



# SmartCell Insight Release 2.2

## Installation Guide

Part Number: 800-71388-001  
Published: 17 October 2016

[www.ruckuswireless.com](http://www.ruckuswireless.com)

# Contents

|  |   |
|--|---|
| Copyright Notice and Proprietary Information |   |
| About This Guide.....                        | 5 |
| Document Conventions.....                    | 5 |
| Related Documentation.....                   | 6 |
| Documentation Feedback.....                  | 6 |

## 1 Before You Begin

|   |   |
|---|---|
| System Requirements.....                  | 7 |
| Minimum Hardware Requirements.....        | 7 |
| Guidelines for Setting Up Data Nodes..... | 8 |
| Storage Requirements.....                 | 9 |
| Minimum Software Requirements.....        | 9 |
| DHCP Server Requirements.....             | 9 |
| NTP Server Requirements.....              | 9 |

## 2 Installing SCI

|   |    |
|---|----|
| Installation Overview.....                                    | 11 |
| Setting Up the Virtual Machine Using VMware ESXi.....         | 12 |
| Setting Up the Virtual Machine Using AWS.....                 | 14 |
| Setting Up the Virtual Machine Using a Static IP Address..... | 15 |
| Setting Up the Virtual Machine Using KVM.....                 | 19 |
| Setting Up the Nodes.....                                     | 20 |
| Firewall Rules.....   | 22 |
| Web API Setup.....  | 23 |
| Secure Shell Access to SCI.....                               | 23 |

## 3 Configuring SCI

|   |    |
|---|----|
| Configuring SMTP.....   | 25 |
| Managing Controllers.....   | 26 |
| Editing Controllers.....  | 29 |
| Enabling AP SCI Statistics Delivery on SmartZone Controllers..... | 30 |

## 4 Configuring the Controller

|  |    |
|--|----|
| Configuring Controllers from the Web UI.....   | 32 |
| Example to add controllers: SmartZone 3.4..... | 32 |

## 5 Updating the SCI Software

## 6 Managing Licenses

|                                   |    |
|-----------------------------------|----|
| Trial License.....                | 35 |
| Upgrading to the SCI License..... | 35 |

# Copyright Notice and Proprietary Information

Copyright 2016. 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.

## About This Guide

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

[Table 1: Text conventions](#) on page 5 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<br>ipaddr 10.0.0.12                                     |
| <b>user interface controls</b> | Keyboard keys, software buttons, and field names                   | Click <b>Create New</b>   |
| <b>Start &gt; All Programs</b> | Represents a series of commands, or menus and submenus             | Select <b>Start &gt; All Programs</b>                                       |
| <b>ctrl+V</b>                  | Represents keyboard keys pressed in combination                    | Press <b>ctrl+V</b> to paste the text from the clipboard.                   |
| <b>screen or page names</b>    |  | Click <b>Advanced Settings</b> . The <b>Advanced Settings</b> 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}  |

| Convention | Description                          | Example                   |
|------------|--------------------------------------|---------------------------|
| filepath   | Represents file names or URI strings | http://ruckuswireless.com |

Table 2: Notice conventions

| Notice type     | Description  |
|-----------------|--|
| <b>NOTE:</b>    | Information that describes important features or instructions  |
| <b>CAUTION:</b> | Information that alerts you to potential loss of data or potential damage to an application, system, or device |
| <b>WARNING:</b> | 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](mailto: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 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 (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   |

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        | 80 GB    |
| Secondary HDD   | 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: 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 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 15 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.

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 23

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.

# Installing SCI

# 2

In this chapter:

- [Installation Overview](#)
- [Setting Up the Virtual Machine Using VMware ESXi](#)
- [Setting Up the Virtual Machine Using AWS](#)
- [Setting Up the Virtual Machine Using a Static IP Address](#)
- [Setting Up the Virtual Machine Using KVM](#)
- [Setting Up the Nodes](#)
- [Secure Shell Access to SCI](#)

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:**

- 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 12 or [Setting Up the Virtual Machine Using AWS](#) on page 14.

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 12 or [Setting Up the Virtual Machine Using AWS](#) on page 14.

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 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

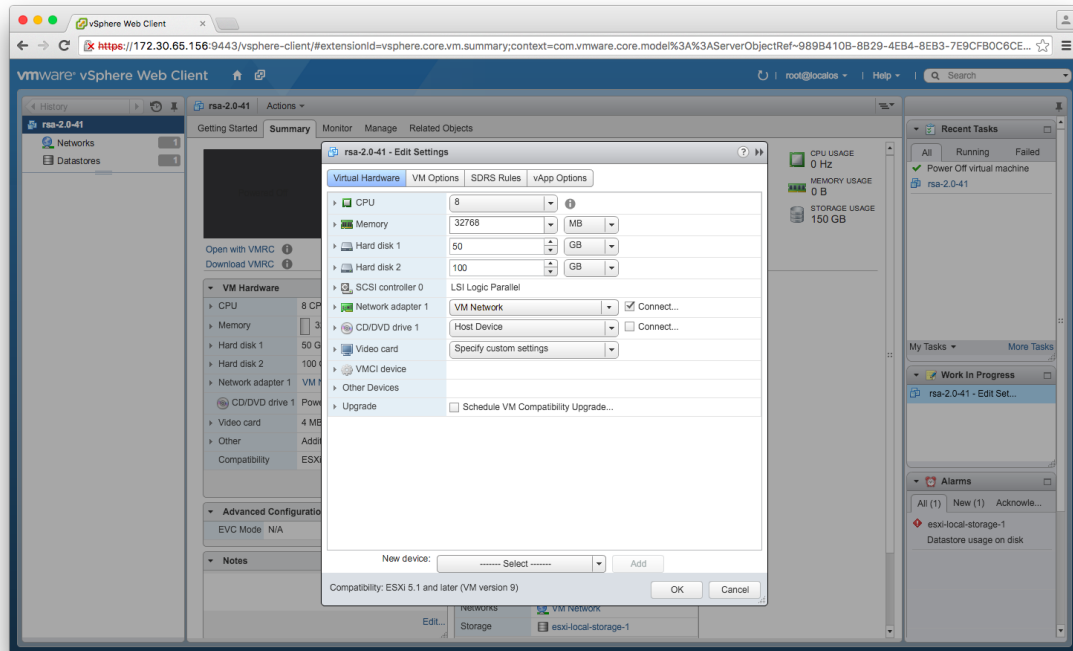
VMware ESXi is an enterprise-class hypervisor used for deploying and serving virtual computers.

