Ruckus Wireless™ Virtualized SmartCell Gateway™

Getting Started Guide for RuckOS 3.0.3

Part Number 800-70797-001 Rev A
Published January 2015

www.ruckuswireless.com

Copyright Notice and Proprietary Information

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, Bark Logo, BeamFlex, ChannelFly, Ruckus Pervasive Performance, SmartCell, ZoneFlex, Dynamic PSK, FlexMaster, MediaFlex, MetroFlex, Simply Better Wireless, SmartCast, SmartMesh, SmartSec, SpeedFlex, ZoneDirector, ZoneSwitch, and ZonePlanner 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 Guide

Document Conventions 6
Related Documentation 6
Documentation Feedback 7

1 Preparing to Install the vSCG

Preparing a Hypervisor 8
Obtaining the vSCG Distribution 8
Preparing the vSCG Interface Settings to Use 9
Determining the System Resources That the Virtual Machine Requires 10

2 Installing the vSCG on a Hypervisor

Installing the vSCG on VMWare™ vSphere Hypervisor 11
Before You Begin 11
Creating a vSCG Instance from the OVA File 12
Allocating Resources and Assigning Network Interfaces 22
Configuring the Interfaces 25
Setting Up the vSCG Interface or Interfaces 26
Installing the vSCG on a Kernel-based Virtual Machine Hypervisor 34
Extracting the vSCG Image 34
Setting Up the vSCG 36

3 Using the Setup Wizard to Install vSCG

Before You Begin 46
Step 1: Start the Setup Wizard and Set the Language 47
Step 2: Select the Profile Configuration That Corresponds to Your vSCG License 48
Step 3: Configure the Management IP Settings 49
Step 4: Configure the Cluster Settings 51
If This vSCG Is Forming a New Cluster 51
If This vSCG Is Joining an Existing Cluster 52
Step 5: Set the Administrator Password 54
Step 6: Verify the Settings 56
Logging On to the Web Interface 58

4 Configuring the vSCG Carrier for the First Time

Creating an AP Zone . . . 61
Configuring AAA Servers and Hotspot Settings . . . 65
Adding an AAA Server . . . 65
Creating a Hotspot Service . . . 67
Creating a Registration Rule . . . 70
Configuring the Rule Priority . . . 72
Defining the WLAN Settings of an AP Zone . . . 73
General Options . . . 74
WLAN Usage . . . 74
Authentication Options . . . 75
Encryption Options . . . 75
Authentication & Accounting Service . . . 77
Options . . . 77
RADIUS Options . . . 78
Advanced Options . . . 78
Configuring DHCP Option 43 . . . 79
Verifying That Wireless Clients Can Associate with a Managed AP . . . 83
What to Do Next . . . 84

5 Ensuring That APs Can Discover the Controller on the Network

Is LWAPP2SCG Enabled on the Controller? . . . 86
Obtaining the LWAPP2SCG Application . . . 86
Enabling LWAPP2SCG . . . 86
Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server . . . 87
Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet . . . 88
Method 3: Register the Controller with the DNS Server . . . 88
Method 4: Configure DHCP Option 43 on the DHCP Server . . . 91
Method 5: Manually Configure the Controller Address on the AP's Web Interface . . . 94
What to Do Next . . . 95

Index

About This Guide

This *Virtualized SmartCell Gateway™ (vSCG) Getting Started Guide* provides information on how to set up the vSCG virtual appliance on the network. You can install the vSCG on any of the supported hypervisors.

Topics covered in this guide include preparing your chosen hypervisor. installing the vSCG image on to the hypervisor, and completing the vSCG Setup Wizard.

This guide is intended for use by those responsible for installing and setting up network equipment. Consequently, it assumes a basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE: If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support website at

https://support.ruckuswireless.com/documents.

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

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

In addition to this *Getting Started Guide*, each Virtualized SmartCell Gateway documentation set includes the following:

- *Administrator Guide*: Provides detailed information on how to configure the vSCG. The Administrator Guide is available for download on the Ruckus Wireless Support website at http://support.ruckuswireless.com.
- *Online Help*: Provides instructions for performing tasks using the vSCG web interface. The online help is accessible from the web interface and is searchable.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

NOTE: 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)

For example:

- Virtualized SmartCell Gateway (vSCG) Getting Started Guide for RuckOS 3.0
- Part number: 800-70797-001
- Page 88

Preparing to Install the vSCG

1

In this chapter:

- Preparing a Hypervisor
- Obtaining the vSCG Distribution
- Preparing the vSCG Interface Settings to Use
- Determining the System Resources That the Virtual Machine Requires

Preparing a Hypervisor

Table 3 lists the hypervisors (and their release versions) on which you can install the vSCG.

Table 3. Hypervisors that the vSCG supports

Vendor	Hypervisor	Version
VMWare	ESXi	5.x
KVM	Linux	2.6.32, 3.10.0

The vSCG installation procedures for each of these hypervisors vary. For more information, see Installing the vSCG on a Hypervisor.

Obtaining the vSCG Distribution

From the vSCG download page on the Ruckus Wireless support website, download the .OVA file and documentation for the vSCG appliance. The vSCG distribution package, which is based on the Open Virtualization Format (OVF) framework, consists of a virtual appliance containing the following files:

- Description file (.ovf)
- Manifest file (.mf)
- Virtual machine state file (.vmdk)

These three files are consolidated into a TAR archive file and distributed as an Open Virtual Appliance (OVA) package. This OVA package can be imported directly into your chosen hypervisor.

Preparing the vSCG Interface Settings to Use

The vSCG comes with the option to operate with either one (1) network interface or three (3) network interfaces (see Table 4). Once the network interface configuration has been made and setup executed, the number of network interfaces can no longer be modified.

CAUTION! If you choose to operate the vSCG with three network interfaces, you must configure the three vSCG interfaces to be on three different subnets when you run the Setup Wizard. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

Before installing the vSCG, prepare the following required network settings:

- IP address
- Netmask
- Gateway
- Primary DNS server
- Secondary DNS server

Table 4. vSCG interfaces

Interface	Description
AP	Used for AP configuration and client traffic
Cluster	Used for cluster traffic
Management (Web)	Used for management traffic. The IP address that you assign to this interface will be the IP address at which you can access the vSCG web interface.

Determining the System Resources That the Virtual Machine Requires

The number of APs and clients that the vSCG can support depends on the system resources (CPU and memory) that the virtual machine running the vSCG has. The vSCG is capable of automatically scaling to and supporting a higher number of APs and clients if it determines, at system bootup, that there is sufficient CPU and memory on the virtual machine to support more APs and clients.

Table 5 (carrier profile configuration) and Table 6 (enterprise profile configuration) list the maximum recommended number of APs and clients that the vSCG can support based on the available vCPU and memory available on the virtual machine[1]. The first row in Table 5, for example, shows that to support 25 APs, the vSCG must have at least 2-core CPU and 7GB of RAM. Whenever the CPU or memory settings are changed, the vSCG instance must be rebooted for the updated settings to be applied to it.

Table 5. Carrier profile configuration: Recommended system resources

AP Count	Wireless Client Count	CPU Core Count	Memory Size (GB)	HD Size (GB)	AP Groups Per System
100	2,000	2	7	100	6
500	10,000	4	8	100	26
1,000	20,000	4	10	100	52
2,500	50,000	6	14	300	128
10,000	100,000	16	48	600	512

Table 6. Enterprise profile configuration: Recommended system resources

AP Count	Wireless Client Count	CPU Core Count	Memory Size (GB)	HD Size (GB)
100	2,000	2	10	100
1,000	20,000	6	17	100

1. These scalability figures have been observed on the vSCG for RuckOS 3.0.3.

Installing the vSCG on a Hypervisor 2

In this chapter:

- Installing the vSCG on VMWare™ vSphere Hypervisor
- Installing the vSCG on a Kernel-based Virtual Machine Hypervisor

Installing the vSCG on VMWare™ vSphere Hypervisor

Follow these steps to install the vSCG on a VMWare vSphere hypervisor:

- Before You Begin
- Creating a vSCG Instance from the OVA File
- Allocating Resources and Assigning Network Interfaces
- Configuring the Interfaces

Before You Begin

Verify that you have the prerequisites before installing the vSCG on VMWare vSphere.

- Verify that vSphere client is installed.
- You can deploy the vSCG only on hosts that are running ESXi version 5.1 or later.
- The vSCG appliance requires at least 100GB of disk space and is limited to a maximum size of 600GB. The vSCG appliance can be deployed with thin-provisioned virtual disks that can grow to the maximum size of 600GB.

Creating a vSCG Instance from the OVA File

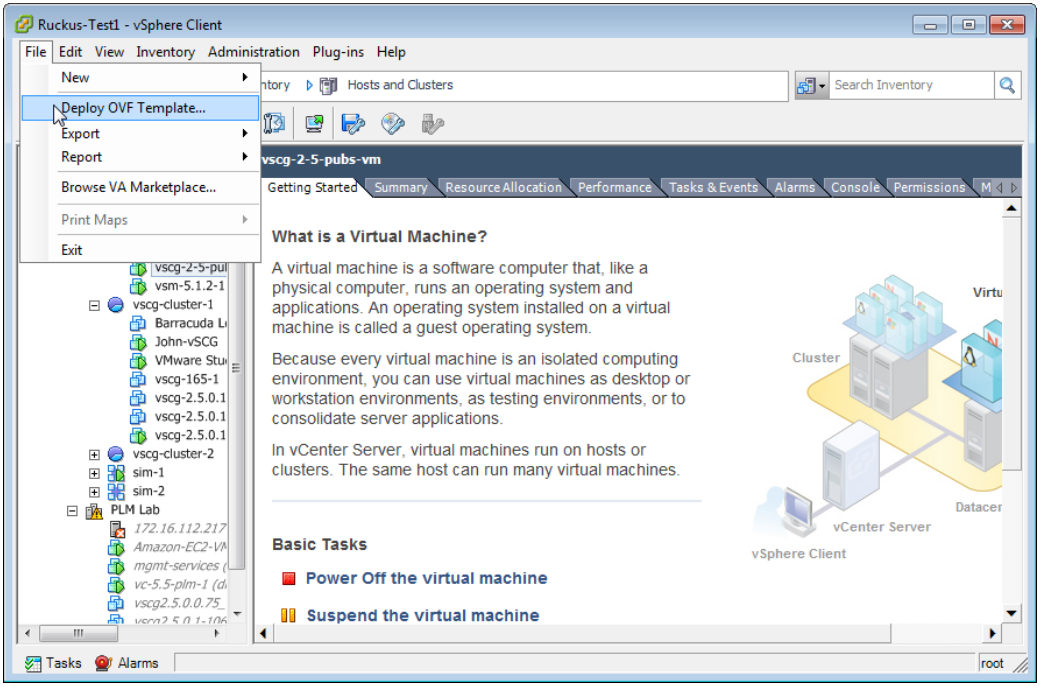
Before continuing, make sure you have already downloaded the vSCG distribution package from the Ruckus Wireless. See Obtaining the vSCG Distribution for more information.

NOTE: The following procedure describes how to create a vSCG instance using the vSphere Web Client.

Follow these steps to create a vSCG instance from the OVA file.

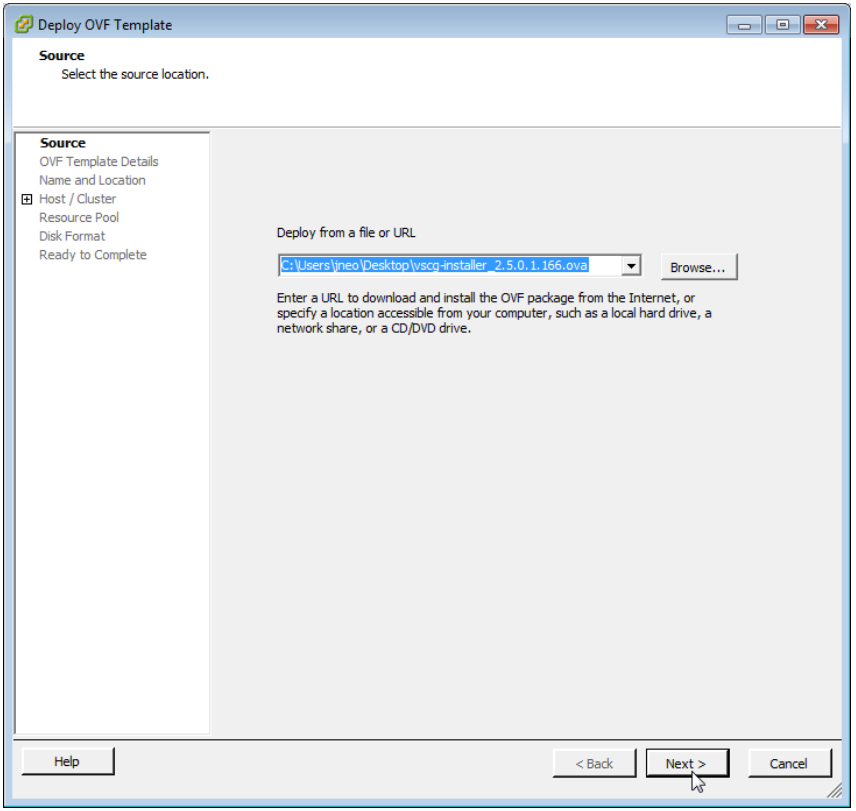
1. Use the VMWare vSphere client to log on to the ESXi management interface.
2. Click **File** > **Deploy OVF Template**. The *Source* screen of the *Deploy OVF Template* wizard appears.

Figure 1. Click Deploy OVF Template



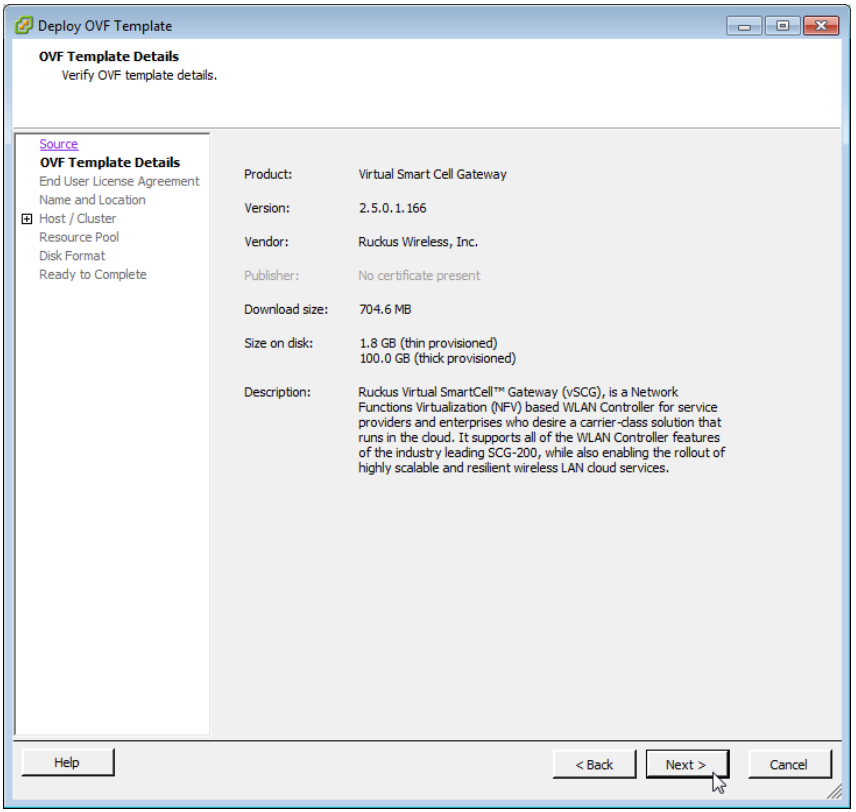
3 Click **Browse** to locate the `.ova` file that you downloaded earlier. Select the template.

Figure 2. Click Browse, and then locate and select .ova file



4 Click **Next**. The *OVF Template Details* screen appears.

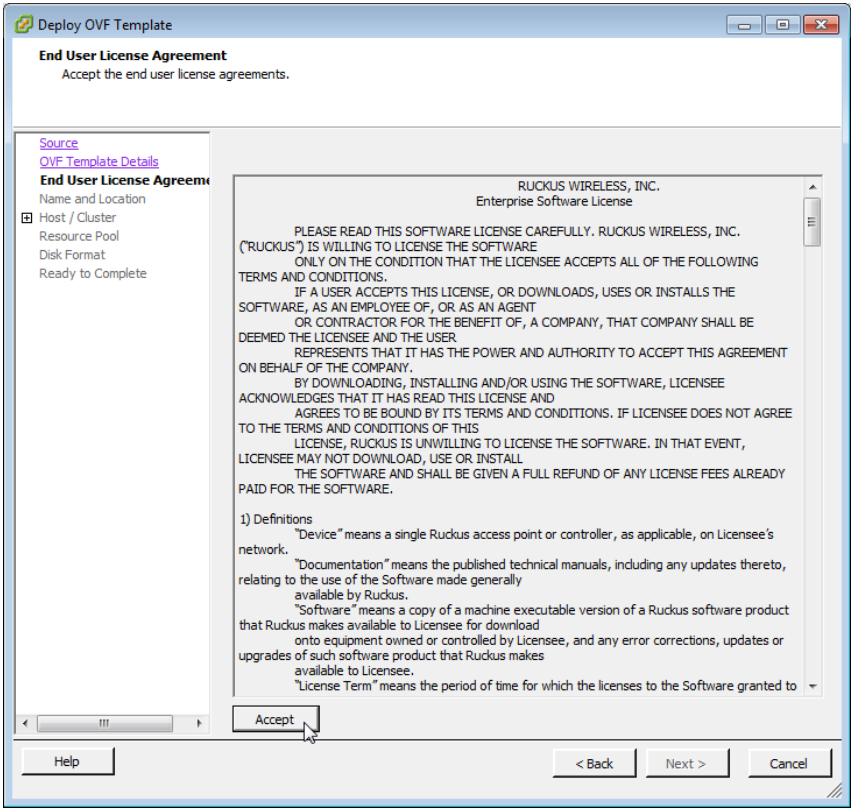
Figure 3. The OVF Template Details screen



5 Review the OVA virtual appliance details, and then click **Next**. The End User License Agreement (EULA) screen appears.

