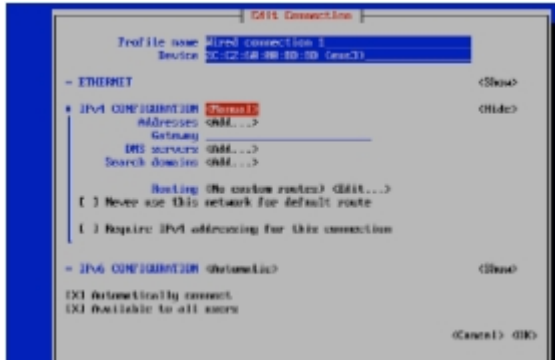The **Edit Connection** screen is displayed.

Figure 7: Edit

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

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 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 either select to set up the new VM as the Master Node in a new SCI cluster, or as a new Data Node in an existing cluster.

   Figure 10: Ruckus Smart Access page
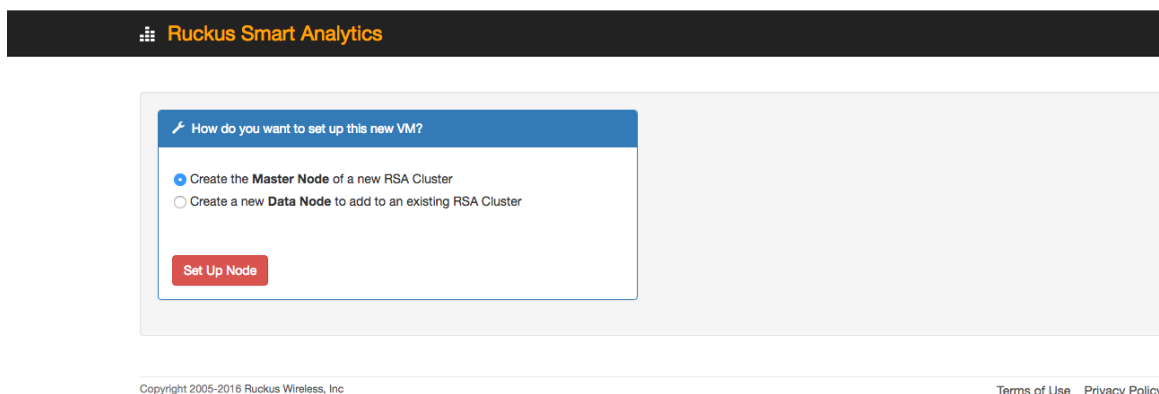
3. From Ruckus Smart Analytics, select the **Create the Master Node of a new RSA cluster** or **Create the Data Node of a new RSA cluster** as appropriate.

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 will also need the **RSA Portal User** and **RSA Portal User Password** to log into the newly created user portal.

5. Click **Activate Master Node** or **Activate Data 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 21

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 6: 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 7: 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

Table 8: 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 or Data 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]", "data_node_master_timeout": [Cluster's Master Node Verification Time Out (optional; as integer value in seconds)]}}' https://[SCI IP or domain name]/nodes
- curl -k -X PUT https://[SCI IP or domain name]/nodes/data/activate

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 with your user name and password.

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

   Figure 11: 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 VM, go to http://172.30.65.184/ for initial set up options.