Follow these steps to install and configure the VM:

1. Download the VMware ESXi software and ensure that it is running on a suitable 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 15 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.

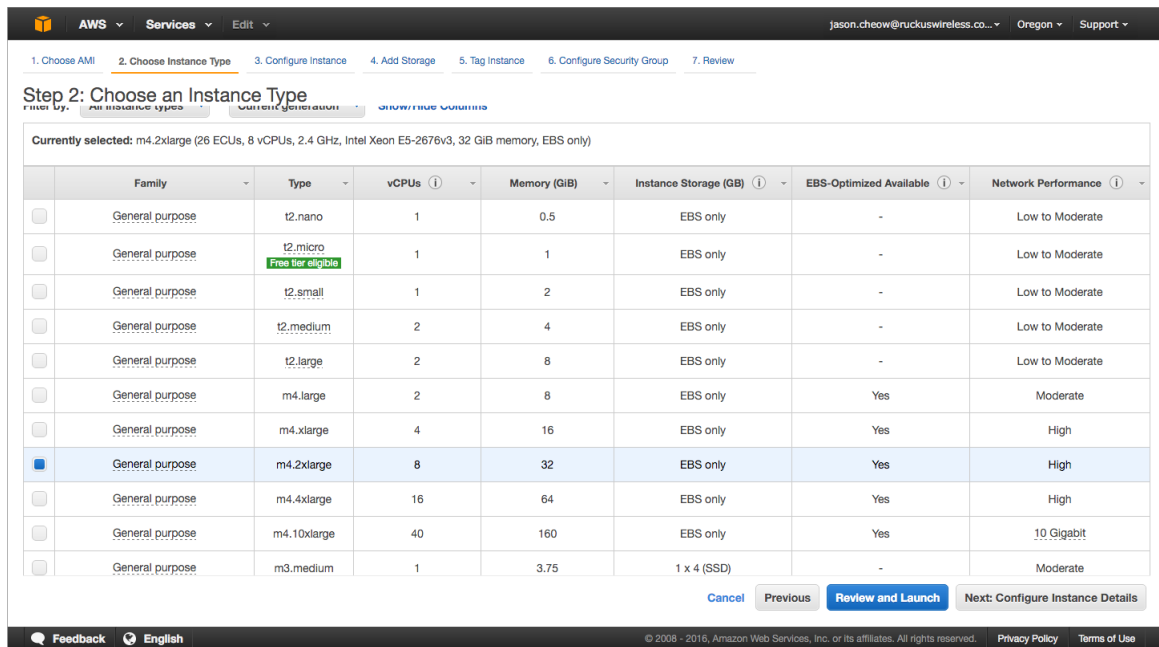
Contact Ruckus Wireless customer support and provide your AWS account ID, so that the company can share the SCI private AMI (Amazon Machine Image) number with you. For more information regarding AWS accounts IDs, see <http://docs.aws.amazon.com/general/latest/gr/acct-identifiers.html>.