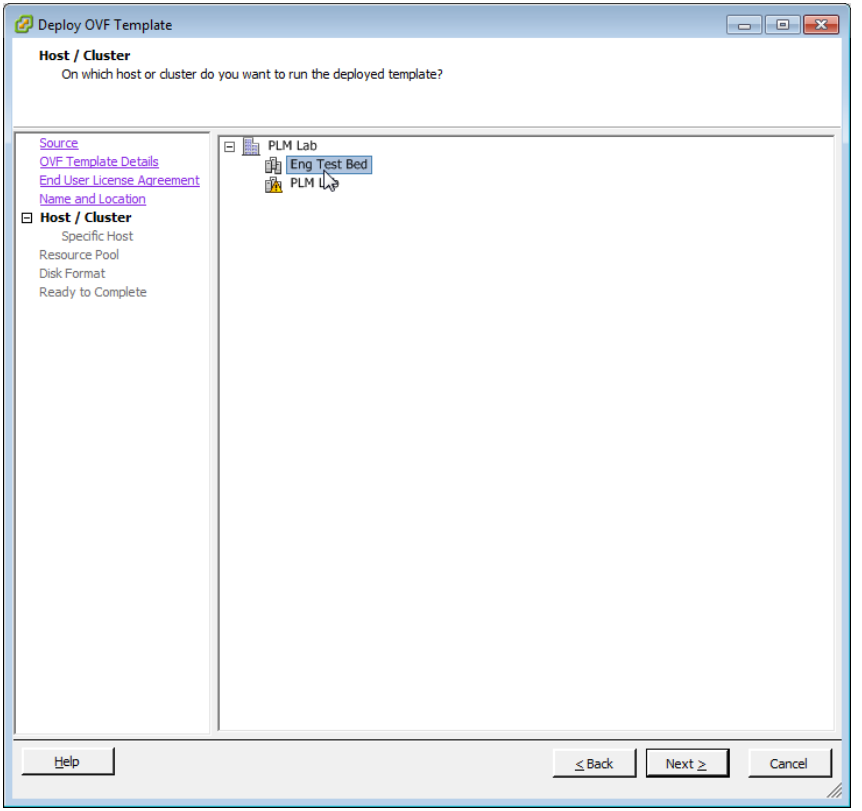
6 Click **Accept** to agree to the EULA terms, and then click **Next**. The *Host/Cluster* screen appears.

Figure 4. Accept the EULA for the vSCG OVA



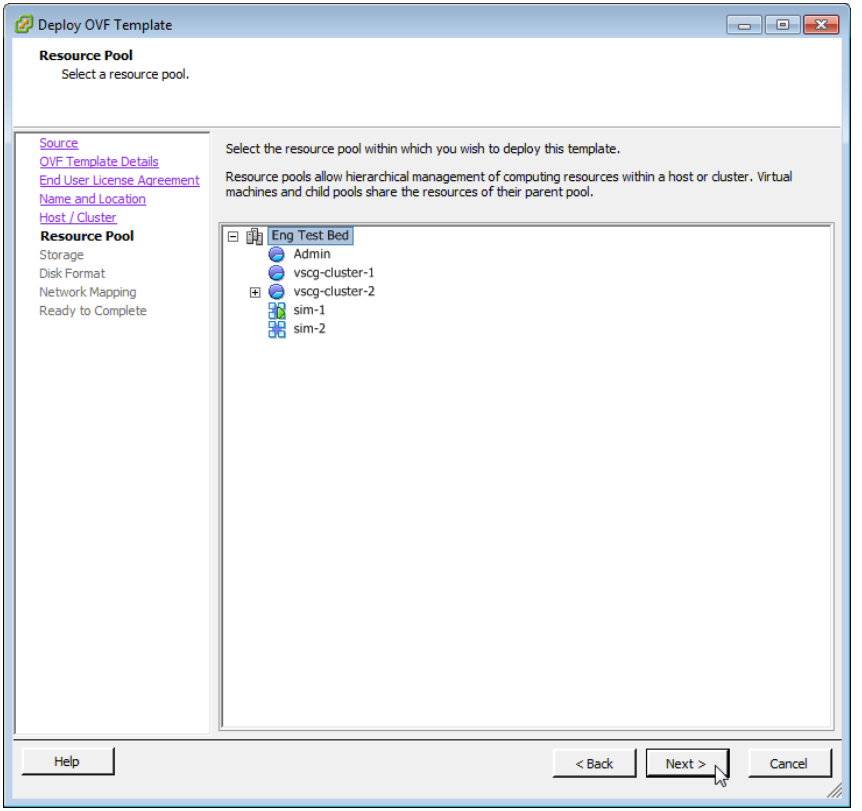
7 Select the host or cluster on which you want to run the deployed template, and then click **Next**. The *Resource Pool* screen appears.

Figure 5. Select the destination host or cluster



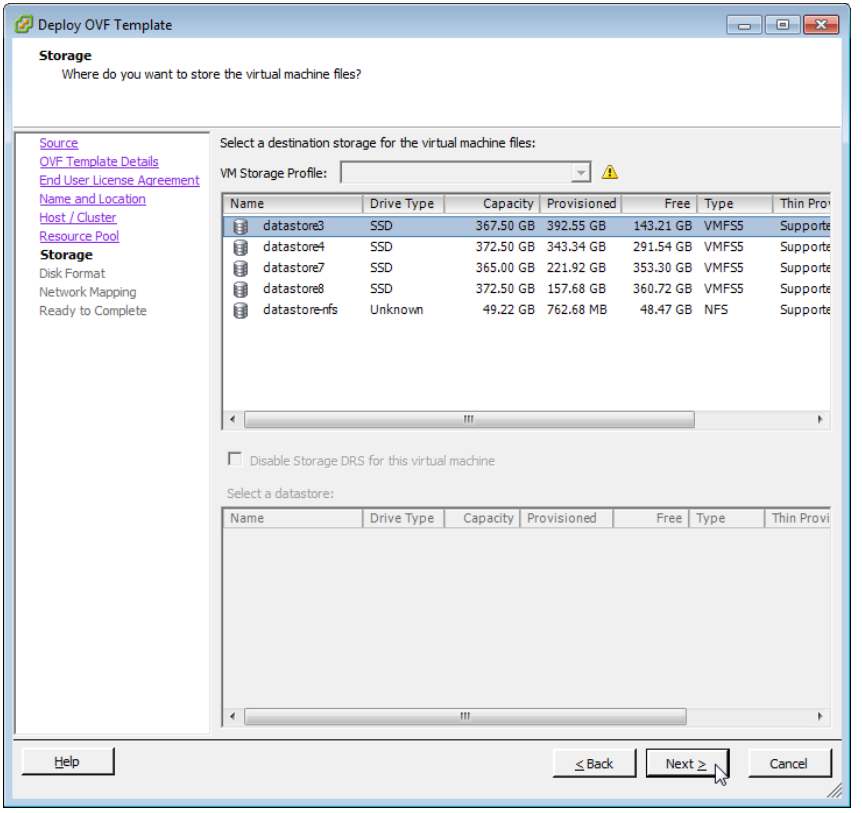
8 Select the resource pool within which you want to deploy the template, and then click **Next**. The storage screen appears.

Figure 6. Select the resource pool for the OVA template



9 Select the destination storage (data store) for virtual machine files, and then click **Next**. The *Disk Format* screen appears.

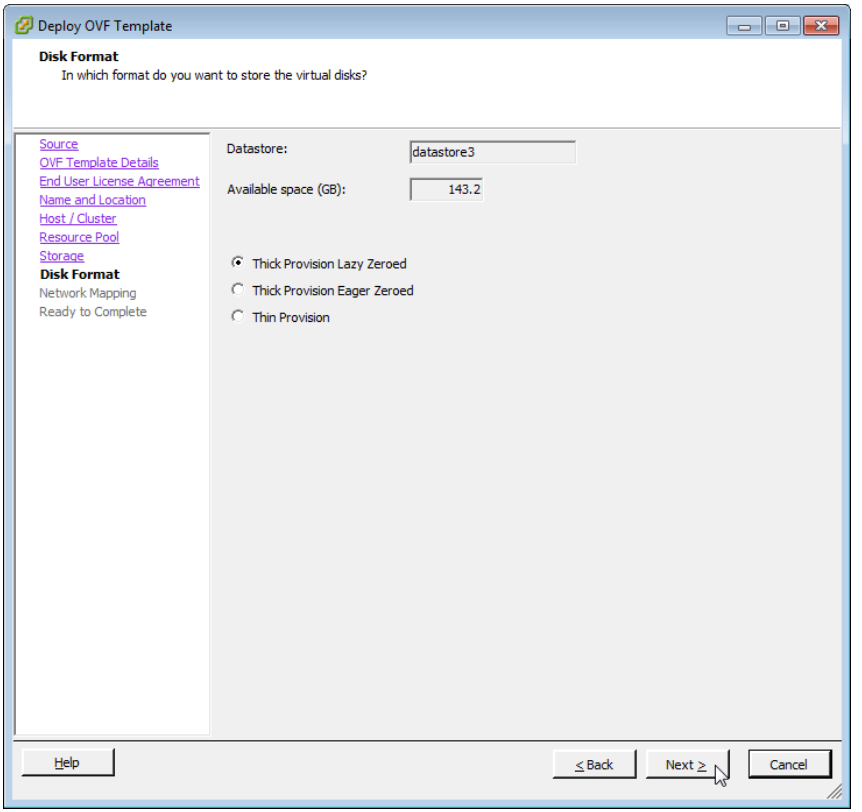
Figure 7. Select the data store for the virtual machine files



10 Select the disk format that is appropriate for your deployment scenario. Options include:

- Thick Provision Lazy Zeroed
- Thick Provision Eager Zeroed
- Thin Provision

Figure 8. Select the disk format for your deployment scenario

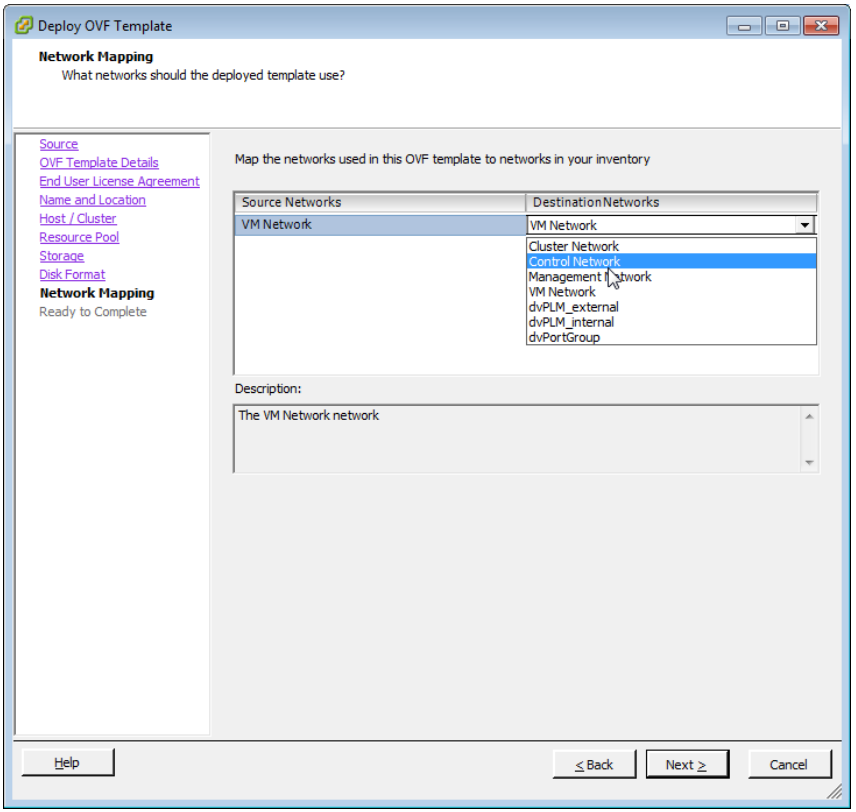


11 Click **Next**. The *Network Mapping* screen appears.

12 Select the ESXi virtual network interface that you want to use for the control interface, and then click **Next**. The *Ready to Complete* screen appears.

NOTE: The installation screen only allows you to select the virtual network interface for the control interface. After you complete the installation (and before you power on and set up the vSCG), you will need to adjust the cluster and management interfaces as appropriate.

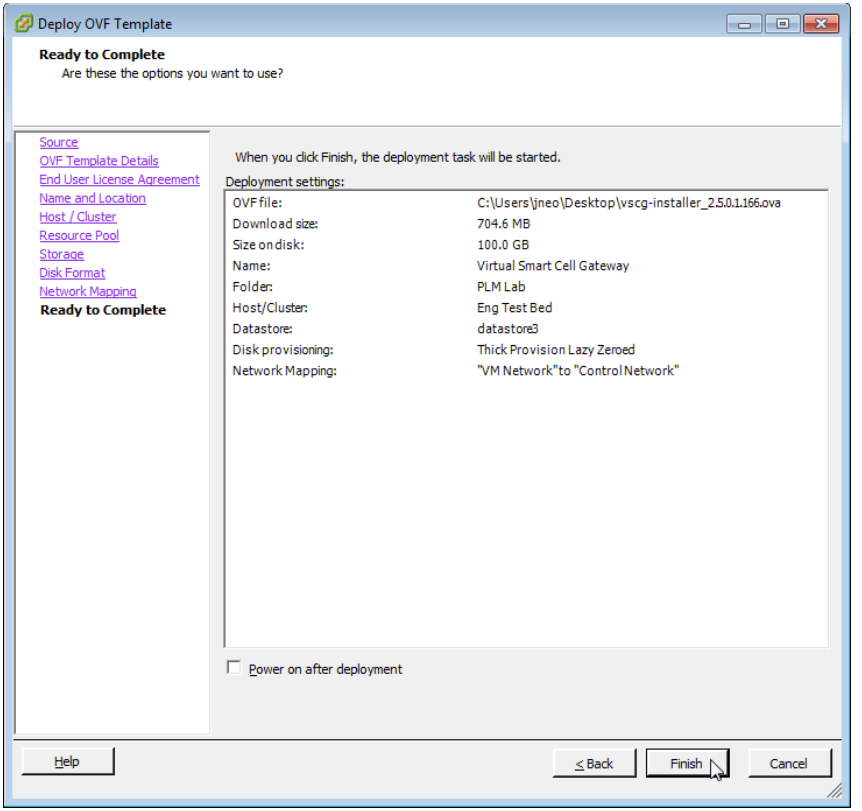
Figure 9. Select the virtual network interface that the template will use



13 Review the settings that you have configured on the previous screens.

If you find a setting that you want to change, click **Back** until you reach the screen where you can edit the setting. Update the setting, and then click **Next** until you reach the *Ready to Complete* screen again.

Figure 10. Review the settings that you have configured



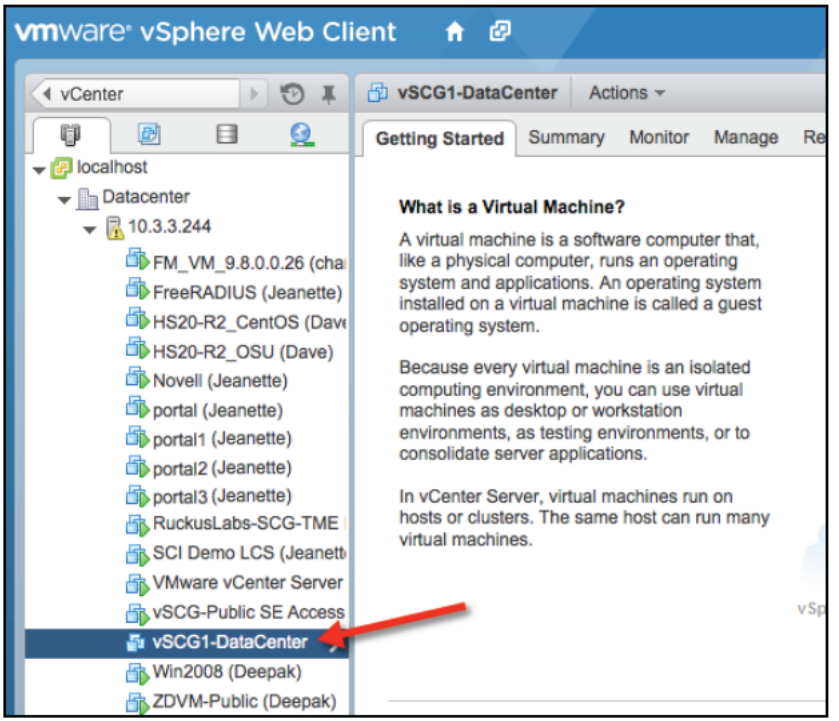
14 Make sure that the **Power on after deployment** check box is clear so you can adjust the network settings before the vSCG setup.

CAUTION! If you power on the vSCG after installation, you will no longer be able to adjust the network settings.

15 Click **Finish**.

ESXi deploys the new vSCG instance. When ESXi completes the deployment, the new vSCG instance appears on the list of installed virtual machines on the target host.

Figure 11. The vSCG instance appears on the list of installed VMs



You have completed creating a vSCG instance from the OVA file.

Allocating Resources and Assigning Network Interfaces

Before starting the vSCG instance for the first time, edit the virtual machine settings to allocate CPU and memory resources to the vSCG and to assign the ESXi network interfaces to the remaining vSCG interfaces (cluster and management).

Follow these steps to allocate resources and assign network interfaces to the vSCG.

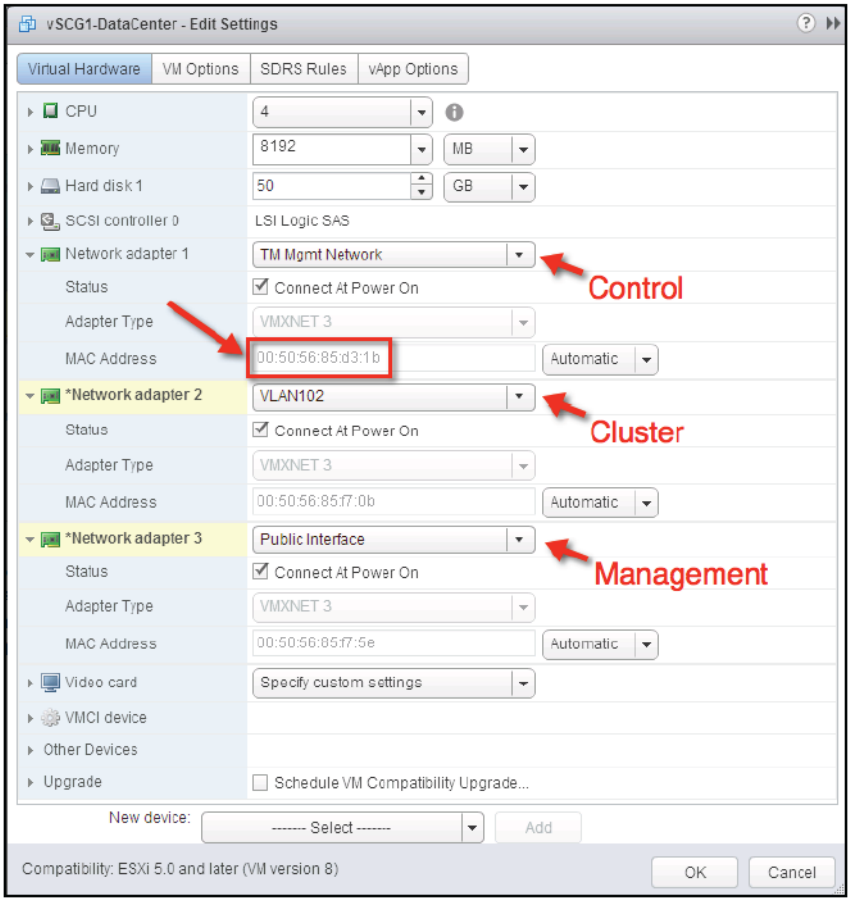
1. On the list of virtual machines, click the new vSCG instance.
2. Click **Actions** to display the additional options, and then click **Edit Settings**.
3. Set the number of CPUs and the amount of RAM to allocate to the vSCG instance. By default, the OVA template is set to 4 CPUs and 8GB of RAM.