localhost login:
```

Configuring SCI

3

In this chapter:

- Configuring SMTP
- Managing Controllers

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.

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

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

   Figure 12: SMTP configuration
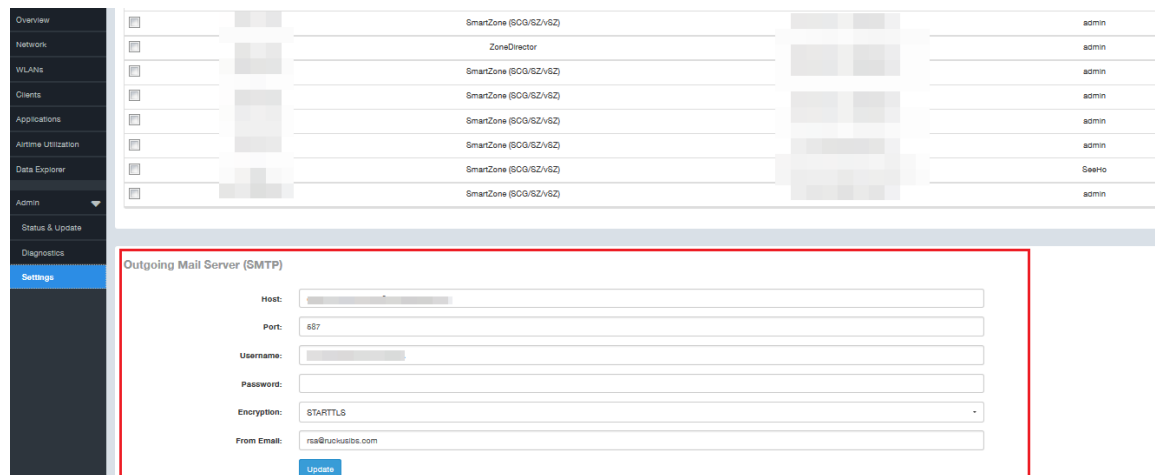
2. Configure the following information:

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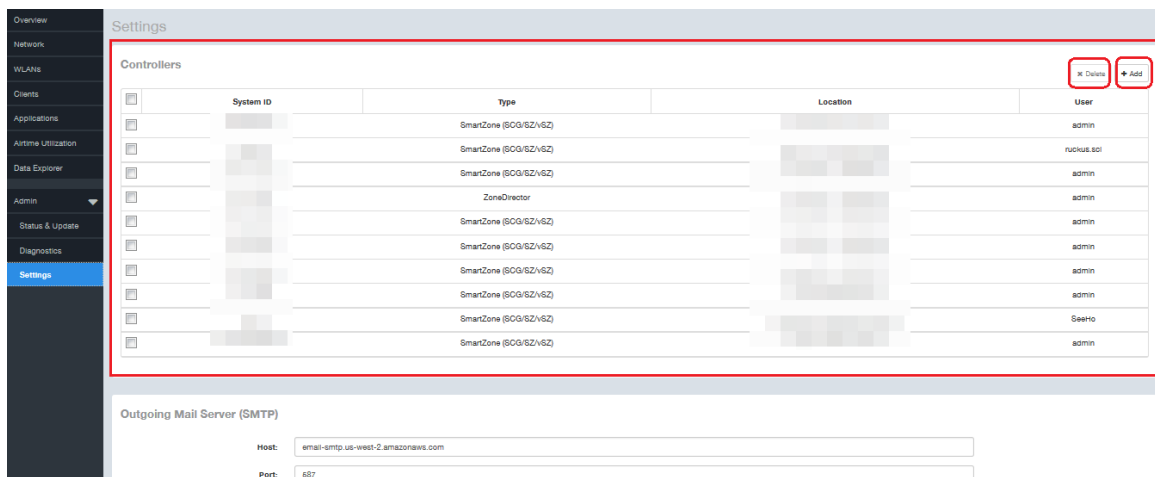
2. In **Controllers**, click **Add**.

   The **New Controller** dialog box appears.

   Figure 14: New controller information

3. Provide the following information:

- 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
- Location: type the IP address of the controller
- Username: type the username to access the controller
- Password: type the password to access the controller

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

4. Click **Create**.

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

Figure 15: 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 16: Selecting the controller

3. Click the controller row.

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

Figure 17: Editing controller information
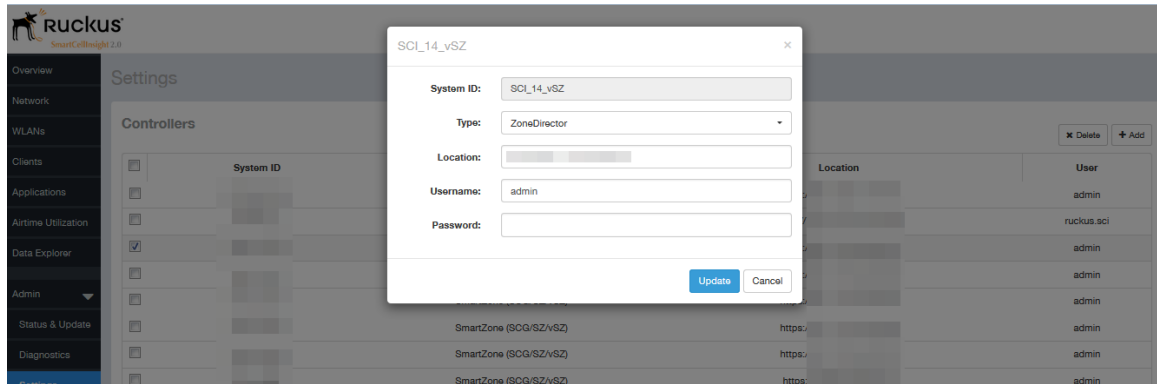
4. Click **Update**.