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

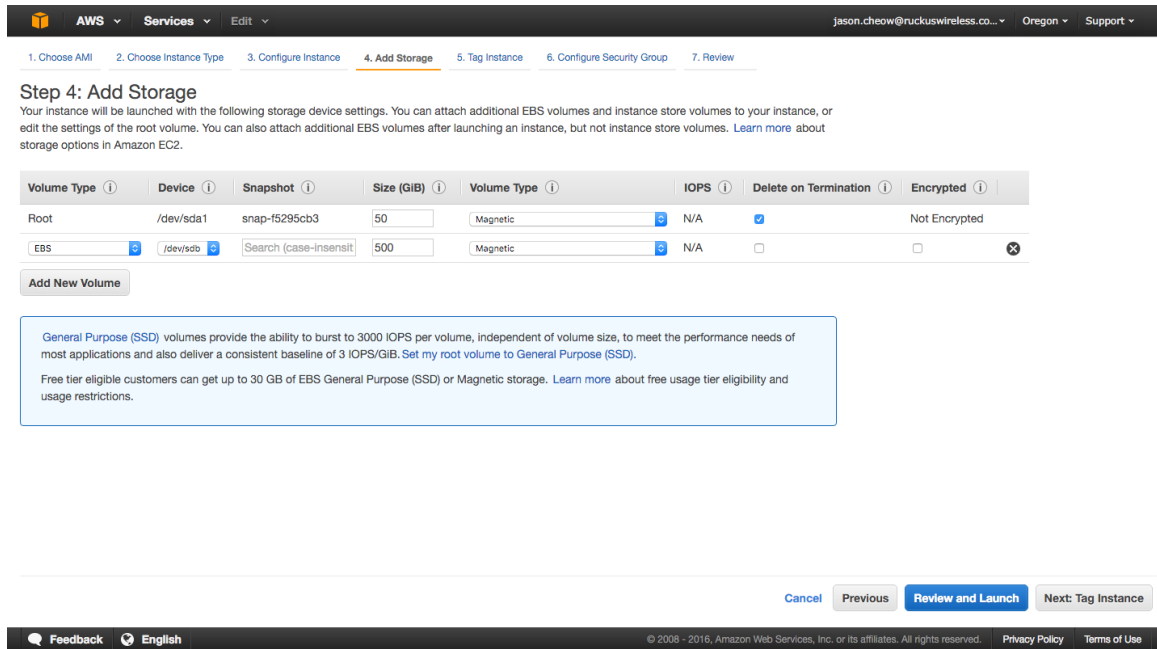


3. Configure the instance you have chosen based on your requirements.
4. Add storage to the instance.

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:**

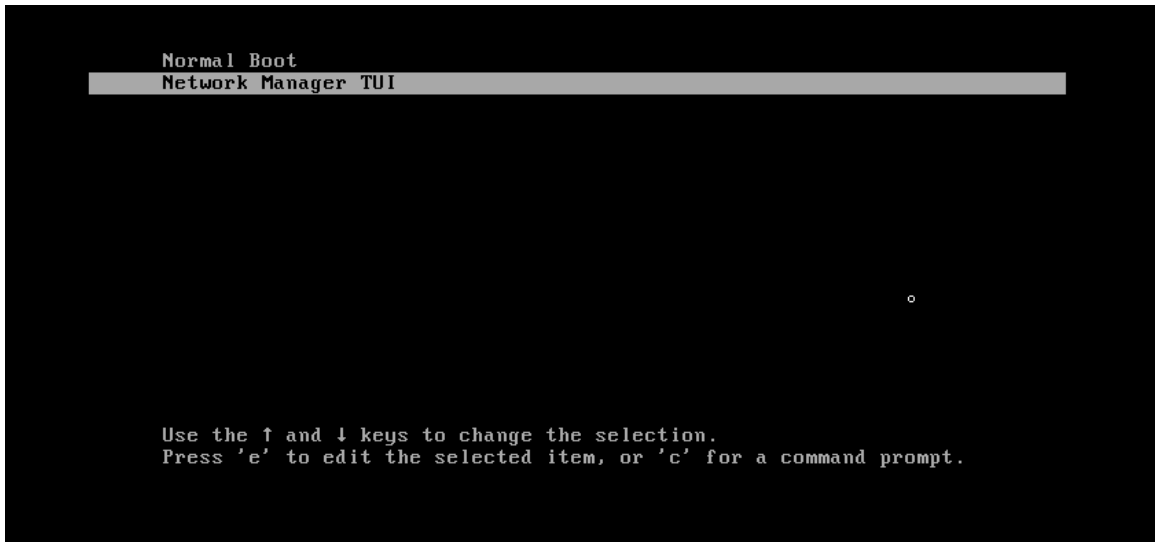
The static IP can be set only when you set up a VM. Once the VM is set up, there is no option to change the IP address.

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 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

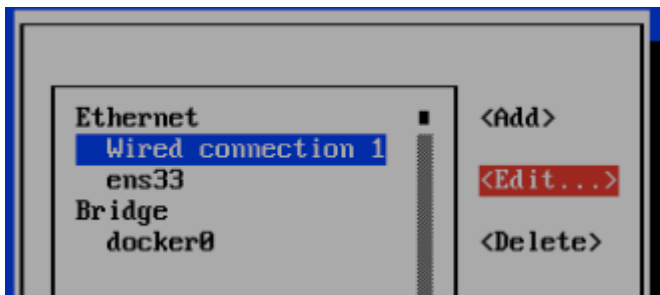


3. Select **Edit a connection**.
4. Press **Enter**.



The following screen appears.

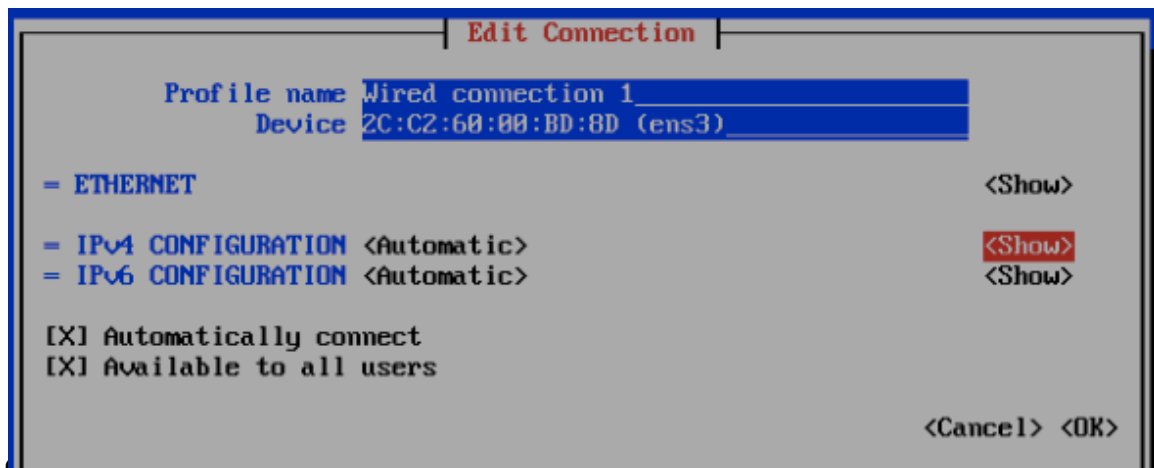
**Figure 6: Selecting a wired connection**