4 Under *Network adapter 1*, verify that it is the same ESXi network interface that you selected for the control interface during the OVA import process. Ensure that the **Connect at Power On** check box is selected.

5 Under *Network adapter 2*, select the ESXi network interface for the cluster interface from the drop-down list. Ensure that the **Connect at Power On** option is selected.

6 Under *Network adapter 3*, select the ESXi network interface for the management interface from the drop-down list. Ensure that the **Connect at Power On** option is selected.

Figure 12. Select the interfaces to use



7 Click **OK**.

You have completed allocating resources and assigning network interfaces to the vSCG.

Configuring the Interfaces

The next step is to power on the vSCG virtual appliance and configure its interfaces.

1 From the list of virtual machines on the host, click the vSCG instance.

2 Under *Basic Tasks*, click **Power on the virtual machine**.

Figure 13. Click Power on the virtual machine

3 Open a console window to monitor the startup process. To do this, click the *Action* menu, and then click **Open Console**.

After the vSCG completes its startup process, you are ready to perform the initial IP address setup of the vSCG. You will use the console connection to perform this task.

Setting Up the vSCG Interface or Interfaces

The vSCG comes with the option to operate with either one (1) network interface or three (3) network interfaces. Therefore the procedure for setting up the vSCG interface depends on the number of interfaces that it has.

Follow the procedure below that corresponds to the number of interfaces that the vSCG you are installing has.

- Setting Up a vSCG with One Interface
- Setting Up a vSCG with Three Interfaces

NOTE: By default, the VMWare Esxi package comes with three network interfaces. If you want to deploy the vSCG with only one interface, you can edit the virtual machine settings to remove the extra interfaces. The KVM package, on the other hand, comes with a single interface. If you want to deploy the vSCG with three interfaces, edit the virtual machine settings to create two additional interfaces.

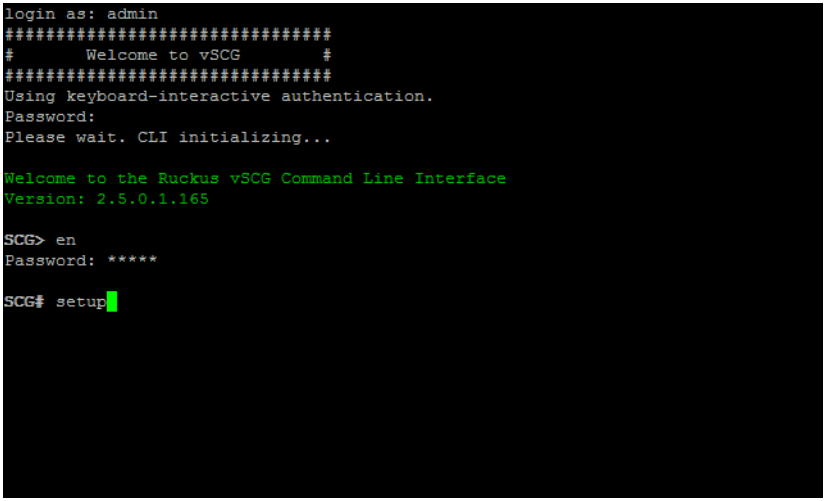
Setting Up a vSCG with One Interface

Follow these steps to set up the vSCG with a single network interface.

1. Log on to the console using the following credentials:
   - User name: admin
   - Password: admin
2. At the `SCG>` prompt, enter **`en`** to enable privileged mode.
3. At the `Password` prompt, enter **`admin`**. The `SCG#` prompt appears.
4. Enter **`setup`**. The console displays the current network settings (if any), and then displays the following prompt:

   ```
   Do you want to setup network? [YES/no]
   ```

Figure 14. At the SCG> prompt, enter setup



5 Enter **YES**. The next screen prompts you to select the profile configuration that you want to use for this instance of vSCG. The options include:

- Carrier
- Enterprise

6 Select the profile configuration that you want to use.

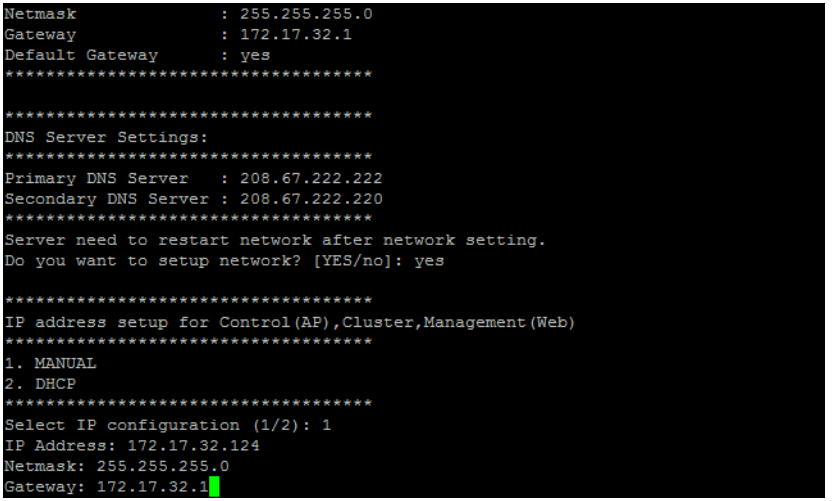
NOTE: If you selected Enterprise and the virtual machine has insufficient memory resources available (for example, the VM has only 8GB of RAM when the minimum RAM requirement is 10GB), you will be unable to continue with the setup process.

7 At the `Select IP configuration` prompt, enter **1** to set up the single vSCG interface (for Control [AP], Cluster, and Management [Web]) manually.

8 Configure the IP address, netmask, and gateway of the *control interface*, and the press **<Enter>**. The IP address configuration that you entered appears.

9 When the prompt `Are these correct? (y/n)` appears, enter **y** to confirm the IP address configuration.

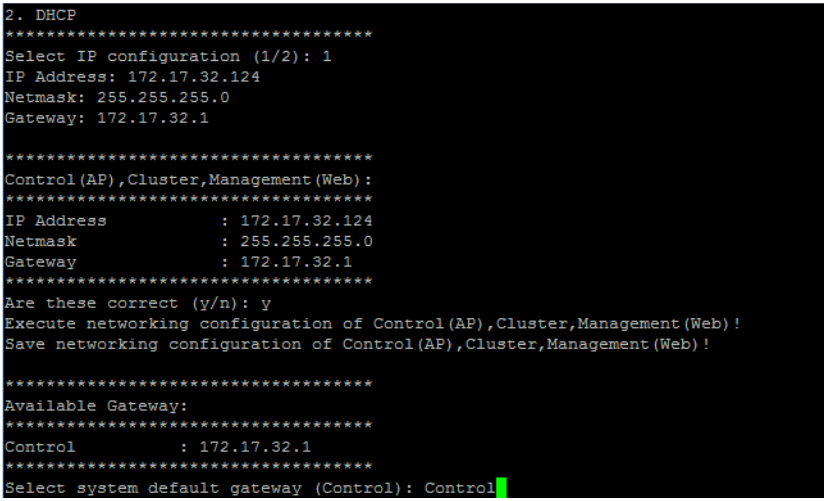
Figure 15. Configure the IP address settings of the single interface



10 When the prompt `Select system default gateway (Control, Cluster, Management)?` appears, enter **`Control`**.

NOTE: This entry is case-sensitive. Make sure you enter the system default gateway exactly as shown at the prompt.

Figure 16. When prompted for the system default gateway, enter Control

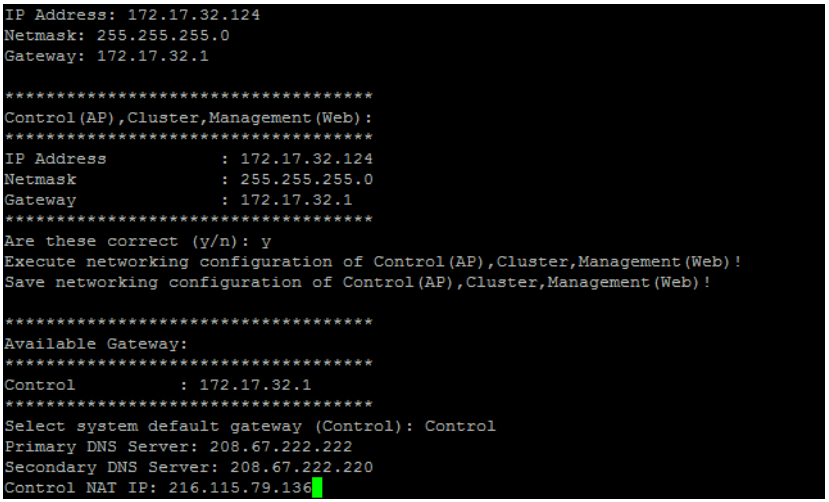


11 At the `Primary DNS Server` prompt, enter the primary DNS server on the network.

12 At the `Secondary DNS Server` prompt, enter the secondary DNS server (if any) on the network.

13 At the `Control NAT IP` prompt, enter the public IP address of the NAT server on the network. If you are not deploying the vSCG behind a NAT server, press `<Enter>` without typing an IP address.

Figure 17. Enter the public IP address of the NAT server (if any)



14 Enter **`restart network`**.

You have completed configuring the vSCG interfaces. You are now ready to run the vSCG Setup Wizard. See Using the Setup Wizard to Install vSCG

Setting Up a vSCG with Three Interfaces

1 Log on to the console using the following credentials:
   - User name: admin
   - Password: admin

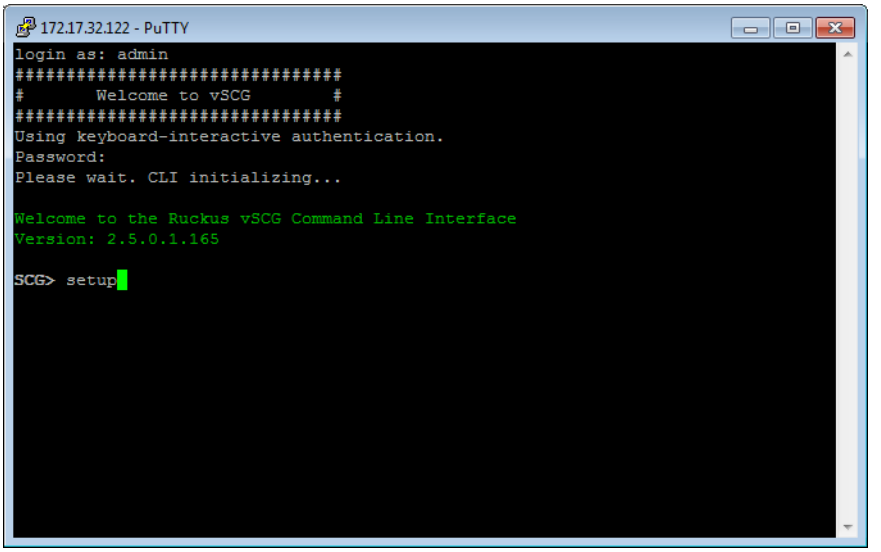
2 At the *SCG*> prompt, enter **`en`** to enable privileged mode.

3 At the `Password` prompt, enter **`admin`**. The SCG# prompt appears.

4 Enter **`setup`**. The console displays the current network settings (if any), and then displays the following prompt:

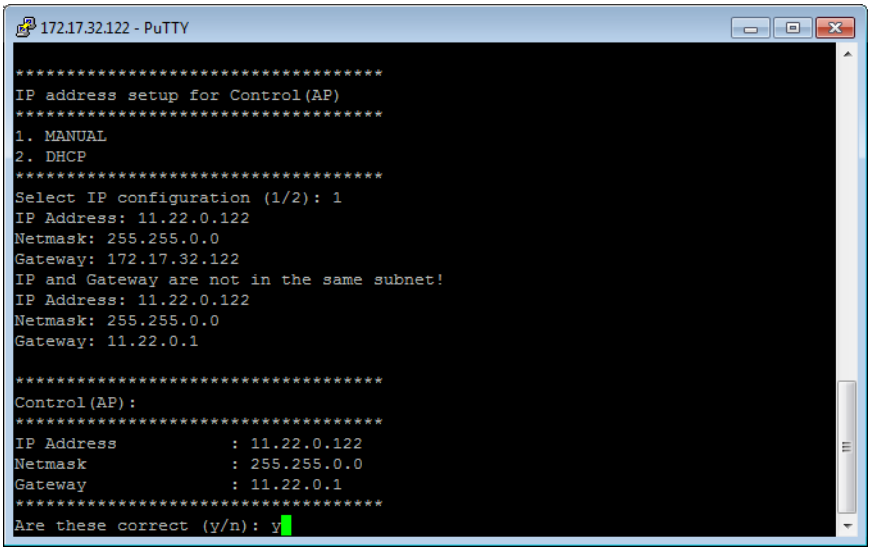
   `Do you want to setup network? [YES/no]`

Figure 18. At the SCG> prompt, enter setup



5 At the `Select IP configuration` appears prompt, enter **`1`** to set up the *control interface* manually.
   - **a** Configure the IP address, netmask, and gateway of the *control interface*, and the press <Enter>. The IP address configuration that you entered appears.
   - **b** When the message *Are these correct?* appears, enter **`y`** to confirm the IP address configuration.

Figure 19. Configure the IP address settings of the control interface



6 At the `Select IP configuration` prompt, enter **1** to set up the *cluster interface* manually.

   a Configure the IP address, netmask, and gateway of the *cluster interface*, and then press <Enter>. The IP address configuration that you entered appears.

   b When the message *Are these correct?* appears, enter **y** to confirm the IP address configuration.

7 At the `Select IP configuration` prompt, enter **1** to set up the *management interface* manually.

   a Configure the IP address, netmask, and gateway of the *management interface*, and the press <Enter>. The IP address configuration that you entered appears.

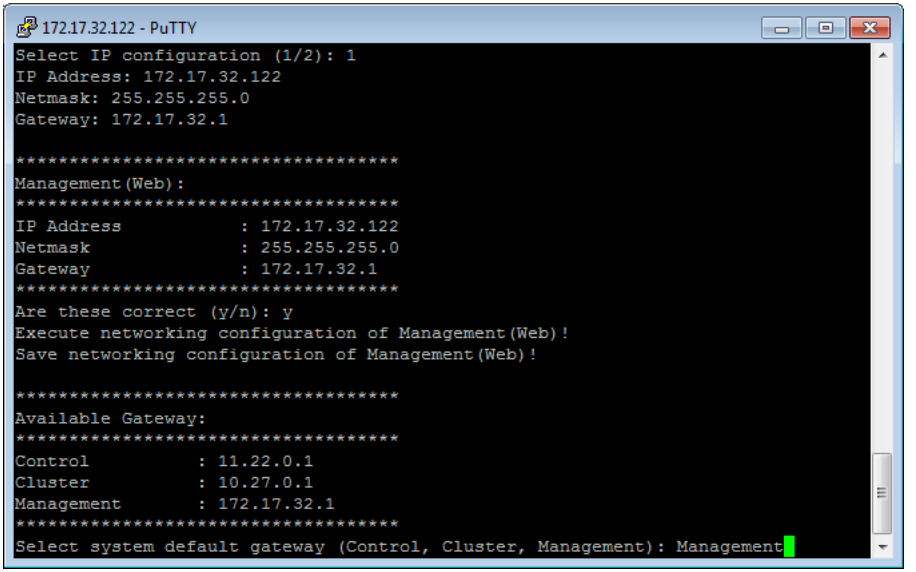
NOTE: Take note of the IP address that you assign to the management interface – you will use this IP address to log on to the vSCG web interface.

   b When the message *Are these correct?* appears, enter **y** to confirm the IP address configuration.

8 When the message `Select system default gateway (Control, Cluster, Management)?`, enter **`Control`** or **`Management`**, depending on your network topology (see Important Notes About Selecting the System Default Gateway).

NOTE: This entry is case-sensitive. Make sure you enter the system default gateway exactly as shown at the prompt.

Figure 20. When prompted for the system default gateway, enter either Management or Control (depending on your network design)



9 When prompted, enter the primary and secondary DNS server IP addresses.

10 Enter **`restart network`**.

You have completed configuring the vSCG interfaces. You are now ready to run the vSCG Setup Wizard. See Using the Setup Wizard to Install vSCG.

Important Notes About Selecting the System Default Gateway

Depending on your network topology, you may select either the **Management** or **Control** interface as the system default gateway.

- If all of the managed APs are located in different locations on the Internet, the vSCG may not know all of the IP subnets of these APs. In this case, the control interface should be set as the default gateway for the vSCG and you will need to add a static route to reach the management network.
- If all of the managed APs belong to a single subnet or to multiple subnets on which you can set the route statically, then you can set the management interface as the default gateway users can set default gateway for the vSCG and set static routes for the vSCG to reach all of its managed APs.

Installing the vSCG on a Kernel-based Virtual Machine Hypervisor

This section describes how to install the vSCG on a KVM hypervisor.

- Extracting the vSCG Image
- Setting Up the vSCG

Extracting the vSCG Image

The vSCG image for a kernel-based virtual machine (KVM) is distributed in QCOW2 format.

1 Obtain the vSCG image in QCOW2 format.

2 Copy the image to the KVM.

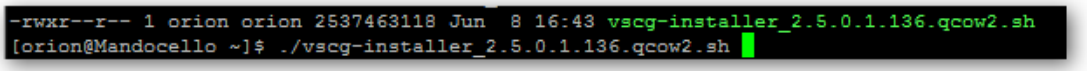
3 Extract the contents of the QCOW2 image by running the following command:

`vscg-installer_2.5.0.1.<build number>.qcow2.bin`

In the example in Figure 21, the actual command is:

`./vscg-installer_2.5.0.1.136.qcow2.bin`

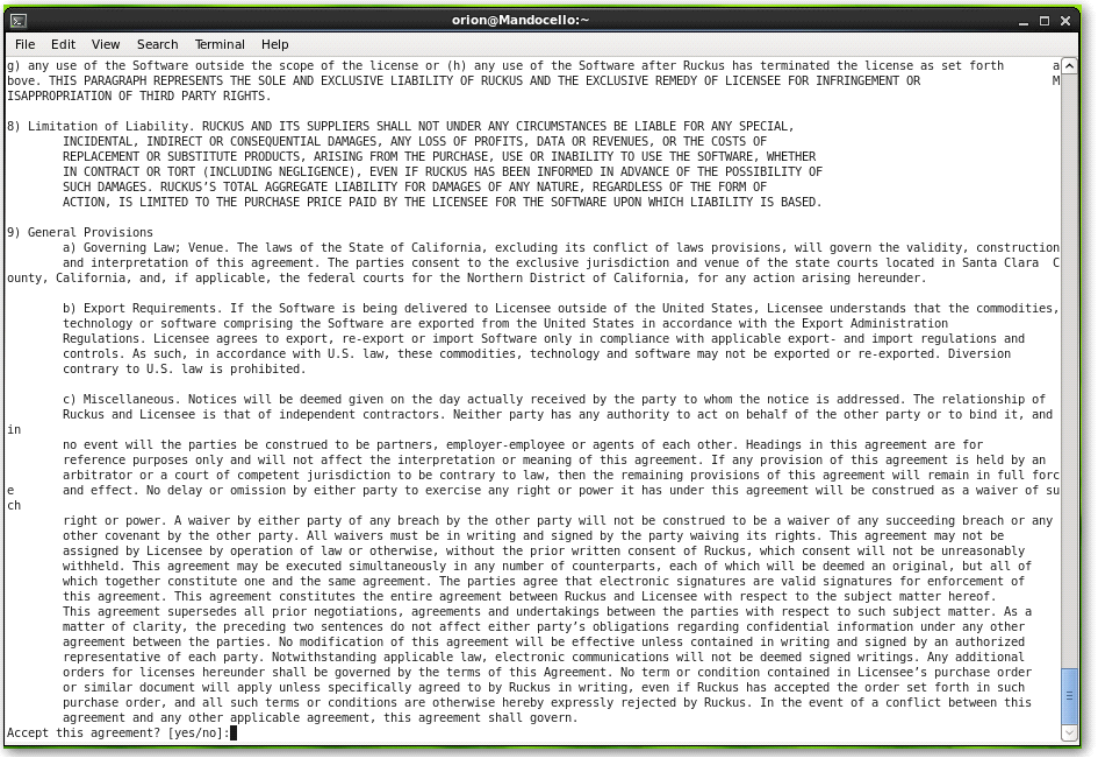
Figure 21. Extract the contents of the QCOW2 image



The end user license agreement appears on screen.