You have successfully edited the controller's information.

Configuring the Controller

<div style="text-align: right; font-size: 3em;">4</div>

In this chapter:

- Configuring Controllers from the Web UI

To understand the performance trends of a controller, you must add the controller to SCI and configure it's 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. An example to manage the SCI settings for the Virtual SmartZone-Essesntials (vSZ-E) controller, version 3.4 is shown.

Example to add controllers: SmartZone 3.4

Adding a SmartZone controller

Follow these steps to modify the SCI settings from the vZS-E web UI:

1. In the vSZ-E web UI, click **Configuration** > **System** > **SCI Setting**.

   The **SCI Setting** page appears.

   Figure 18: vSZ-E SCI settings page
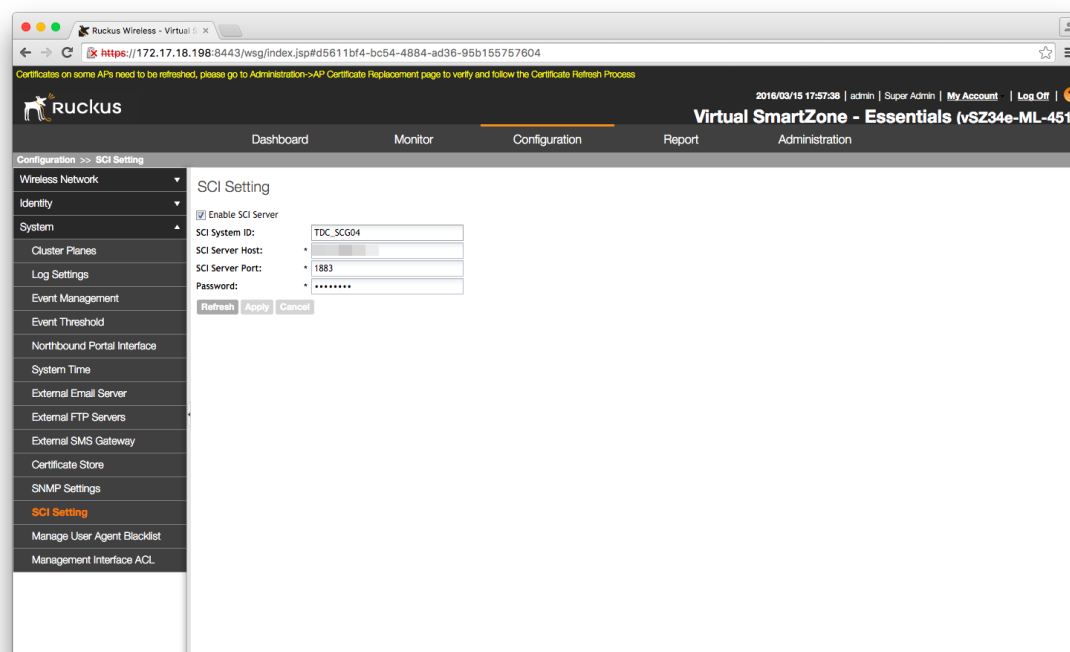
2. Select the **Enable SCI Server** check-box.
3. Configure the following SCI settings:

   - 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 controller.

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

Managing Licenses

<div align="right">5</div>

In this chapter:

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.
The trial license:

* 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 19: 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.

Index