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

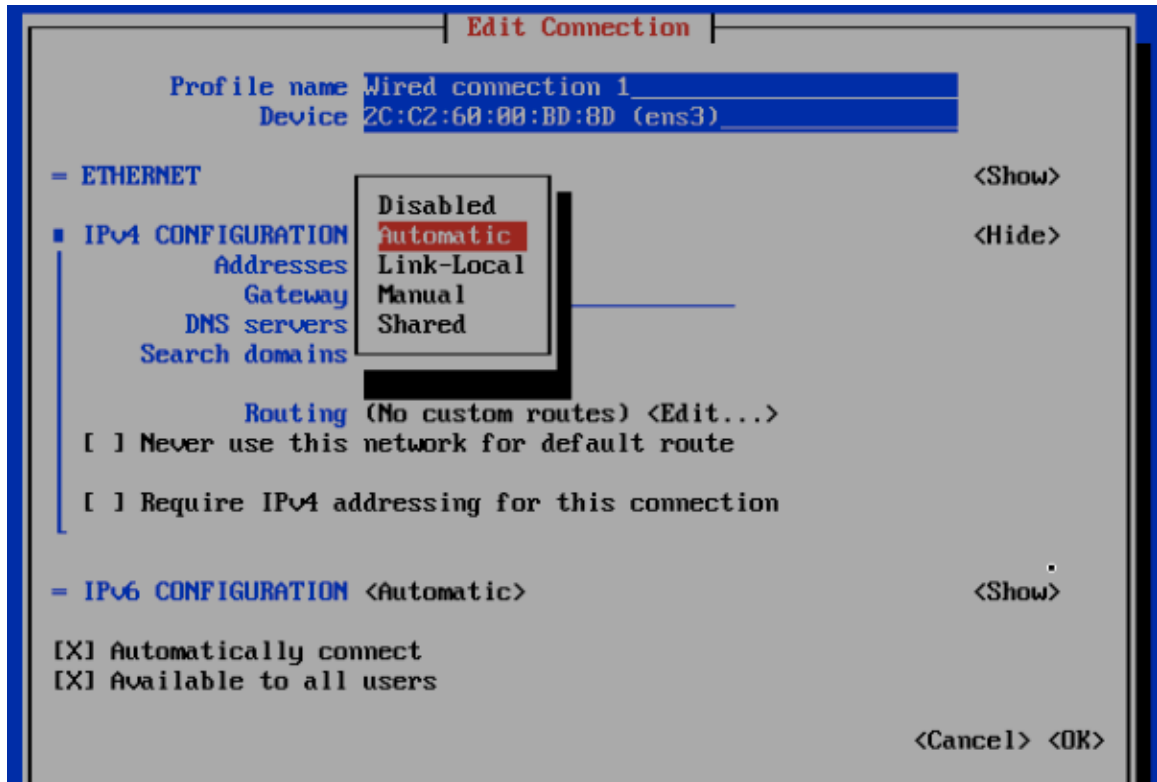
The **Edit Connection** screen is displayed.

**Figure 7: Edit**



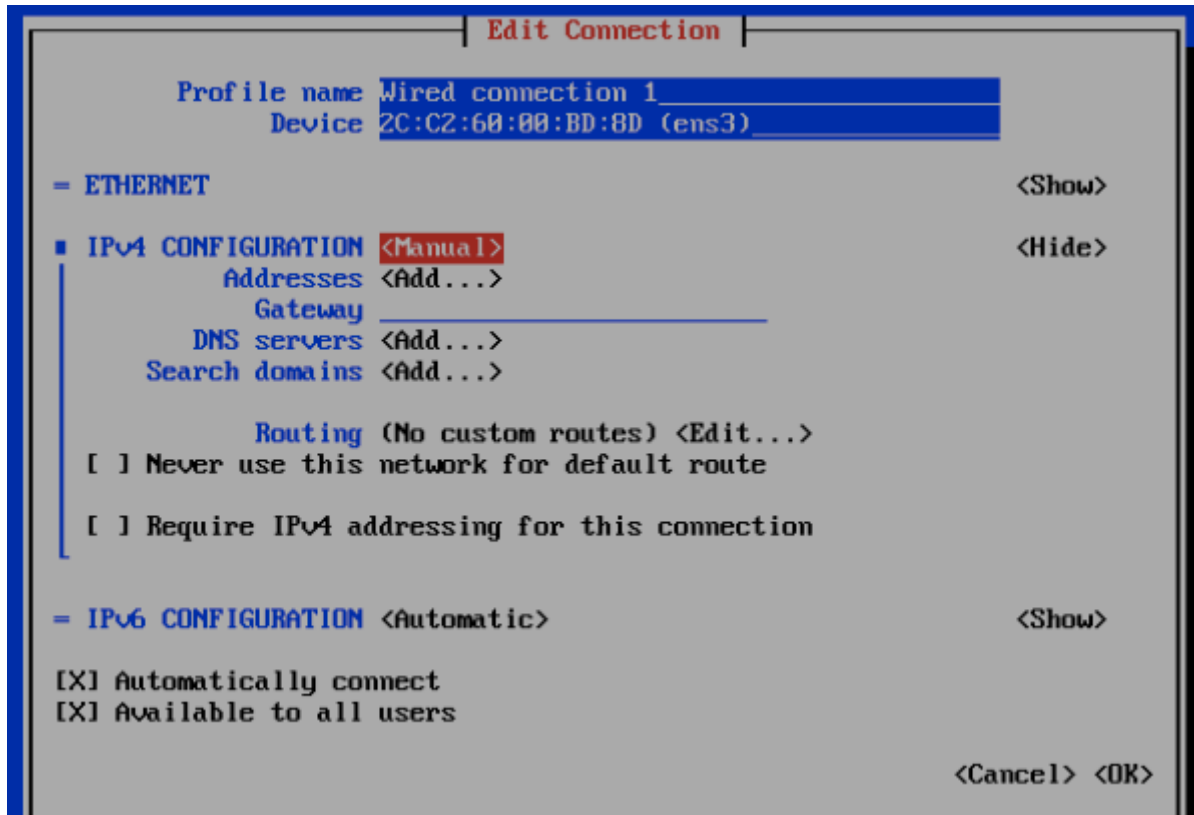
7. Select **Show** against the IPv4 configuration.
- The following screen appears.