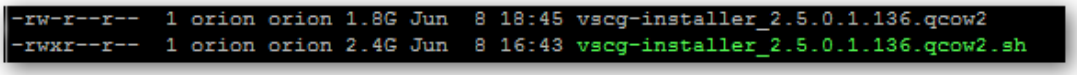
4 At the `Accept this agreement? [yes/no]` prompt, enter **`yes`**.

Figure 22. Accept the EULA terms



The KVM continues to extract the contents of the image. When the extraction process is complete, the QCOW2 file appears in the same directory as the .sh file.

Figure 23. The QCOW2 file appears in the same directory as the .sh file



NOTE: If the "uudecode: command not found" error appears during the extraction process, install the "sharutils" package on the KVM, and then retry extracting the image.

5 Resize the vSCG disk image, if necessary. By default, the vSCG disk size is 50GB. If you want to allocate more disk space to the vSCG, run the `qemu-img` command. The complete syntax is as follows:

`qemu-img resize <vSCG QCOW2 disk image> +size`

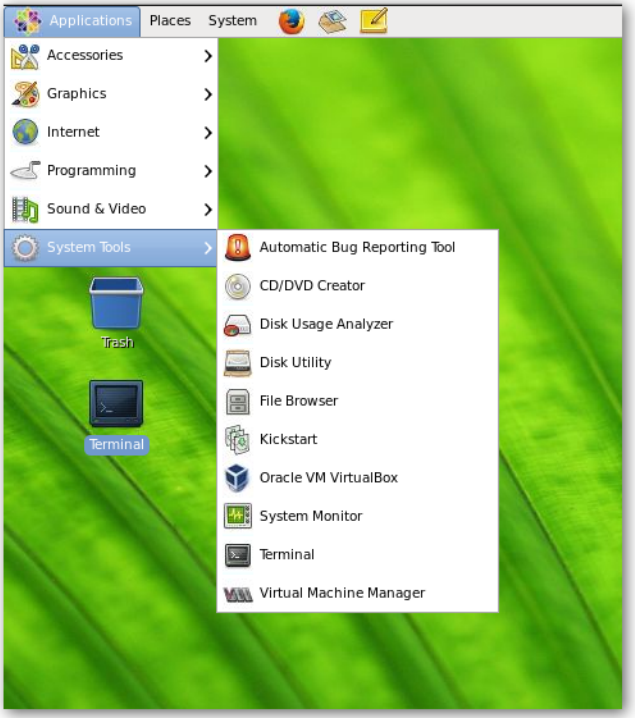
Setting Up the vSCG

This section describes how to set up the vSCG using the Red Hat Virtual Machine Manager (also known as "virt-manager"). If you are installing the vSCG on a different hypervisor or virtual machine monitor, the procedure may be slightly different. Refer to the hypervisor documentation for more information.

Follow these steps to set up the vSCG on the Virtual Machine Manager.

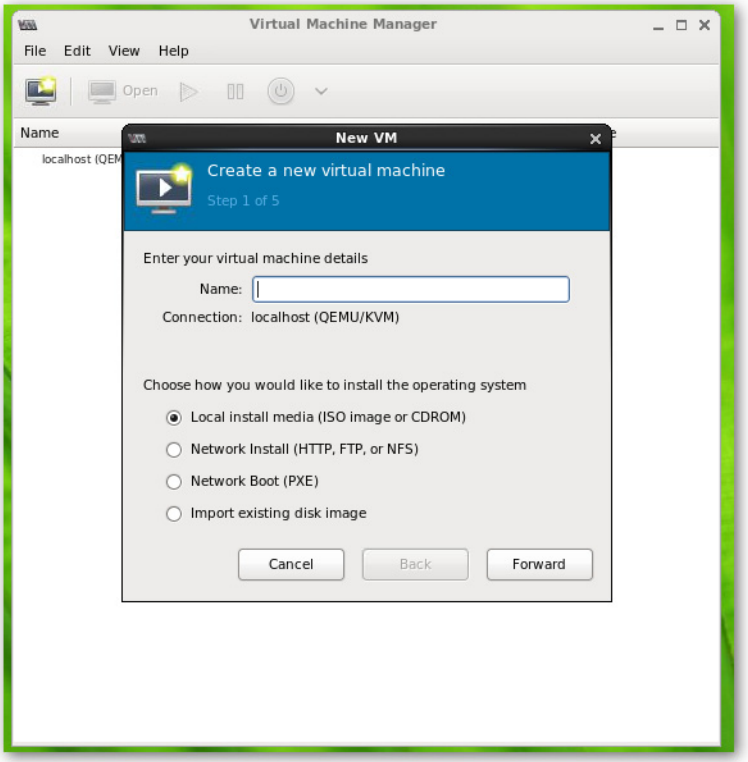
1 Start the Virtual Machine Manager by clicking **Applications** > **System Tools** > **Virtual Machine Manager**. The Virtual Machine Manager interface appears.

Figure 24. Start the Virtual Machine Manager



2 In *File*, click **Create New VM**. The *New VM* screen appears.

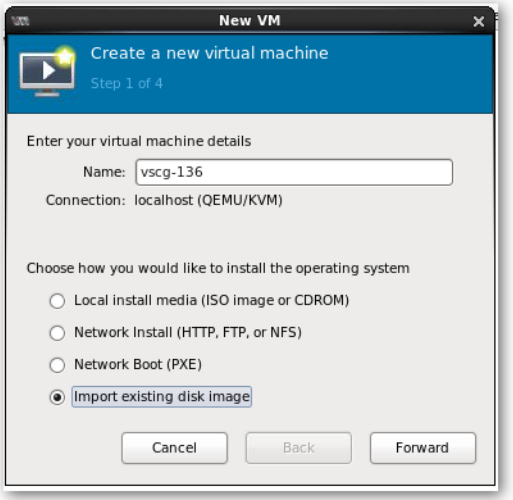
Figure 25. After you click Create New VM, the New VM screen appears



3 Configure the options on the *New VM (Step 1 of 4)* screen.

- In *Name*, type a name that you want to assign to the virtual machine.
- In *Choose how you would like to install the operating system*, click **Import existing disk image**.

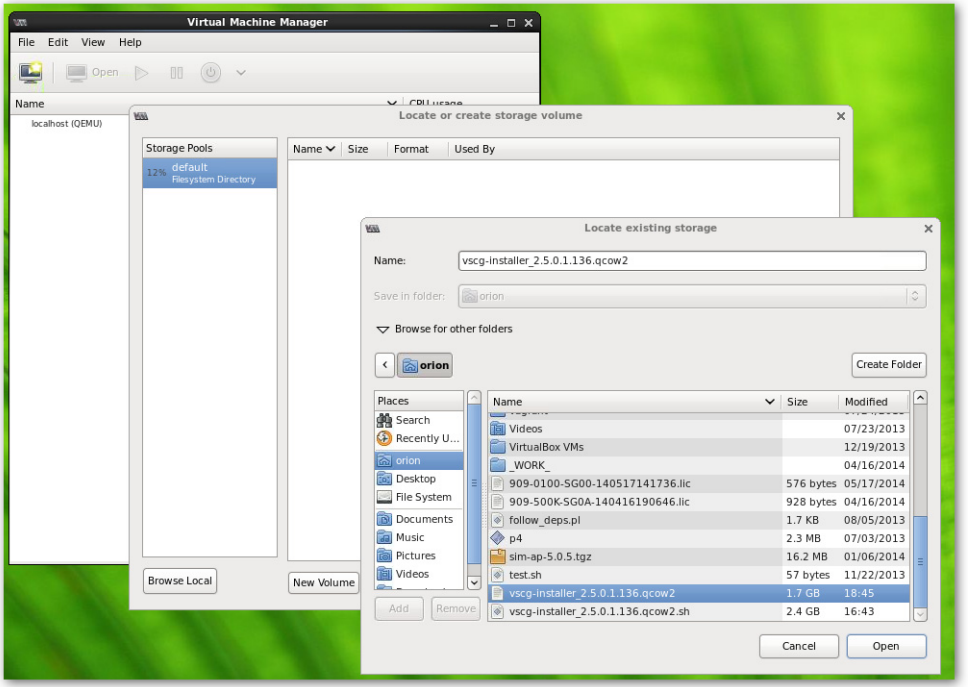
Figure 26. Type a name and select how you want to install the operating system



4 Click **Forward**. The *Locate Existing Storage* dialog box appears.

5 Browse to the location of the vSCG QCOW2 image, select the image file, and then click **Open**. The *New VM (Step 2 of 4)* screen reappears and displays the storage path to the QCOW2 image file that you selected.

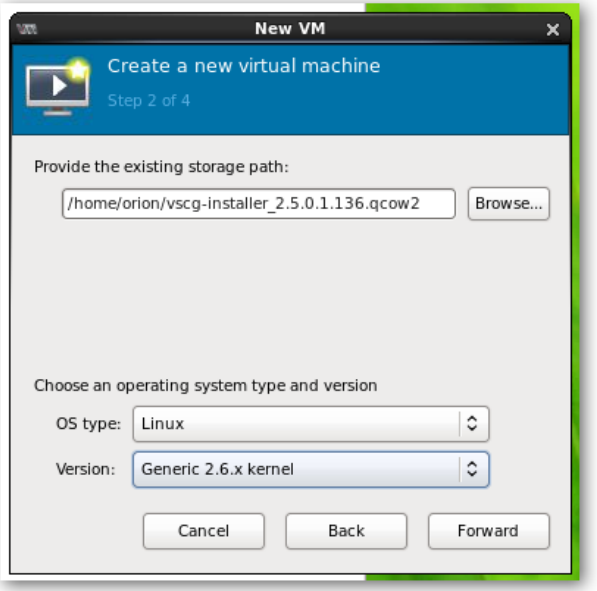
Figure 27. Browse to the vSCG QCOW2 image



6 In the lower portion of the *New VM (Step 2 of 4)* screen, select the operating system type and version.

- In *OS type*, select **Linux**.
- In *Version*, select **Generic 2.6.x kernel**.

Figure 28. Select the operating system and version



7 Click **Forward**. The *New VM (Step 3 of 4)* screen appears.

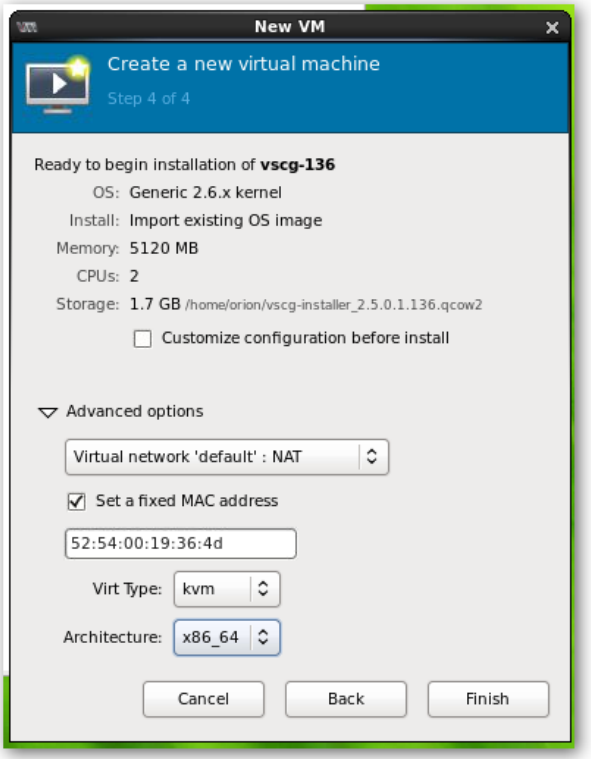
8 Configure the memory and CPU settings of the virtual machine.

- In *Memory (RAM)*, set to memory (in MB) that you want to allocate to the vSCG.
- In *CPU*, set the number of CPUs that you want to allocate to the vSCG.

Figure 29. Configure the memory and CPU settings

9 Click **Forward**. The *New VM (Step 4 of 4)* screen appears and displays a summary of the settings you configured.

Figure 30. A summary of the settings you configured appears



10 Verify that the settings you configured on the previous screens are correct. If you need to make changes to any of the settings, click **Back** until you reach the screen on which the setting appears, make the change, and then click **Forward** until you reach the *New VM (Step 4 of 4)* screen again.

11 Click **Finish** to install the vSCG on the virtual machine.

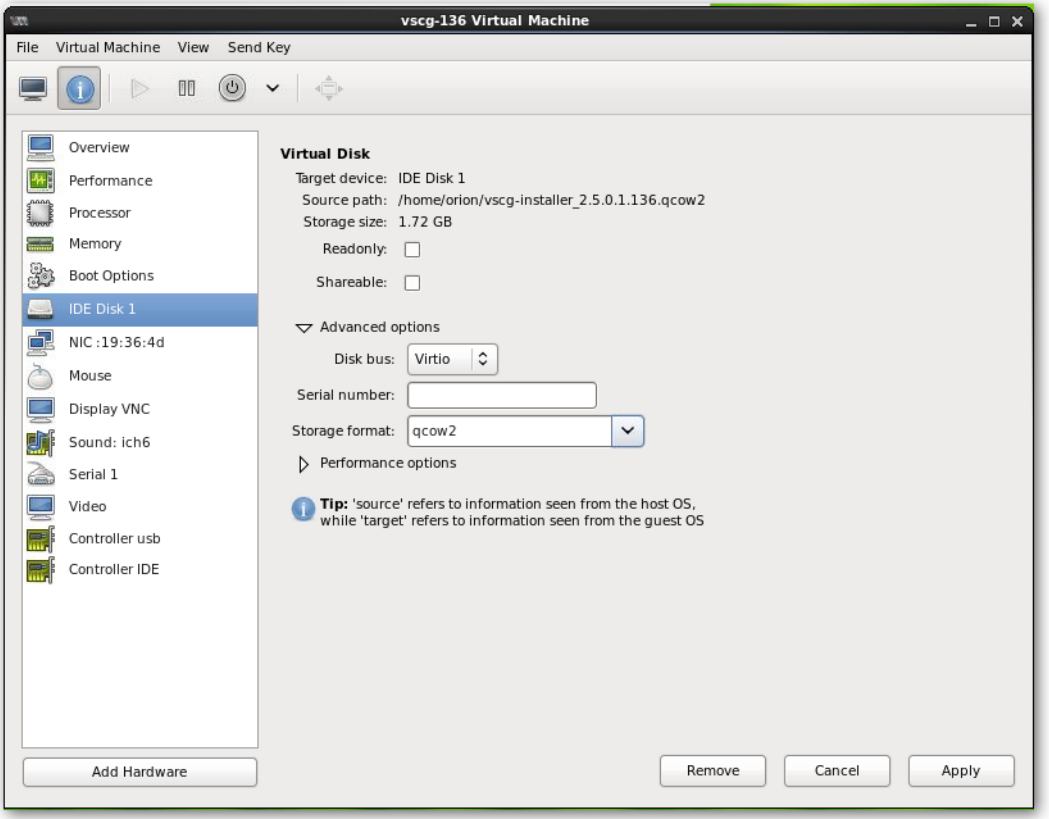
12 After you complete installing the vSCG on the virtual machine, decide how many interfaces you want the vSCG to use. The vSCG supports either a single interface or three interfaces. By default, a single interface exists after installation.

- If you want the vSCG to use a single interface, you do not need to take action in this step. Continue to the next step.

- If you want the vSCG to use three interfaces, you must create the two additional interfaces before the initial bootup of the vSCG. Once the vSCG has completed its initial bootup, you will no longer be able to change the number of interfaces.

CAUTION! If you want to add interfaces, you must do so before the initial bootup of the vSCG. After the initial bootup, you will no longer be able to change the number of interfaces.

Figure 31. By default, a single interface exists



13 Power on the virtual machine. The vSCG performs its initial bootup.

14 When the `SCG login` prompt appears, enter **`admin`**.

You have completed setting up the vSCG on a KVM hypervisor. You are now ready to start the vSCG Setup Wizard. See Using the Setup Wizard to Install vSCG for more information.

Using the Setup Wizard to Install vSCG

3

In this chapter:

- Before You Begin
- Step 1: Start the Setup Wizard and Set the Language
- Step 2: Select the Profile Configuration That Corresponds to Your vSCG License
- Step 3: Configure the Management IP Settings
- Step 4: Configure the Cluster Settings
- Step 5: Set the Administrator Password
- Step 6: Verify the Settings
- Logging On to the Web Interface

Before You Begin

The Setup Wizard helps you perform the initial configuration of the vSCG by presenting the vSCG configuration options in a set of easy-to-complete screens.

The Setup Wizard will prompt you to select one of the two available profile configurations (carrier profile and enterprise profile). You must select the profile configuration that corresponds to the vSCG license that you purchased.

Before you start the Setup Wizard, make sure you know the profile configuration that you need to select. If you are unsure which profile configuration you need to select, contact Ruckus Wireless Support.