**Figure 8: Changing the connection**



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

Figure 9: Manual IPv4 connection selected



**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

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

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

**NOTICE:** Installing and using the KVM software suite is beyond the scope of this guide, and there are multiple ways to provision a KVM guest.

Following is a Linux command line example to start a RSA VM as a KVM guest:

1. Run the `virt-install` command to define a RSA VM that meets the specifications available in [Minimum Hardware Requirements](#) on page 7.

For example, to provision a VM with 8 vCPUs, 32GB memory, 80GB root volume and a secondary 500GB data volume, using bridged networking, run the following command:

```
virt-install --name rsa --vcpus 8 --memory 32768 --disk  
rsa-vm-image.qcow2,size=80 --import --disk size=500 --graphics vnc  
--noautoconsole --network bridge=br0.
```

2. Run the `virsh` command to start, terminate or monitor the VM (assuming it is named "rsa") as follows:

```
a) virsh --connect qemu:/system list  
b) virsh --connect qemu:/system start rsa  
c) virsh --connect qemu:/system shutdown rsa
```

3. Use a suitable VNC viewer to access the console. Run the following command to receive information about the VNC connection: `virsh --connect qemu:/system vncdisplay rsa`.

If you use CentOS, see <https://wiki.centos.org/HowTos/KVM> for more information about setting up and using KVM.

## 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>>).

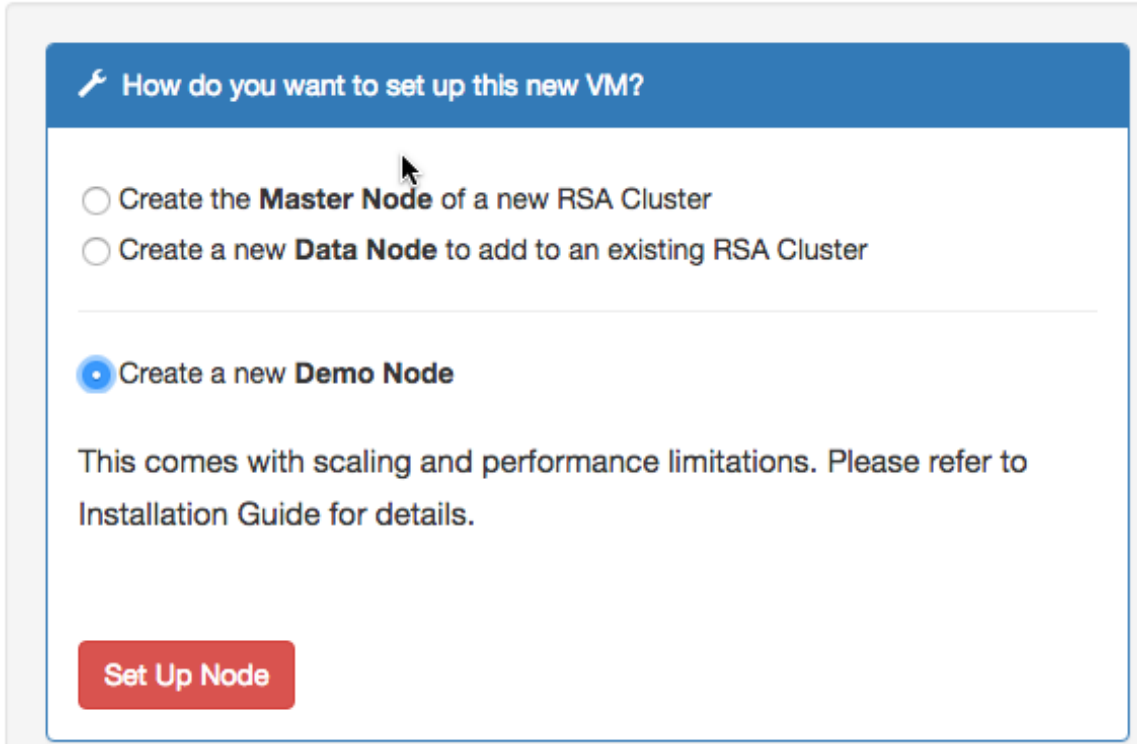
The **Ruckus Smart Access** page appears.

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**

## Ruckus Smart Analytics



How do you want to set up this new VM?

Create the **Master Node** of a new RSA Cluster

Create a new **Data Node** to add to an existing RSA Cluster

Create a new **Demo Node**

This comes with scaling and performance limitations. Please refer to Installation Guide for details.

**Set Up Node**

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 22

- 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 7: 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 8: 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 9: 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]", "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`

### 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`

## 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.

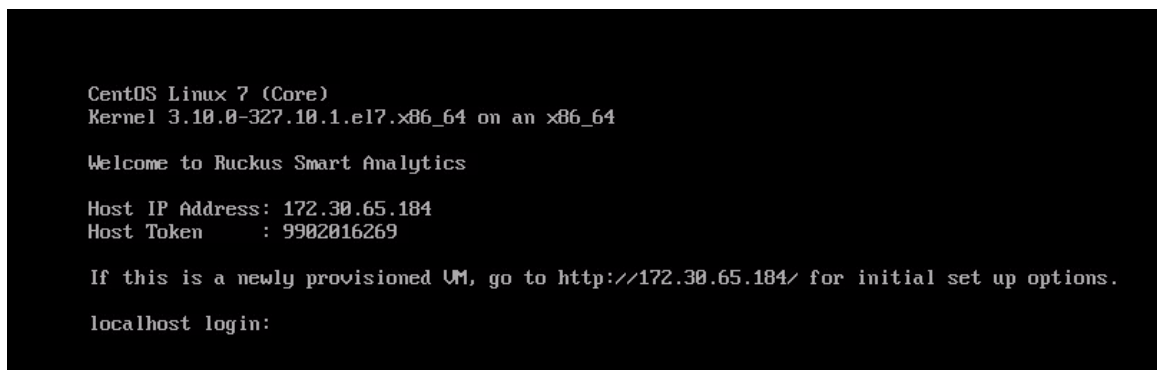
**ATTENTION:** Login with the following credentials:

Username: rsa

Password: Node token

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

**Figure 11: Sample SSH screen**



```
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

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.

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

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

**Figure 12: SMTP configuration**

|                          |  |                        |  |       |
|--------------------------|--|------------------------|--|-------|
| <input type="checkbox"/> |  | SmartZone (SCG/SZ/v62) |  | admin |
| <input type="checkbox"/> |  | ZoneDirector           |  | admin |
| <input type="checkbox"/> |  | SmartZone (SCG/SZ/v62) |  | admin |
| <input type="checkbox"/> |  | SmartZone (SCG/SZ/v62) |  | admin |
| <input type="checkbox"/> |  | SmartZone (SCG/SZ/v62) |  | admin |
| <input type="checkbox"/> |  | SmartZone (SCG/SZ/v62) |  | admin |
| <input type="checkbox"/> |  | SmartZone (SCG/SZ/v62) |  | SeeHo |
| <input type="checkbox"/> |  | SmartZone (SCG/SZ/v62) |  | admin |

**Outgoing Mail Server (SMTP)**

Host:

Port:

Username:

Password:

Encryption:

From Email:

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

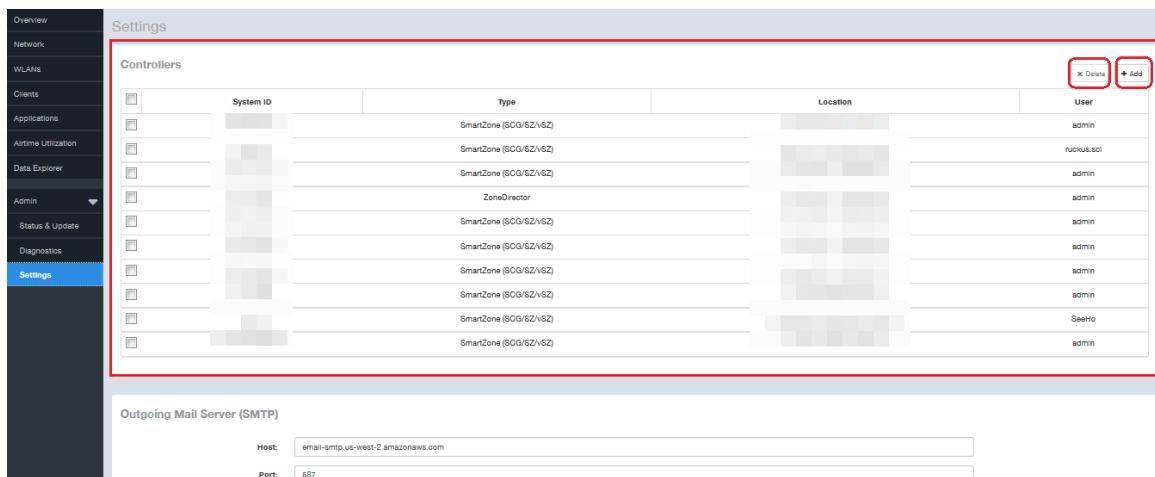
You must add controllers to SCI to monitor and manage them. SCI analyzes data from the controller and provides information about the WiFi network performance.

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 -

The image shows a 'New Controller' dialog box with the following fields and controls:

- System ID:** An empty text input field.
- Type:** A dropdown menu with 'ZoneDirector' selected.
- Location:** A text input field containing 'scheme://host:port'.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Buttons:** 'Create' (blue) and 'Cancel' (white) buttons located at the bottom right.

If you have an SmartZone cluster, 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**

The screenshot shows a 'New Controller' dialog box with the following fields and values:

- System ID:** [Empty text field]
- Type:** SmartZone (SCG/SZ/vSZ) [Dropdown menu]
- Location:** scheme://host:port [Text field]
- Backup Location:** scheme://host:port [Text field]
- Username:** [Text field with a cursor]
- Password:** [Empty text field]

Buttons: Create, Cancel

**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 URL of the controller
- Backup Location: type the URL of the backup controller location
- 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.

**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

#### 4. Click **Create**.

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

**Figure 16: New controller is added**

| <input type="checkbox"/> | System ID    | Type                   | Location             | User  |
|--------------------------|--------------|------------------------|----------------------|-------|
| <input type="checkbox"/> | Controller 0 | SmartZone (SCG/SZ/VSZ) | https://1.1.1.0:8443 | admin |
| <input type="checkbox"/> | Controller 1 | SmartZone (SCG/SZ/VSZ) | https://1.1.1.1:8443 | admin |
| <input type="checkbox"/> | Controller 2 | SmartZone (SCG/SZ/VSZ) | https://1.1.1.2:8443 | admin |

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.

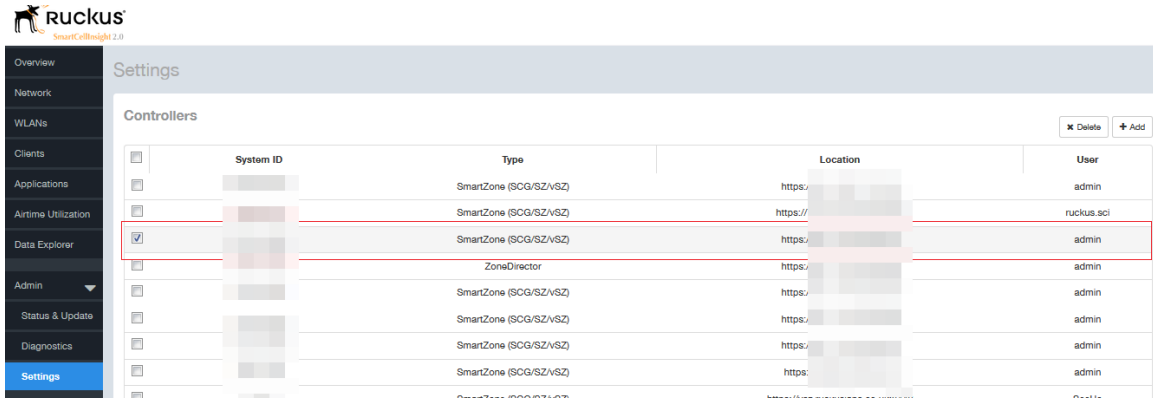
Follow these steps to edit the controller's information:

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.

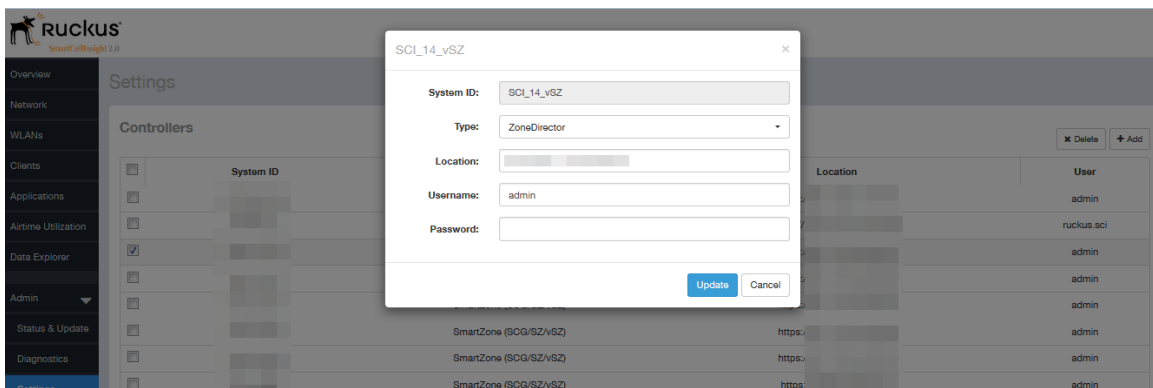
**Figure 17: Selecting the controller**



3. Click the controller row.