Follow these steps to run and complete the vSCG Setup Wizard for the carrier profile configuration:

Step 1: Start the Setup Wizard and Set the Language

Step 3: Configure the Management IP Settings

Step 4: Configure the Cluster Settings

Step 5: Set the Administrator Password

Step 6: Verify the Settings

Step 1: Start the Setup Wizard and Set the Language

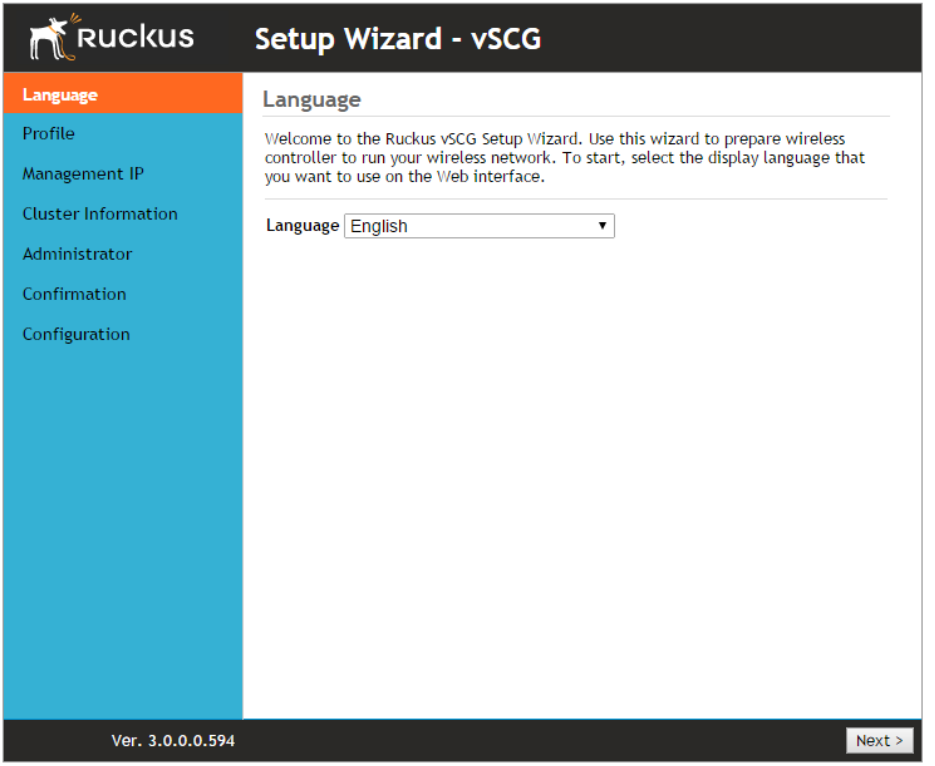
1 Start your web browser, and then enter the following in the address bar:

`http://{management-IP-address}:8080`

where management-IP-address is the address you assigned to the management interface.

The vSCG Setup Wizard appears, displaying the *Language* page.

Figure 32. The Language page



2 Select your preferred language for the vSCG web interface. Available options include:

- English
- Traditional Chinese

- Simplified Chinese

3 Click **Next**. The *Profile* page appears.

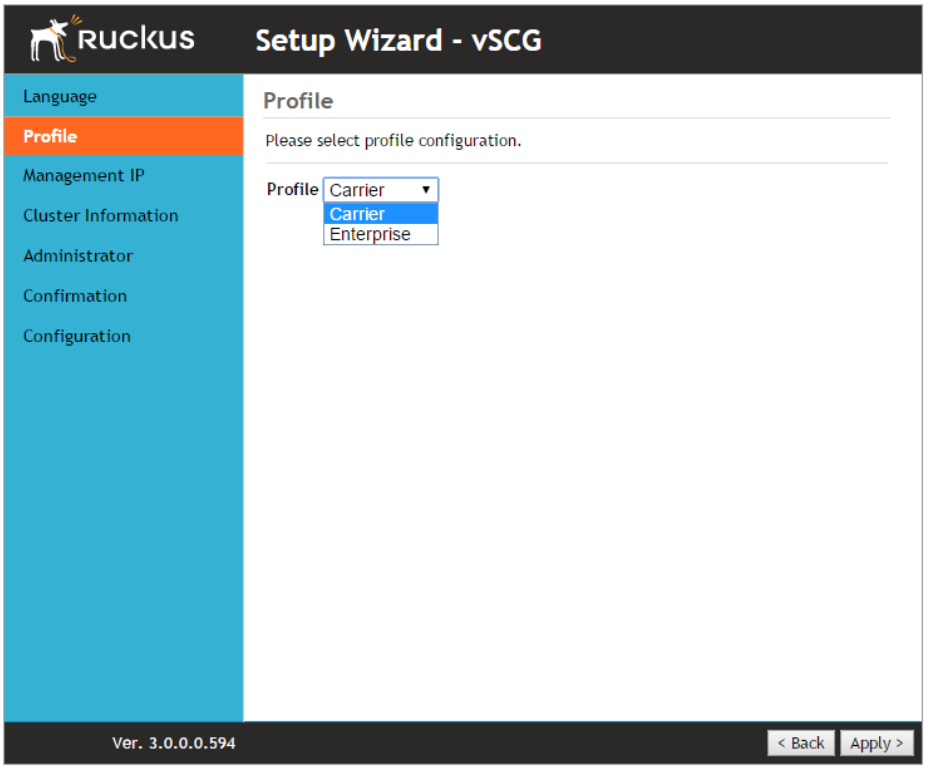
Step 2: Select the Profile Configuration That Corresponds to Your vSCG License

1 Select the profile configuration that corresponds to the vSCG license that you purchased. Available profile configurations include:

- Carrier
- Enterprise

2 Click **Next**. The *Management IP* page appears.

Figure 33. The Profile page



Step 3: Configure the Management IP Settings

NOTE: The vSCG comes in either a single network interface or three network interfaces (one interface each for Control (AP), Cluster, and Management (Web) traffic). The following procedure assumes that the vSCG you are installing uses a single network interface.

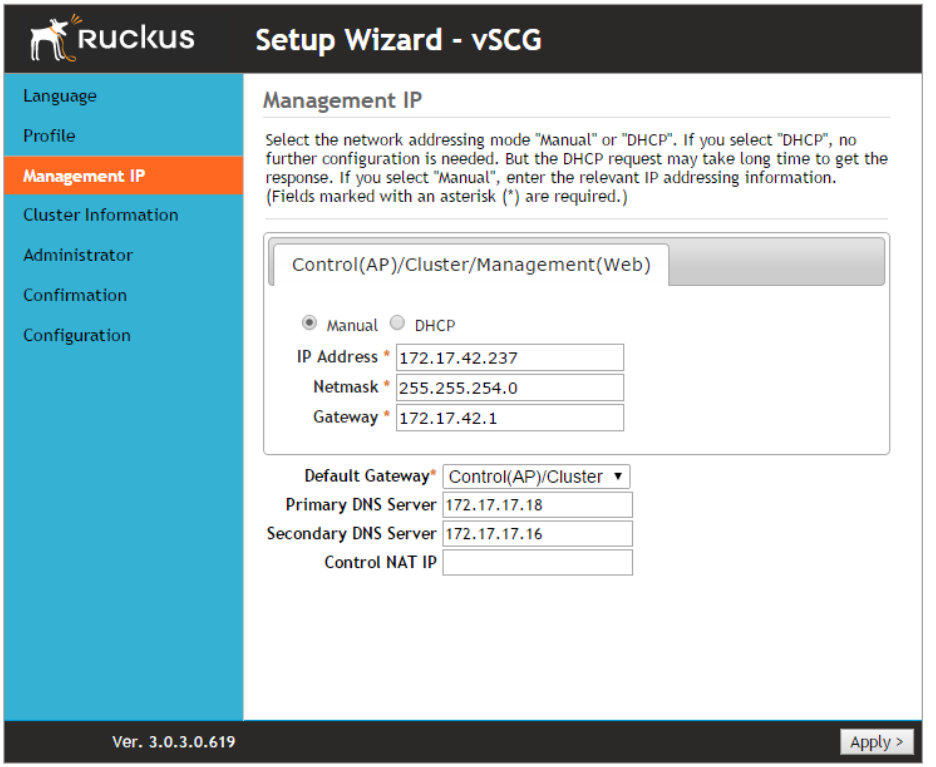
WARNING! If the vSCG that you are installing comes with three network interfaces, you must configure each of the three SCG interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

1 On the *Control(AP)/Cluster/Management(Web)* tab, click **Manual**.

2 Enter the network settings that you want to assign to the Management (Web) interface through which management traffic will be sent and received. The following network settings are required (others are optional):

- IP address
- Netmask
- Default gateway

Figure 34. The Management IP page



NOTE: : Although it is possible to use DHCP to assign IP address settings to the Management (Web) interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

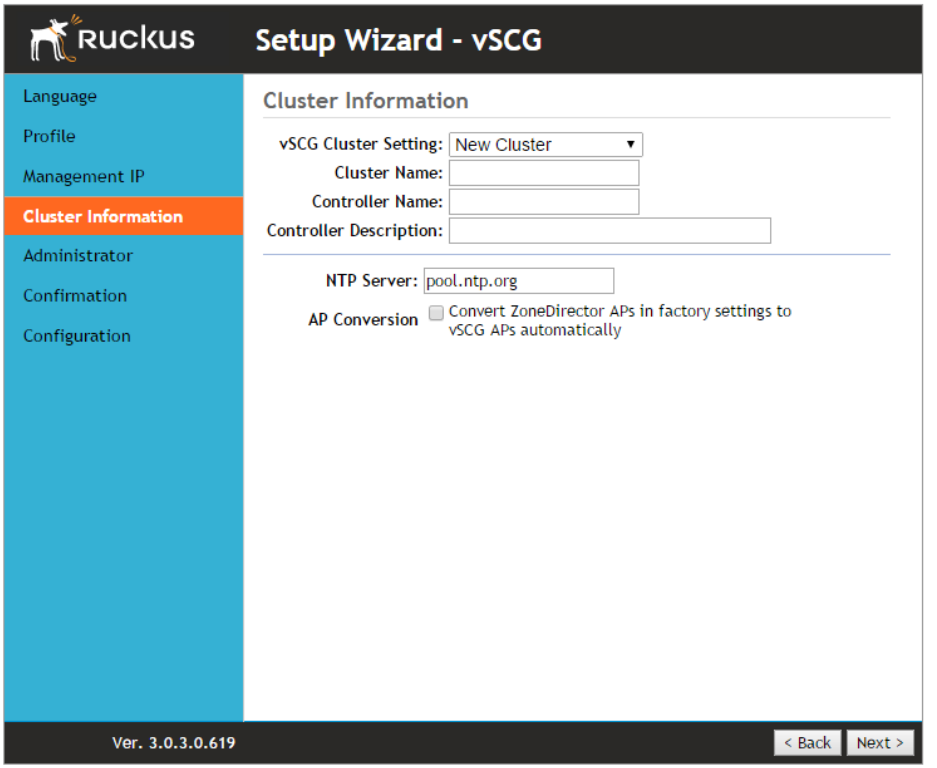
3 Click **Apply**. The *Cluster Information* page appears.

Step 4: Configure the Cluster Settings

The next step is to configure the vSCG cluster settings. The actions that you need to perform in this step depends on whether you are creating a new cluster (with this vSCG as the first node) or you are setting up this vSCG to join an existing cluster.

- If This vSCG Is Forming a New Cluster
- If This vSCG Is Joining an Existing Cluster

Figure 35. The Cluster Information page, showing the New Cluster option



If This vSCG Is Forming a New Cluster

Follow these steps if you want to use this vSCG to create a new cluster.

1 On the *Cluster Information* page, configure the following settings:

- In *vSCG Cluster Setting*, select **New Cluster**.
- In *Cluster Name*, type a name that you want to assign to this new cluster.

NOTE: The *Cluster Name* and *Controller Name* boxes only accept alphanumeric characters, hyphens (-), and underscores (_). They do not accept the space character or other special characters (for example, $, *, #, !).

- In *Controller Name*, type a name for the vSCG controller in this new cluster.
- In *Controller Description*, type a description for the vSCG controller.
- In *NTP Server*, type the address of the NTP server from which members of the cluster will obtain and synchronize time. The default NTP server is `pool.ntp.org`.

CAUTION! Before continuing, verify that the cluster settings are correct. Once the cluster is created, you will be unable to edit its settings without rebuilding the cluster from scratch.

2 Click **Next** to continue to the *Administrator* page (see Step 5: Set the Administrator Password).

If This vSCG Is Joining an Existing Cluster

If this is not the first vSCG cluster on the network, you can set up this vSCG virtual appliance to join an existing cluster.

CAUTION! To add this vSCG to an existing cluster, the entire target cluster must be in a healthy state (no node must be in “out of service” state). If any member node is out of service, the join request will fail. You will need to remove any out-of-service node from the cluster before you can add a new node successfully.

Follow these steps to configure this vSCG to join an existing cluster.

1 In *vSCG Cluster Setting*, select **Join Existing Cluster**.

2 In *Cluster Name*, type the name of the cluster that this vSCG is joining.

NOTE: The *Cluster Name* and *Controller Name* boxes only accept alphanumeric characters, hyphens (-), and underscores (_). They do not accept the space character or other special characters (for example, $, *, #, !).

3 In *Controller Name (optional)*, type the name of the vSCG controller in the existing cluster.

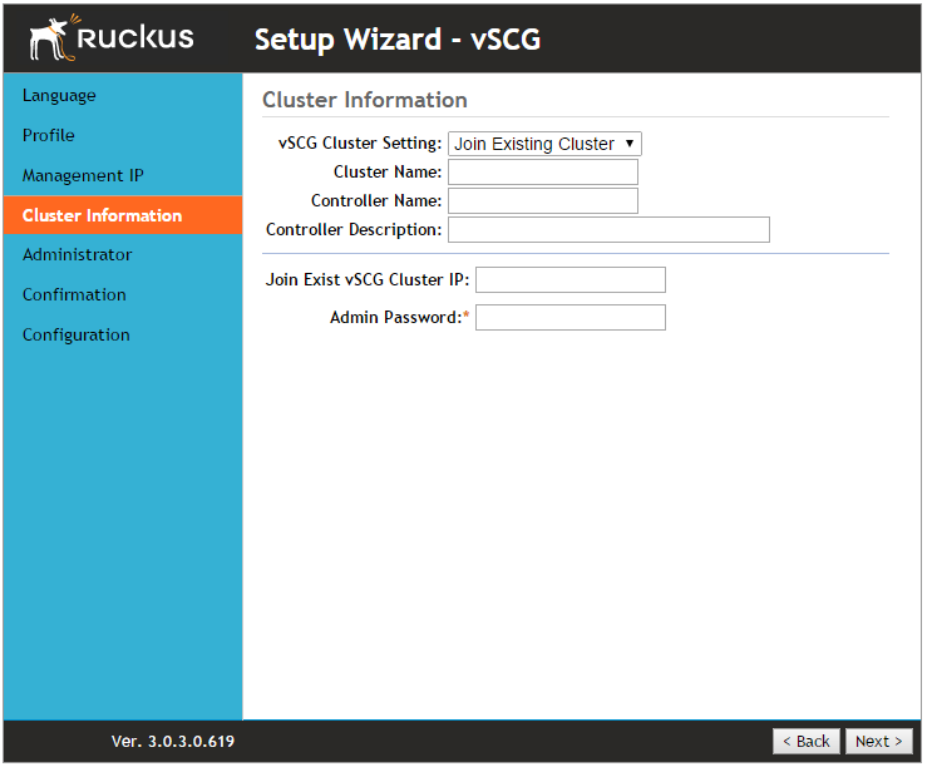
4 In *Controller Description (optional)*, type a description for the vSCG controller.

5 In *Join Exist vSCG Cluster IP*, type the IP address of the leader in the existing cluster.

6 In *Admin Password*, type the administrator password to the web interface of the leader node.

7 Click **Next** to continue to the *Administrator* page (see Step 5: Set the Administrator Password).

Figure 36. The Cluster Information page, showing the Join Existing Cluster option



NOTE: If the firmware version on this vSCG (shown in the lower left area of the *Cluster Information* page) does not match the firmware version of the cluster, a message appears and prompts you to upgrade the vSCG firmware. Click **Upgrade**, and then follow the prompts to perform the upgrade.

Step 5: Set the Administrator Password

1 On the *Administrator* page, configure the web interface and CLI passwords. All fields are required.

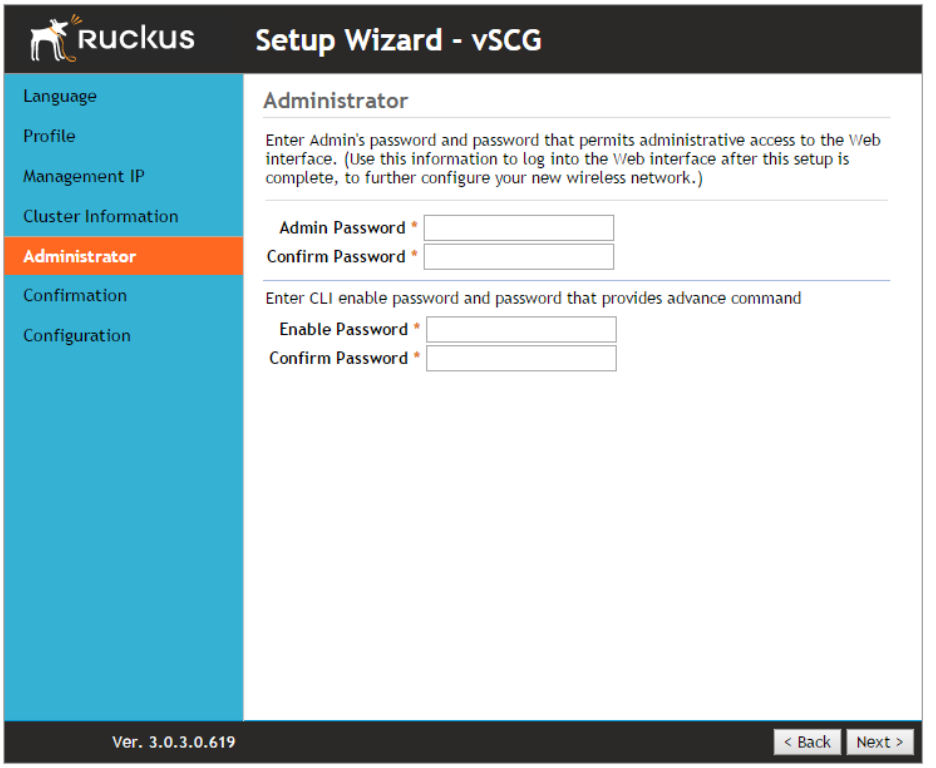
- *Admin Password*: Type a password that you want to use to access the web interface.
- *Confirm Password*: Retype the password above to confirm.
- *Enable Password*: Type a password that you want to use to enable CLI access to the vSCG.
- *Confirmation Password*: Retype the password above to confirm.

NOTE: The web interface and CLI passwords must be at least eight (8) characters and must include one number, one letter, and one special character (for example, $, *, #, !).

---

2 Click **Next** to continue. The *Confirmation* page appears and displays all the vSCG settings that you have configured using the Setup Wizard.

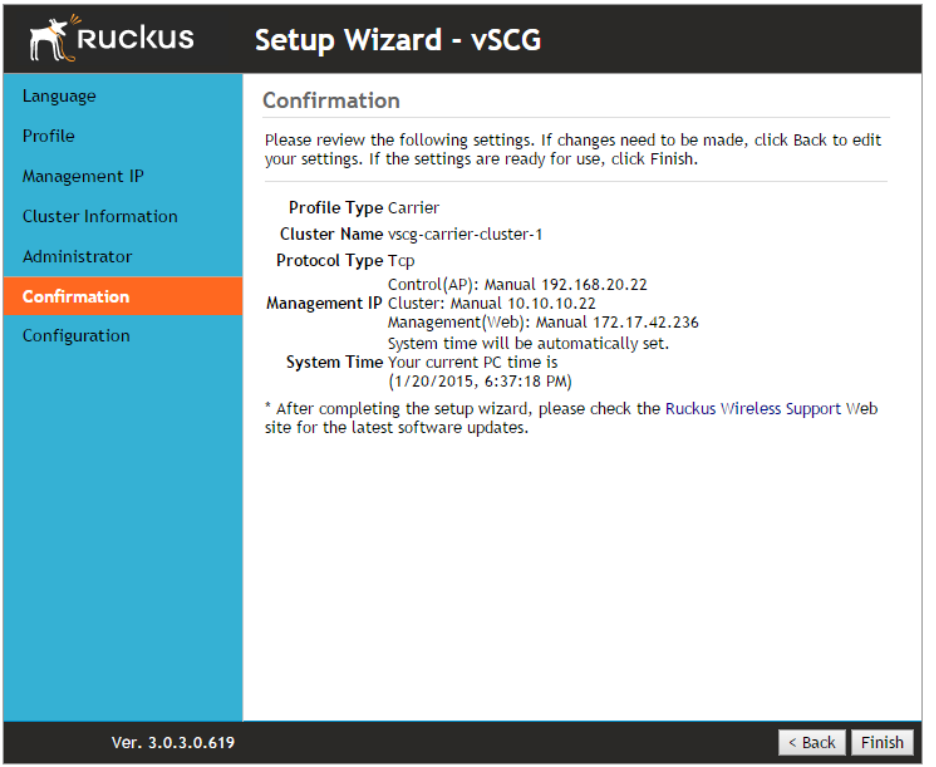
Figure 37. Set the web interface and CLI passwords



Step 6: Verify the Settings

Verify that all the settings displayed on the *Confirmation* page are correct. If they are all correct, click **Finish** to apply the settings and activate the vSCG on the network.

Figure 38. The Confirmation page

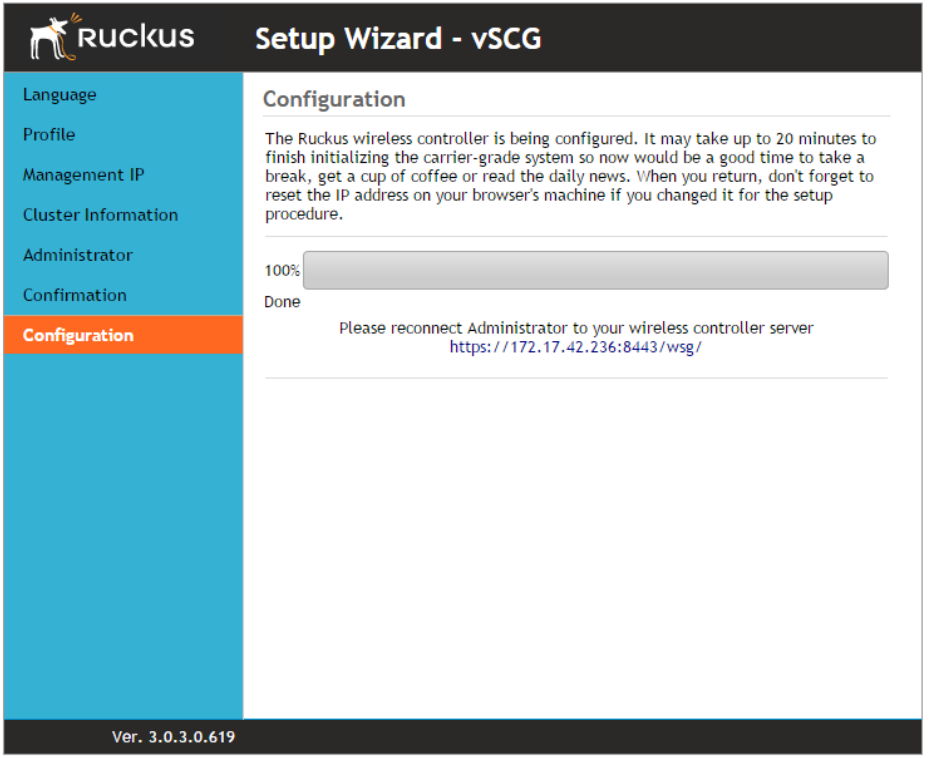


NOTE: If you find an incorrect setting, click the **Back** button until you reach the related page, and then edit the settings. When you finish editing the settings, click the **Next** button until you reach the *Confirmation* page again.

A progress bar appears and displays the progress of applying the settings, starting the vSCG services, and activating the vSCG on the network.

When the process is complete, the progress bar shows the message `100% Done`. The page also shows the IP address through which you can access the vSCG web interface to manage the appliance.

Figure 39. Setup is complete when the progress bar shows “100% Done”



Congratulations! You have completed the vSCG Setup Wizard. You are now ready to log on to the vSCG web interface. Go to `https://{management-IP-adddress}:8443`, and then log on with the user name and password that you assigned to the vSCG web interface.

Logging On to the Web Interface

You can access the vSCG web interface from any computer that is on the same subnet as the management (web) interface.

Follow these steps to log on to the vSCG web interface.

1 On a computer that is on the same subnet as the Management (Web) interface, start a web browser.

2 In the address bar, enter the IP address that you assigned to the Management (Web) interface and append a colon and `8443` (vSCG management port number) at the end of the address.

For example, if the IP address that you assigned to the Management (Web) interface is `10.10.101.1`, then you should enter:

https://10.10.101.1:8443

The vSCG web interface logon page appears.

Figure 40. vSCG web interface logon page

3 Log on to the vSCG web interface using the following logon details:

- User Name: **`admin`**
- Password: **`{the password that you set when you ran the vSCG Setup Wizard}`**

4 Click **Log On**.

The web interface refreshes, and then displays the vSCG dashboard page, which indicates that you have logged on successfully.

You are now ready to configure the vSCG.

Configuring the vSCG Carrier for the First Time

4

NOTE: This chapter describes the initial configuration tasks that Ruckus Wireless recommends you perform for the *vSCG Carrier*. The initial configuration of the *vSCG Enterprise* is more straightforward and, therefore, is not described here. For information on configuring the vSCG Enterprise, refer to the *vSCG Enterprise Administrator Guide*.

In this chapter:

- Creating an AP Zone
- Configuring AAA Servers and Hotspot Settings
- Creating a Registration Rule
- Defining the WLAN Settings of an AP Zone
- Configuring DHCP Option 43
- Verifying That Wireless Clients Can Associate with a Managed AP
- What to Do Next

Creating an AP Zone

The first step in configuring the vSCG is to create an AP zone. An AP zone functions as a way of grouping APs and applying a particular set of settings (including WLANs and their settings) to these groups of APs. Each AP zone can include up to six WLAN services.

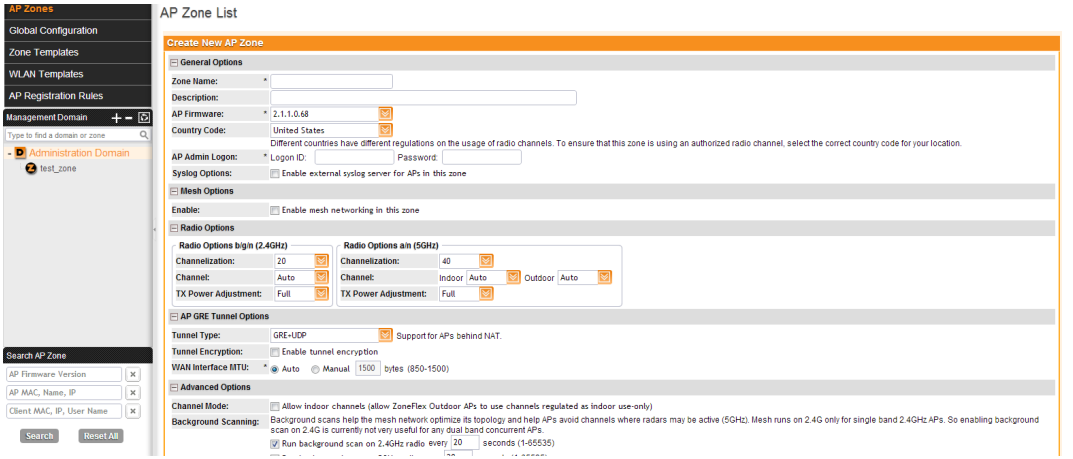
A zone called `Staging Zone` exists by default. Any AP that registers with the vSCG that is not assigned a specific zone is automatically assigned to the `Staging Zone`.

Follow these steps to create a new AP zone.

1 Click **Configuration** > **AP Zones**.

2 Click **Create New**.

Figure 41. Creating a new AP zone



3 Configure the options listed in Table 7.

Table 7. Configuration options in the Create New Zone form

Option	Description
General Options	
Zone Name	Type a name that you want to assign to this new zone.
Description	Type a description for this new zone.
AP Firmware	Displays the latest AP firmware available on the vSCG. If you want this zone to use a different firmware, click **Change**, and then select a firmware from the list.

Table 7. Configuration options in the Create New Zone form (Continued)

Option	Description
Country Code	Different countries and regions maintain different rules that govern which channels can be used for wireless communications. Set the country code to the proper regulatory region ensures that your vSCG network does not violate local and national regulatory restrictions.
AP Admin Logon	Specify the user name and password that administrators can use to log on directly to the managed access point's native web interface. The following boxes are provided: • *Logon ID*: Type the admin user name. • *Password*: Type the admin password.
Syslog Options	If you have a syslog server on the network and you want the vSCG to send syslog data to it, select the **Enable external syslog server for APs in this zone** check box. The following boxes are provided: • *IP Address:* Type the IP address of the syslog server. • *Port*: Type the port number that has been opened on the server for syslog data. The default port number is 514.
Mesh Options	
Enable	Select the **Enable mesh networking in this zone** check box if you want managed devices that belong to this zone to be able to form a mesh network automatically.
Radio Options	
Radio Options b/g/n (2.4GHz)	Configure the following 2.4GHz radio options: • *Channelization*: Select either 20MHz or 40MHz channel width. • *Channel*: Select Auto or manually assign a channel for the 2.4GHz radio. • *TX Power Adjustment*: Manually set the transmit power on all 2.4GHz radios (default is Full).

Table 7. Configuration options in the Create New Zone form (Continued)

Option	Description
Radio Options a/n (5GHz)	Configure the following 5GHZ radio options: • *Channelization*: Select either 20MHz or 40MHz channel width. • *Channel (Indoor and Outdoor)*: Select Auto or manually assign channels to the indoor and outdoor 5GHz radios. • *TX Power Adjustment*: Manually set the transmit power on all 5GHz radios (default is **Full**).
AP GRE Tunnel Options	
Tunnel Type	Select a protocol to use for tunneling WLAN traffic back to the vSCG. Options include **Ruckus GRE** and **SoftGRE**.
Tunnel Profile	Select the tunnel profile that you want to use. If you want to use Ruckus GRE tunneling for this AP zone, you can use the default tunnel profile or you can select a profile that you created. If you want to use Soft GRE tunneling, you must first create a Soft GRE tunnel profile. NOTE: Instructions for creating Ruckus GRE and Soft GRE tunnel profiles are provided in the *vSCG 2.5 Administrator Guide*.
Advanced Options	
Channel Mode	If you want to allow outdoor APs that belong to this zone to use wireless channels that are regulated as indoor use only, select the **Allow indoor channels** check box.
Background Scanning	If you want APs to automatically evaluate radio channel usage, enable and configure the background scanning settings on both the 2.4GHz and 5GHz radios. By default, background scanning is enabled on both radios and set to run every 20 seconds.

Table 7. Configuration options in the Create New Zone form (Continued)

Option	Description
Client Load Balancing	Improve WLAN performance by enabling load balancing. Load balancing spreads the wireless client load between nearby access points, so that one AP does not get overloaded while another sites idle. Load balancing must be enabled on a per-radio basis. To enable load balancing, select the **Enable load balancing on [2.4GHz or 5GHz]** check box, and then set or accept the default *Adjacent Radio Threshold* (50dB for the 2.4GHz radio and 43dB for the 5GHz radio).
Smart Monitor	To disable the WLANs of an AP (that belongs to this zone) whenever the AP uplink or Internet connection becomes unavailable, select the **Enable** check box. And then, configure the following options: • *Health Check Interval*: Set the interval (between 5 and 60 seconds) at which the vSCG will check the AP's uplink connection. The default value is 10 seconds. • *Health Check Retry Threshold*: Set the number of times (between 1 and 10 times) that the vSCG will check the AP's uplink connection. If the vSCG is unable to detect the uplink after the configured number of retries, the vSCG will disable the AP's WLANs. The default value is 3 retries. NOTE: When the vSCG disables the AP's WLANs, the AP creates a log for the event. When the AP's uplink is restored, the AP sends the event log (which contains the timestamp when the WLANs were disabled, and then enabled) to the vSCG.

4 Click **Create New** to finish creating your first AP Zone. When the vSCG completes creating the AP zone, the following confirmation message appears:

```
AP zone created successfully. Do you want to view the zone
information?
```

5 Click **Yes** to view the zone details, or click **No** to close the confirmation message and return to the zone list.

You have completed creating your first AP zone. You can create additional AP zones, if needed.

Configuring AAA Servers and Hotspot Settings

NOTE: If you do not have an AAA server on the network, skip this step.

If you have an existing RADIUS (AAA) server on the network, you can set up hotspot services across the network using the Ruckus Wireless access points that the vSCG is managing. To provide hotspot services, you need to add at least one AAA server to the vSCG and create a hotspot service.

AAA servers and hotspot settings must be configured on a per-AP zone basis.

Adding an AAA Server

Follow these steps to add an AAA server to an AP zone.

1 Go to **Configuration** > **AP Zones**.

2 Click the AP zone for which you want to add an AAA server. Alternatively, click the AP zone from the *Management Domains* tree.

3 Under the *AP Zones* menu on the sidebar, click **AAA**.

4 Click **Create New**. The *Create New RADIUS Server* form appears.

5 In the *General Options* section, configure the following settings:

- *Name*: Type a name for the AAA server that you are adding.
- *Description*: Type a description for the AAA server that you are adding.
- *Type*: Click either **RADIUS** or **RADIUS Accounting**, depending on the type of RADIUS server that you are using.
- *Backup RADIUS*: If a backup RADIUS server exists on the network, you may enable RADIUS backup support by selecting the **Enable backup RADIUS support** check box.

6 Configure the options in the Health Check Policy section. These options define the health monitoring settings of the primary RADIUS server by the secondary RADIUS server. The secondary RADIUS is responsible for monitoring the health of the primary RADIUS and for periodically synchronizing its settings to match those of the primary RADIUS.

- *Response Window*: Set the time (in seconds) during which the secondary RADIUS must wait for a response from the primary RADIUS. If the secondary RADIUS does not receive a response during the defined Response Window, the Zombie Period (see below) is started for the primary RADIUS. The default Response Window is 20 seconds.
- *Zombie Period*: Set the time (in seconds) during which the secondary RADIUS must wait for a response from the primary RADIUS before marking it as "down". If the secondary RADIUS does not receive a response during the defined Zombie Period, the Revive Interval (see below) is started for the primary server. The default Zombie Period is 40 seconds. If the primary RADIUS still does not respond when the Zombie Period expires, it will be marked as down and the secondary RADIUS will start receiving new requests from the Network Access Server (NAS).
- *Revive Interval*: Set the time (in seconds) during which the secondary RADIUS must wait for the primary RADIUS to start responding to requests again. If the primary RADIUS starts responding before the Revive Interval expires, new requests will be forwarded to the primary RADIUS again. The default Revive Interval is 120 seconds.
- *No Response Fail*: Click Yes to respond with a reject message to the NAS if no response is received from the RADIUS server. Click No to skip sending a response.

7 In the *Primary Server* section, configure the following settings:
- *IP Address*: Type the IP address of the AAA server.
- *Port*: Type the AAA port number. The default AAA port number is 1812.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the AAA shared secret that you typed above.

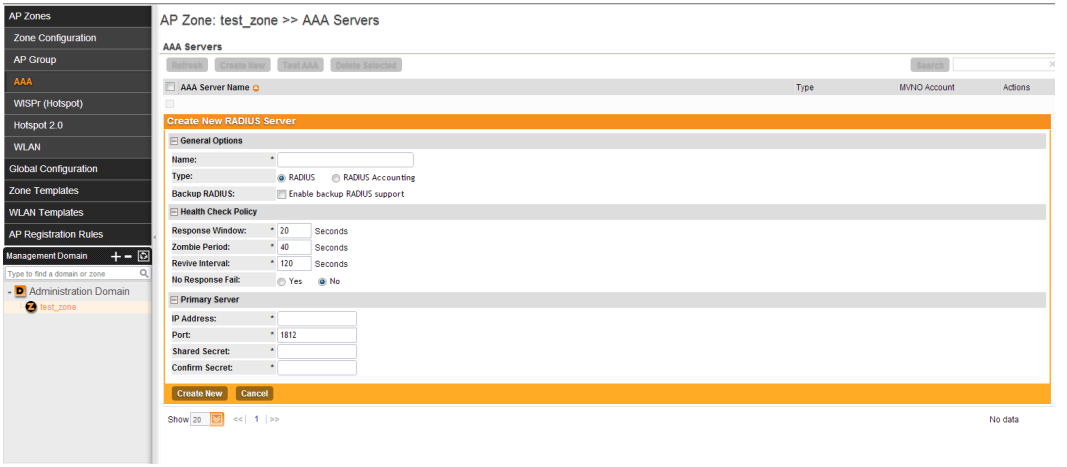
8 If you selected the **Enable backup RADIUS support** check box, the *Secondary Server* section is visible. Configure the following *Secondary Server* settings:
- *IP Address*: Type the IP address of the secondary AAA server.
- *Port*: Type the AAA port number. The default AAA port number is 1812.
- *Shared Secret*: Type the AAA shared secret.
- *Confirm Secret*: Retype the AAA shared secret that you typed above.

9 Click **Create New**. The following message appears to confirm that you have successfully added the AAA server to the vSCG:

```
Authentication server created successfully.
```

The page refreshes, and then the AAA server that you created appears under the *AAA Servers Configuration* section.

Figure 42. The Create New RADIUS Server form



Creating a Hotspot Service

NOTE: If you do not want to provide a hotspot service to users, skip this step.

NOTE: Before creating a hotspot, you need to create a user defined interface. For information on how to create a user defined interface, see the *Administrator Guide* for release 2.5.

A hotspot service requires an AAA server. Before creating a hotspot service, make sure you have already added an AAA server to the vSCG. For more information, refer to Adding an AAA Server.

Follow these steps to create a hotspot service for an AP zone.

1. Go to **Configuration** > **AP Zones**.
2. Click the AP zone for which you want to create a hotspot service. Alternatively, click the AP zone from the *Management Domains* tree.
3. Under the *AP Zones* menu on the sidebar, click **WISPr (Hotspot)**.
4. Click **Create New**. The *Create New Hotspot Service* form appears.

5 Configure the hotspot service settings listed in Table 8.

Table 8. Hotspot service settings

Setting	Description
General Options	
Name	Type a name for this new hotspot service that you are creating.
Description	Type a description for this new hotspot service (for example, `Main Office Lobby`).
Type	Click **Registered Users** if you want only users with existing profiles on the vSCG to be able to connect to this hotspot. Click **Guest-Access** if you want guest users to be able to connect to this hotspot.
Redirection	
Smart Client Support	• **None**: Click to disable Smart Client support. • **Enable**: Click to enable Smart Client support. • **Only Smart Client allowed**: Click to allow only Smart Clients to access this hotspot service.
Logon URL	Type the URL of the subscriber portal (the page where hotspot users can log in to access the service). For more information, see the section "Configuring the Logon URL" in the *Administrator Guide* for release 2.5.
Start Page	Set where users will be redirected after logging in successfully. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected (for example, your company website).
User Session	
Session Timeout	Set a time limit after which users will be disconnected from the hotspot service and required to log on again. Allowed session timeout range is between 2 and 14400 minutes. The default value is 1440 minutes.
Grace Period	Allow disconnected users a grace period after disconnection, during which clients will not need to re-authenticate. Allowed grace period range is between 1 and 14399 minutes. The default value is 60 minutes.