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

**Figure 18: Editing controller information**



4. Click **Update**.

You have successfully edited the controller's information.

### Enabling AP SCI Statistics Delivery on SmartZone 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 zoneglobal ap-sci` command.

# 4

## Configuring the Controller

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 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. An example to manage the SCI settings for the Virtual SmartZone-Essentials (vSZ-E) controller, version 3.4 is shown.

#### Example to add controllers: SmartZone 3.4

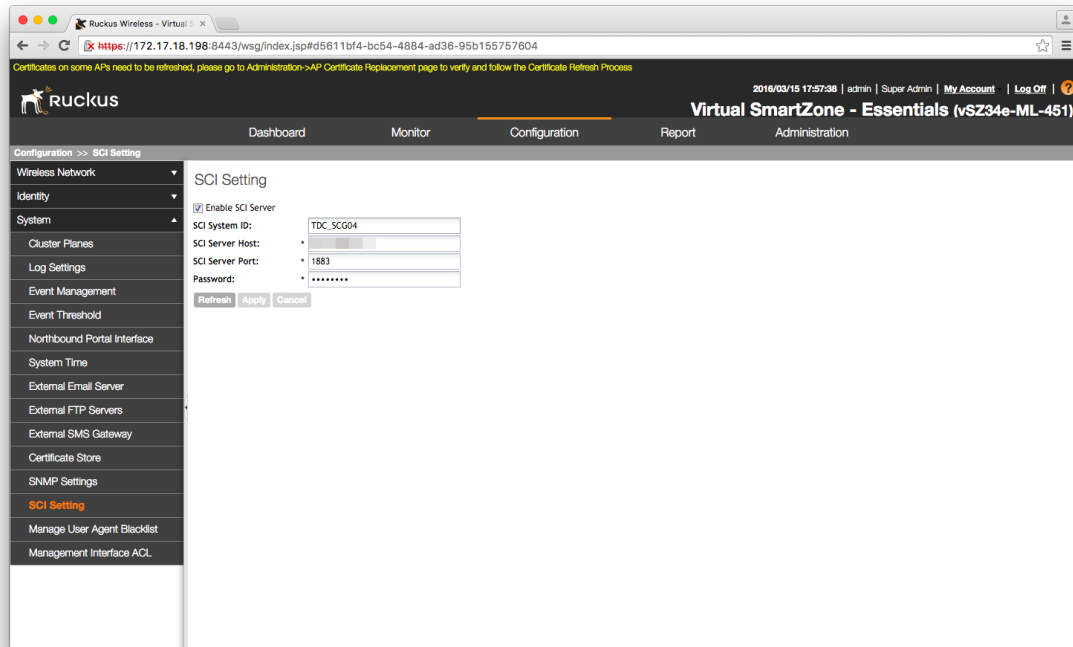
##### Adding a SmartZone controller

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

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

The **SCI Setting** page appears.

Figure 19: 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.

## 5

# Updating the SCI Software

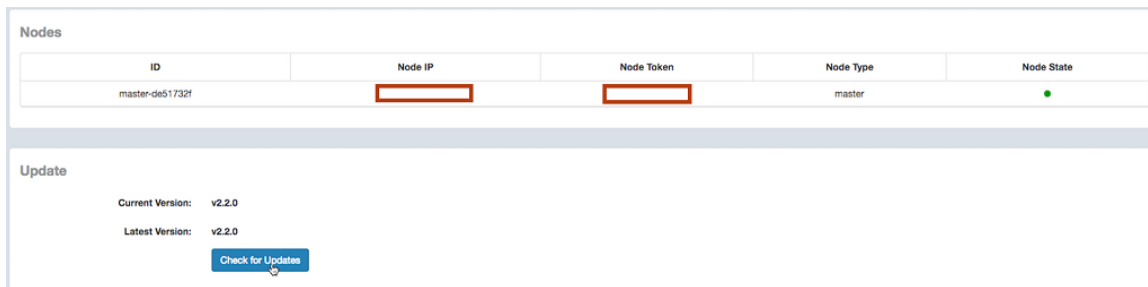
You can update the SCI software from the cloud if you are connected to the internet.

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 20: Updating software**

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

# Managing Licenses

In this chapter:

- [Trial License](#)
- [Upgrading to the SCI License](#)

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 21: License page**

The screenshot shows the Ruckus SmartCell Insight web interface. At the top left is the Ruckus logo. A yellow banner at the top center reads "Please contact our support team to purchase license." The user is logged in as "admin". The left sidebar contains navigation options: Overview, Network, WLANs, Clients, Applications, Airtime Utilization, Data Explorer, Admin, Status & Update, Diagnostics, Settings, and License (which is highlighted). The main content area is titled "License" and contains a table with the following data:

| Feature            | Start             | Expiration        | Notice   |
|--------------------|-------------------|-------------------|--|
| INSTANCE-SCI-TRIAL | Jul 19 2016 15:59 | Oct 17 2016 15:59 | Limited time trial license. Please contact our support team to purchase license. |
| -                  | Jul 19 2016 18:00 | Perpetual License | -  |
| -                  | Jul 19 2016 18:00 | Perpetual License | -  |

Below the table is the "Upload License" section, which includes:

- Serial Number: 1234567890MAIT
- File: Click here to select a file
- Upload button

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

## A

accurate statistics [9](#)  
adding controllers [26](#)  
Amazon EC2 [14](#)  
AWS [14](#)

## C

controller configuration [32](#)  
copyright information [4](#)  
correct time [9](#)

## D

data node guidelines [8](#)  
deleting controllers [26](#)  
dhcp [9](#)

## E

editing controllers [29](#)  
enabling statistics [30](#)

## F

firewall rules [22](#)

## H

hardware requirements [7](#)

## I

installation overview [11](#)  
installation prerequisites [7](#)

## K

kvm [19](#)

## L

legal [4](#)

## N

ntp [9](#)

## S

sci configuration [25](#)  
sci license [35](#)  
setup data node [20](#)  
setup master node [20](#)  
setup sci cluster [20](#)  
smtp [25](#)  
software requirements [9](#)  
ssh [23](#)  
static ip address [15](#)  
storage requirements [9](#)

## T

trademarks [4](#)  
trial license [35](#)

## U

updating software [34](#)

## V

VMware ESXi [12](#)

## W

web api [23](#)  
web ui [32](#)