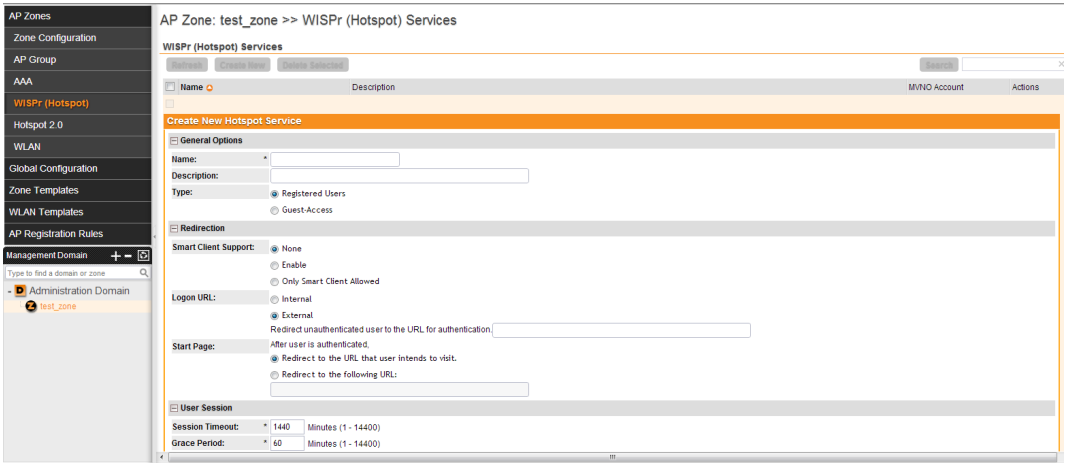
Table 8. Hotspot service settings (Continued)

Setting	Description
Location Information	
Location ID	Type a location ID for the hotspot, for example: `isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport`
Location Name	Type a location name for the hotspot, for example: `ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport`
Walled Garden	Click **Create New** to add a walled garden, which is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. In the box provided, type a URL or IP address to which you want to grant unauthenticated users access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following: • IP address (for example, `10.11.12.13`) • Exact website address (for example, `www.ruckuswireless.com`) • Website address with regular expression (for example, `*.ruckuswireless.com`, `*.com`, `*`) After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as `www.yahoo.com`), as users may be redirected to re-authenticate when they navigate through the page.

6 Click **Create New**.

The page refreshes, and then the hotspot that you created appears under the *WISPr (Hotspot) Configuration* section.

Figure 43. The Create New Hotspot Service form



Creating a Registration Rule

Registration rules enable the vSCG to assign an AP to an AP zone automatically based on the rule that the AP matches.

Follow these steps to create a registration rule.

1 Go to **Configuration** > **AP Zones**.

2 On the sidebar on the left, click **AP Registration Rules**. The *AP Registration Rules* page appears.

3 Click **Create New**. A form appears.

4 In *Rule Description*, type a name that you want to assign to this rule.

5 In *Rule Type*, click the basis upon which you want to create the rule. Options include:

- *IP Address*: If you select this option, type the *From* (starting) and *To* (ending) IP address that you want to use.
- *Subnet Mask*: If you select this option, type the IP address and subnet mask pair to use for matching.
- *GPS Coordinates*: If you select this option, type the GPS coordinates to use for matching. Access points that have been assigned the same GPS coordinates will be automatically assigned to the AP zone that you will choose in the next step.

- *Provision Tag*: If the access points that are joining the vSCG have been configured with provision tags, click the **Provision Tag** option, and then type a tag name in the *Provision Tag* box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

NOTE: Provision tags can be configured on a per-AP basis from the access point's command line interface.

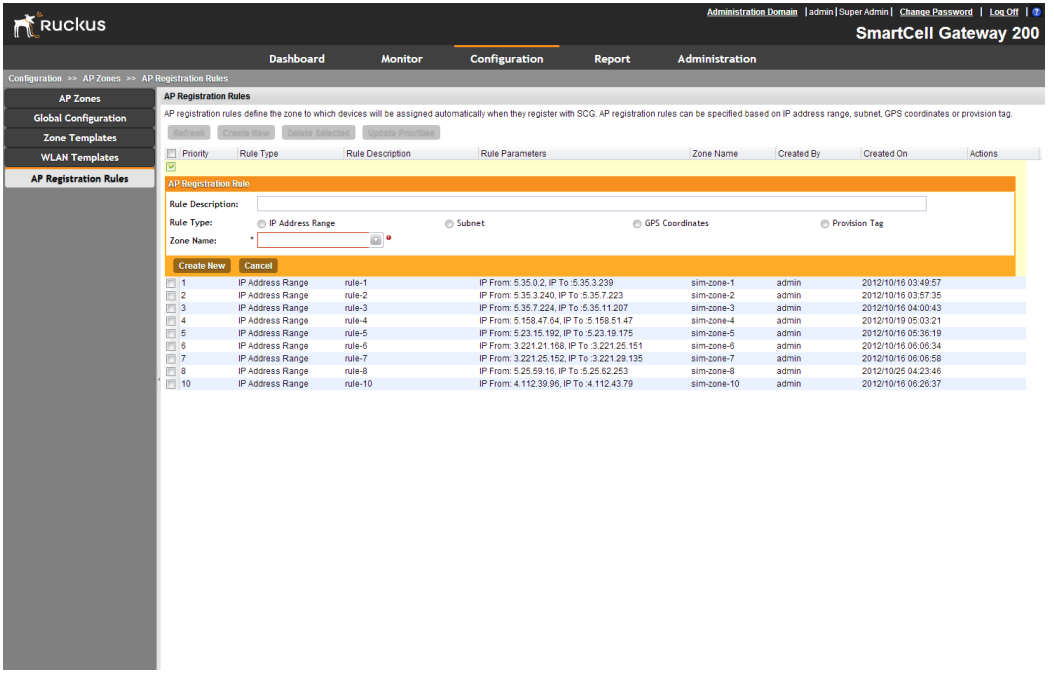
---

6 In *Zone Name*, click the drop-down list to display available AP zones, and then click an AP zone to which APs that match this rule will be assigned.

7 Click **OK.**

You have completed creating an AP registration rule.

Figure 44. Creating an AP registration rule



To create another registration rule, repeat the preceding steps. You can create as many registration rules as you need to manage access points on the network.

Configuring the Rule Priority

The vSCG applies registration rules in the same order as they appear in the AP Registration Rules table (highest to lowest priority). If you want a particular registration rule to have higher priority, you must move it up the table. Once an AP matches a registration rule, the vSCG assigns the AP to the zone specified in the rule and stops processing the remaining rules.

Follow these steps to configure the rule priority.

1 Go to **Configuration** > **AP Zones**.

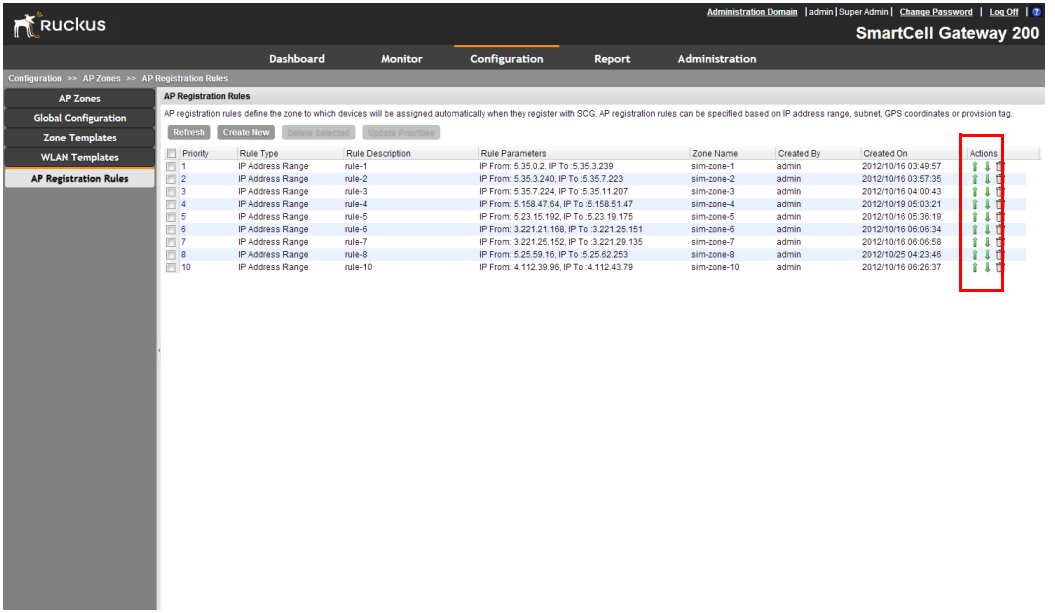
2 On the sidebar on the left, click **AP Registration Rules**. The AP Registration Rules page appears and displays the rules that you have created.

3 Change the priority of each registration rule as required.

- To give a rule higher priority, move it up the table by clicking the (up-arrow) icon that is in the same row as the rule name.
- To give a rule lower priority, move it down the table by clicking the (down-arrow) icon that is in the same row as the rule name.

4 When you finish configuring the rule priority, click **Update Priorities** to save your changes.

Figure 45. Change the rule priority by clicking the up-arrow or down-arrow



Defining the WLAN Settings of an AP Zone

Follow these steps to configure the WLAN settings of an AP zone.

1. Go to **Configuration** > **AP Zones**.
2. Click the AP zone for which you want to add the WLAN settings. Alternatively, click the AP zone from the *Management Domains* tree.
3. Under the *AP Zones* menu on the sidebar, click **WLAN**.
4. Click **Create New**. The *Create New WLAN Configuration* form appears.
5. Configure the WLAN settings listed in Table 9. You can find a detailed description of each setting in the succeeding sections.

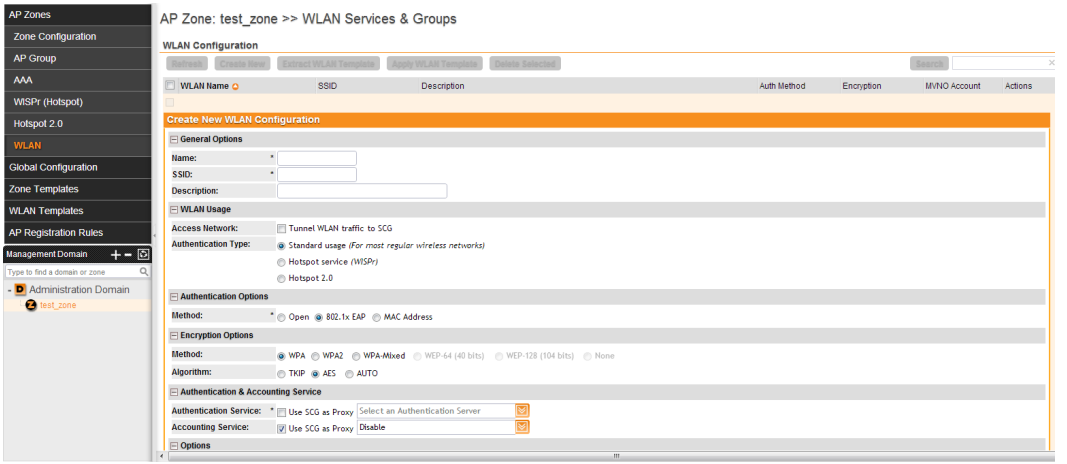
Table 9. Overview of WLAN settings

WLAN Setting	Description
General Options	Enter the WLAN name and description. See General Options.
WLAN Usage	Select the usage type (standard WLAN or hotspot). See WLAN Usage.
Authentication Options	Select an authentication method for this WLAN (open or 802.1X EAP). See Authentication Options.
Encryption Options	Select an encryption method (WPA, WPA2, WPA Mixed, WEP), encryption algorithm (AES or TKIP) and enter a WPA passphrase/WEP key. See Encryption Options.
Authentication & Accounting Service	This section only appears when certain authentication options are selected. See Authentication & Accounting Service.
Options	Select whether web-based authentication (captive portal) will be used, and which type of authentication server will be used to host credentials (local database, Active Directory, RADIUS, LDAP). Also, enable or disable Wireless Client Isolation, Zero-IT Activation, Dynamic PSK and Priority for this WLAN. See Options.
Advanced Options	Select an accounting server and configure ACLs, rate limiting, VLAN/dynamic VLAN settings, tunneling, background scanning, maximum client threshold, and service schedule. See Advanced Options.

6 Click **OK** to finish creating the WLAN service.

You have completed creating your first WLAN. To create another WLAN, repeat Step 4 to Step 6. You can create up to six WLANs per AP zone.

Figure 46. Configuring the WLAN settings of an AP zone



General Options

- *Name/ESSID*: Type a short name (2-31 characters) for this WLAN. In general, the WLAN name is the same as the advertised SSID (the name of the wireless network as displayed in the client's wireless configuration program). However, you can also separate the ESSID from the WLAN name by entering a name for the WLAN in the first field, and a broadcast SSID in the second field. In this way, you can advertise the same SSID in multiple locations (controlled by the same vSCG) while still being able to manage the different WLANs independently. Each WLAN "name" must be unique within the vSCG, while the broadcast SSID can be the same for multiple WLANs.
- *Description*: Enter a brief description of the qualifications or purpose of this WLAN (for example, `Engineering` or `Voice`).

WLAN Usage

- In *Access Network*, select the Tunnel WLAN traffic to vSCG check box if you want to tunnel the traffic from this WLAN back to the vSCG. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP

devices), Ruckus Wireless recommends enabling tunnel mode. When you enable this option, you need to select core network for tunneling WLAN traffic back to the vSCG.

- In *Authentication Type*, click one of the following options:
  - **Standard usage (For most regular wireless networks)**: This is a regular WLAN suitable for most wireless networks.
  - **Hotspot service (WISPr)**: Click this option if want to use a hotspot (WISPr) service that you previously created.
  - **Hotspot 2.0**: Click this option if you want to use a Hotspot 2.0 profile that you previously created.
  - **Guest Access**: Click this option if you want to use this WLAN for guest access.

Authentication Options

Authentication defines the method by which users are authenticated prior to gaining access to the WLAN. The level of security should be determined by the purpose of the WLAN you are creating.

- *Open [Default]*: No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.
- *802.1X/EAP*: Uses 802.1X authentication against a user database.
- *MAC Address*: Uses the MAC address of a client for authentication. MAC address authentication requires a RADIUS server and uses the MAC address as the user logon name and password. You have two options for the MAC address format to use for authenticating clients:
  - Use user defined text as authentication password (default is device MAC address)
  - Set device MAC address in 802.1x format 00-10-A4-23-19-C0. The default is 0010a42319c0.

Encryption Options

Encryption choices include WPA, WPA2, WPA-Mixed, WEP and none. WPA and WPA2 are both encryption methods certified by the Wi-Fi Alliance and are the recommended encryption methods. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and Ruckus Wireless recommends against using WEP if possible.

Method

- *WPA*: Standard Wi-Fi Protected Access with either TKIP or AES encryption.
- *WPA2*: Enhanced WPA encryption using the stronger AES encryption algorithm.
- *WPA-Mixed*: Allows mixed networks of WPA and WPA2 compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- *WEP-64*: Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption.
- *WEP-128*: Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.
- *None*: No encryption; communications are sent in clear text.

CAUTION! If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit) and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

Algorithm (For WPA or WPA2 Encryption Only)

- *TKIP*: This algorithm provides greater compatibility with older client devices, but retains many of the security weaknesses of WEP. Therefore, if you select TKIP encryption, 11n devices will be limited to 11g transfer rates. Furthermore, the Wi-Fi Alliance will be mandating the removal of TKIP, so it should not be used.
- *AES*: This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard. Choose AES encryption if you are confident that all of your clients will be using 802.11i-compliant NICs.
- *Auto*: Automatically selects TKIP or AES encryption based on the client's capabilities. Note that since it is possible to have clients using both TKIP and AES on the same WLAN, only unicast traffic is affected (broadcast traffic must fall back to TKIP; therefore, transmit rates of broadcast packets from 11n APs will be at lower 11g rates).

CAUTION! If you set the encryption algorithm to TKIP and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

CAUTION! If you set the encryption algorithm to TKIP, the AP will only be able to support up to 26 clients. When this limit is reached, additional clients will be unable to associate with the AP. On the other hand, if you select AES or none, the AP will be able to support up to 256 clients (less if wireless mesh is also enabled on the same radio).

WEP Key/Passphrase

- *WEP Key*: WEP methods only. Click the *Hex* field, and then type the required key text. If the key is for WEP 64 encryption, enter ten hexadecimal characters (any combination of 0-9, A-F). If it is for WEP 128 encryption, enter 26 hexadecimal characters (any combination of 0-9, A-F).
- *Passphrase*: WPA-PSK methods only. Click in this field and type the text of the passphrase used for authentication. The passphrase must contain between eight and 63 characters (or 64 hexadecimal characters).

Authentication & Accounting Service

- *Authentication Service*: This option appears only when 802.1x EAP is selected as the authentication method. Select the authentication server that you want to use for this WLAN. Only AAA servers that you previously added appear here.
- *Accounting Service*: This option appears only when 802.1x EAP is selected in Authentication method. Additionally, you must have added a RADIUS Accounting server previously. Select the RADIUS Accounting server from the drop-down list, as a proxy for vSCG.

Options

- *Wireless Client Isolation*: This option appears only when Standard Usage is selected as the WLAN usage type. Wireless client isolation enables subnet restrictions for connected clients. Click Enable if you want to prevent wireless clients associated with the same AP from communicating with each other locally. The default value is Disable.
- *Priority*: Set the priority of this WLAN to Low if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to “Low.” By default, all WLANs are set to high priority.

RADIUS Options

NOTE: The *RADIUS Options* section only appears when *Authentication Type* (under *WLAN Usage*) is set to **Standard usage (For most regular wireless networks)**.

- *RADIUS NAS ID*: Select how the RADIUS server will identify the AP:
  - WLAN BSSID
  - AP MAC
  - User-defined
- *RADIUS NAS Request Timeout*: Type the timeout period (in seconds) after, which an expected RADIUS response message is considered to have failed.
- *RADIUS NAS Max Number of Retries:* Type the number of failed connection attempts after which the vSCG will fail over to the backup RADIUS server.
- *RADIUS NAS Reconnect Primary*: If the vSCG fails over to the backup RADIUS server, this is the interval (in minutes) at which the vSCG will recheck the primary RADIUS server if it is available. The default interval is 5 minutes.
- *Call STA ID*: Use either WLAN BSSID or AP MAC as the station calling ID. Select one.

Advanced Options

- *Rate Limiting*: Rate limiting controls fair access to the network. When enabled, the network traffic throughput of each network device (client) is limited to the rate specified in the traffic policy, and that policy can be applied on either the uplink or downlink.

  Toggle the Uplink and/or Downlink drop-down lists to limit the rate at which WLAN clients upload/download data. The “Disabled” state means rate limiting is disabled; thus, traffic flows without prescribed limits.
- *Access VLAN*: By default, all wireless clients associated with APs that the vSCG is managing are segmented into a single VLAN (with VLAN ID 1). If you want to tag this WLAN traffic with a different VLAN ID, enter a valid VLAN ID (2-4094) in the box. Select the **Enable Dynamic VLAN** check box to allow the vSCG to assign VLAN IDs on a per-user basis. Before enabling dynamic VLAN, you need to define on the RADIUS server the VLAN IDs that you want to assign to users.
- *Hide SSID*: Click this option if you do not want the ID of this WLAN advertised at any time. This will not affect performance or force the WLAN user to perform any unnecessary tasks.

- *Proxy ARP*: When enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (for example, ARP requests and ICMPv6 Neighbor Solicit messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request at the rate limit specified
- *Max Clients*: Limit the number of clients that can associate with this WLAN per AP (default is 100). You can also limit the total number of clients that a specific AP (or radio, on dual radio APs) will manage.
- *802.11d*: The 802.11d standard provides specifications for compliance with additional regulatory domains (countries or regions) that were not defined in the original 802.11 standard. Enable this option if you are operating in one of these additional regulatory domains.
- *DHCP Option 82*: When this option is enabled and an AP receives a DHCP request from a wireless client, the AP will encapsulate additional information (such as VLAN ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.
- *Client TX/RX Statistics*: Select the **Ignore statistics from unauthorized clients** check box if you do not want the vSCG to monitor traffic statistics for unauthorized clients.
- *Inactivity Timeout*: Select the check box and enter a value in minutes (6 to 600 minutes) after which idle clients will be disconnected.
- *Client Fingerprinting*: If you select this check box, the vSCG will attempt to identify client devices by their operating system, device type, and host name, if available. This makes identifying client devices easier on the Dashboard, Monitor and Client Details pages.
- *Disable WLAN*: Select this option to disable this WLAN service.

Configuring DHCP Option 43

To enable the vSCG to manage an AP, the AP must be able to locate the vSCG on the network successfully and register with it. The easiest way to ensure that APs can successfully locate the vSCG on the network is by configuring DHCP Option 43 on your DHCP server.

DHCP Option 43 enables the DHCP server on your network to provide the vSCG server address – either IP address or FQDN– (specifically, the IP address assigned to the vSCG's control plane or cluster plane interface) to DHCP clients, including APs that are connected to the network.

The procedure for configuring DHCP option 43 varies, depending on the DHCP server that you are using. Refer to the documentation provided with your DHCP server software for information on how to configure DHCP option 43.

NOTE: The following procedure describes how to configure DHCP option 43 on a Linux server (Fedora). If your DHCP server is running on a different platform, refer to the DHCP server documentation for the relevant instructions.

Follow these steps to configure DHCP option 43 on a Linux server.

1 Log on to your DHCP server via a console terminal (for example, PuTTY).

2 Go to `/etc` directory.

3 Run `vi dhcpd.conf`. This command opens the DHCP configuration file for editing.

4 At the beginning of the DHCP configuration file, insert the following lines:

```
option space VendorInfo;
option VendorInfo.WSG code 6 = text;
```

OR

```
option space VendorInfo;
option VendorInfo.SCG code 6 = text;
```

CAUTION! Make sure that space characters exist in "6 = text". Omitting these space characters could result in AP connectivity issues.

---

5 Under the subnet section, insert the following lines:

```
Vendor-option-space VendorInfo;
option VendorInfo.WSG "{control-ip-address-or-fqdn}"
```

OR

```
Vendor-option-space VendorInfo;
option VendorInfo.SCG "{control-ip-address-or-fqdn}"
```

NOTE: `{control-ip-address-or-fqdn}` must be the IP address or FQDN of the control plane (br0).

Remember to remove the curly brackets ({ }) that enclose the IP addresses or FQDNs. If the control plane IP addresses are mapped to proper names on the DNS server, you could also use FQDN host names instead of IP addresses.

The vSCG supports two formats for vendor information:

- Plain IP address or FQDN (for example, `10.2.0.87` or `server.company.com`)
- URL-based IP address or FQDN (for example, `https://10.2.0.87/wsg/ap` or `https://server.company.com/wsg/ap`) where `10.2.0.87` or `server.company.com` is the IP address or FQDN of the control plane interface, respectively.

Inserting Multiple IP Addresses or URLs

If you want to insert multiple IP addresses or URLs, use any of the following formats:

- URL format
  - `option VendorInfo.WSG "https://10.2.0.87/wsg/ap,https://10.2.0.88/wsg/ap"`, or
  - `option VendorInfo.SCG "https://10.2.0.87/wsg/ap,https://10.2.0.88/wsg/ap"`
- IP address format
  - `option VendorInfo.WSG "10.2.0.87,10.2.0.88"`, or
  - `option VendorInfo.SCG "10.2.0.87,10.2.0.88"`

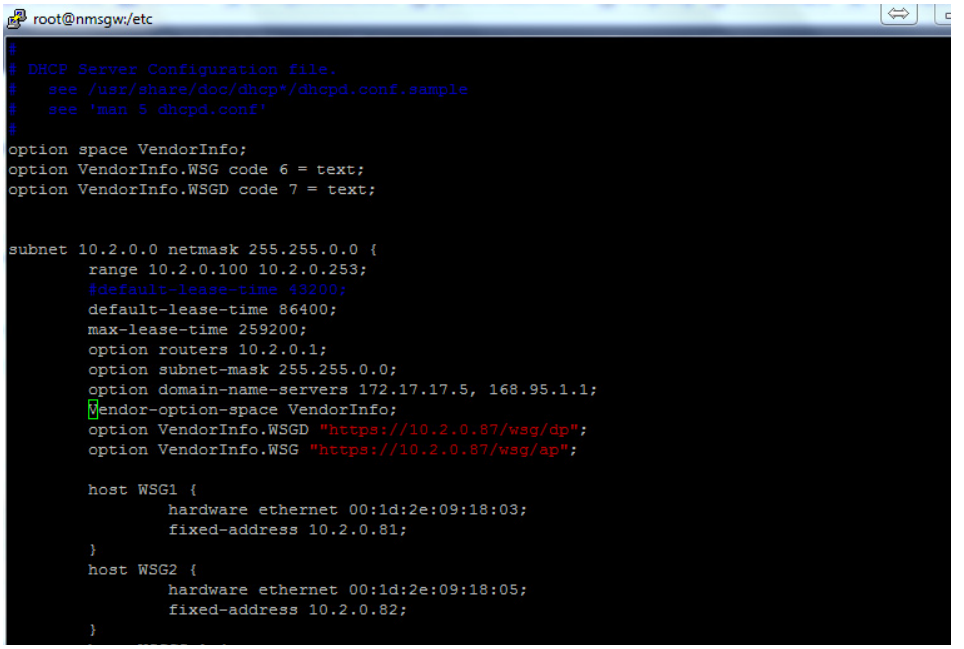
CAUTION! Take care not to insert any space characters before or after the comma (,) character that separates the multiple IP addresses or URLs.

6 Save the changes.

7 Restart the DHCP server to apply the new settings.

You have completed configuring DHCP option 43 on a Linux server.

Figure 47. Editing dhcpd.conf



Verifying That Wireless Clients Can Associate with a Managed AP

The last step in the vSCG setup process is to verify that APs can register with the vSCG and that wireless clients can associate with the APs successfully.

Follow these steps to verify that wireless clients can connect to the network.

1. Verify that the vSCG is connected to the backbone network.
2. Physically connect an AP to the same network as the vSCG. If DHCP option 43 was configured correctly, this AP should be able to locate the vSCG on the network and to register with it successfully.
3. Check the vSCG Dashboard. The AP zone that you created earlier should have at least one member AP (the AP that you connected to the network in Step 2). The AP count appears green, which indicates that it is online.
4. Associate a wireless client with the AP. The following describes the procedure if you are using a Windows-based wireless client.
   a. In the system tray, right-click the (Wireless Network Connection) icon, and then click **View Available Wireless Networks**.
   b. In the list of available wireless network, click the wireless network name (SSID) that you configured on the AP.
   c. Click **Connect**.

   Your wireless client connects to the wireless network. After the wireless client connects to the wireless network successfully, the wireless client icon in the system tray changes to .
5. Start your web browser, and then enter `www.ruckuswireless.com` in the address bar.

If you are able to connect to the Ruckus Wireless website, you have completed setting up the vSCG on the network. Congratulations!

What to Do Next

For more information on configuring and managing the vSCG, refer to the *Virtualized SmartCell Gateway Administrator Guide,* which is available for download on the Ruckus Wireless Support website at
`https://support.ruckuswireless.com/documents`

NOTE: For a complete list of documentation that is available for your vSCG profile configuration, refer to the *Release Notes*.

Ensuring That APs Can Discover the Controller on the Network

5

Before the controller can start managing an AP, the AP must first be able to discover the controller on the network when it boots up. his chapter describes procedures that you can perform to ensure that APs can discover and register with the controller on the network.

In this chapter:

- Is LWAPP2SCG Enabled on the Controller?
- Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server
- Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet
- Method 3: Register the Controller with the DNS Server
- Method 4: Configure DHCP Option 43 on the DHCP Server
- Method 5: Manually Configure the Controller Address on the AP's Web Interface

Is LWAPP2SCG Enabled on the Controller?

All of the controller discovery methods described in this chapter require LWAPP2SCG (the application that enables APs to discover and be managed by a controller) to be installed and enabled on the controller. See Table 10 to check if your controller release includes the LWAPP2SCG application and whether it is enabled or disabled by default.

Table 10. LWAPP2SCG availability on each controller release

Controller Release	LWAPP Discovery	Default Setting	AP Compatibility
SCG 1.1.2, 2.1.2	Application installed by administrator. See Obtaining the LWAPP2SCG Application.	Disabled	• ZF-AP Release 9.6.x – 9.8.x • AP Release 100.0.x and later
SCG 2.5.x	Enabled by administrator. See Enabling LWAPP2SCG.	Disabled	
SCG 2.6.x	Enabled by administrator. See Enabling LWAPP2SCG.	Disabled	• ZF-AP Release 9.7.x – 9.8.x • AP Release 100.0.x and greater
RuckOS 3.0.x	Enabled by default	Enabled	

Obtaining the LWAPP2SCG Application

If your controller release does not have the LWAPP2SCG application pre-installed, contact Ruckus Wireless Support to obtain a copy of the LWAPP2SCG application files and installation instructions.

Enabling LWAPP2SCG

If the LWAPP2SCG application is pre-installed but disabled in your controller release, do the following to enable it:

1 Log on to the controller's console.

2 Enter **`en`** to enable privileged mode.

3 Enter **`config`**.

4 Enter **`lwapp2scg`**.

5 Enter **`policy accept-all`**.

You have completed enabling the LWAPP2SCG application on the controller.

Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server

NOTE: This guide assumes that you have already activated the controller's licenses on the SmartLicense server. If you have not activated the controller's licenses, see the *Virtualized SmartCell Gateway Quick Setup Guide for RuckOS 3.0* for more information.

The Ruckus Wireless SmartLicense registration server is a cloud-based, HTTPS-enabled web server that allows an access point to query information about its parent controller by sending its serial number and base MAC address.

NOTE: If you do not want to (or cannot) use the cloud-based SmartLicense registration server, you can install a local version of the registration server (called the Local License Server). For more information, see the *Local License Server User Guide*.

After you ensure that the controller's licenses have been activated on the SmartLicense server, you only need to connect the AP to the network, ensure that it has Internet connectivity, and then reboot the AP. Upon reboot, the AP will automatically attempt to discover its parent controller by sending the following HTTPS query to ap-registrar.ruckuswireless.com (the SmartLicense server URL):

```
https://ap-registrar.ruckuswireless.com/
controller?ap_mac=APMAC&ap_serial=APSERIAL
```

where APMAC is the AP's MAC address (for example, APMAC: 74:91:1A:20:59:90) and APSERIAL (for example, APSERIAL: 311003001685) is the AP's serial number, both of which are printed on the AP's product label.

If the AP is unable to discover its parent controller after the first attempt, it will continue to do so:

- Once every 5 minutes for up to 60 minutes (12 queries)
- Once every hour for the remaining day (23 queries)
- Once every 24-hour for the remaining two weeks (12 queries)

If the AP is still unable to discover its parent controller after two weeks of uptime, this cloud-based controller discovery method will be disabled permanently. You will need to reset the AP to factory default settings to re-enable this controller discovery method.

Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet

If you are deploying the AP and the controller on different subnets, let the AP perform auto discovery on the same subnet as the controller before moving the AP to another subnet. To do this, connect the AP to the same network as the controller. When the AP starts up, it will discover and attempt to register with the controller. Approve the registration request if auto approval is disabled. After the AP registers with the controller successfully, transfer it to its intended subnet. It will be able to find and communicate with the controller once you reconnect it to the other subnet.

NOTE: If you use this method, make sure that you do not change the IP address of the controller after the AP discovers and registers with it. If you change the controller's IP address, the AP will no longer be able to communicate with it and will be unable to rediscover it.

Method 3: Register the Controller with the DNS Server

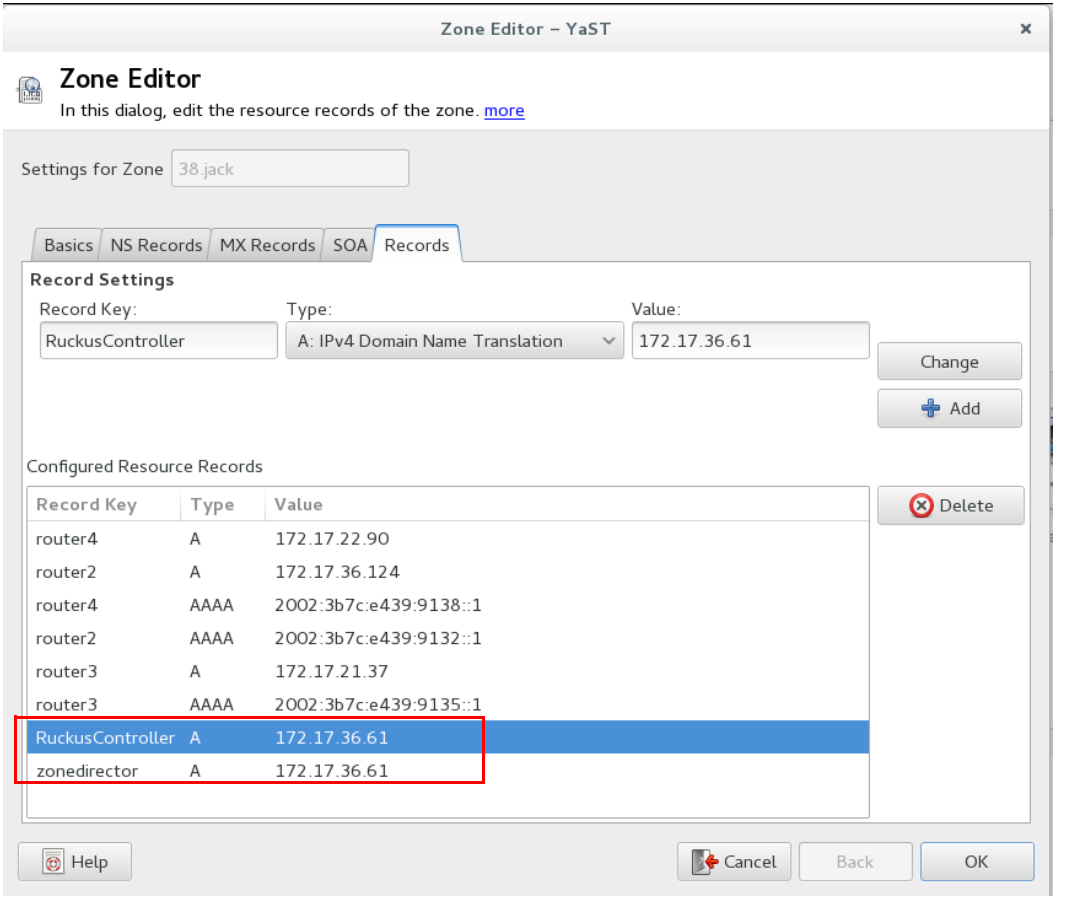
If you register the controller with your DNS server, supported APs that request IP addresses from your DHCP server will also obtain DNS related information that will enable them to discover controllers on the network. Using the DNS information they obtained during the DHCP request, APs will attempt to resolve the controller IP address using RuckusController.{DNS domain name} and zonedirector.{DNS domain name}.

To register the controller with the DNS server, do the following.

1 Open the DNS zone file, and then add two records with the following information:

- Record Key#1: RuckusController
  Type: A (IPv4 Domain Name Translation)
  Value: (IP address of the controller)
- Record Key#2: zonedirector
  Type: A (IPv4 Domain Name Translation)
  Value: (IP address of the controller)

Figure 48. Add records for “RuckusController” and “zonedirector” to the DNS zone file

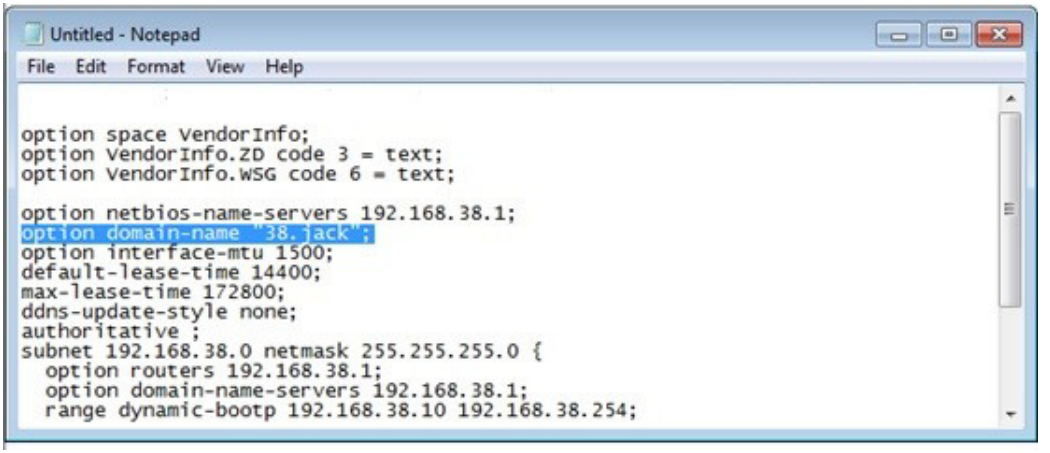


2 Save the zone file.

3 Open the DHCP configuration file, and then insert the DNS domain name in the DHCP configuration file. For example, if the DNS domain name is “38.jack”, insert the following line into the DHCP configuration file:

```
option domain-name “38.jack”
```

Figure 49. Insert option domain-name “38.jack”



4 Save the DHCP configuration file.

When the AP obtains the DNS domain name from the DHCP server (using “Domain Name option 15” in the DHCP-offer packet), it will resolve “RuckusController.{domain-name}” and “zonedirector.{domain-name}” through the DNS server, and then it will obtain the controller’s IP address from the DNS server’s response.

NOTE: If the AP uses a static IP address or it cannot obtain the DNS domain name from the DHCP server, the AP will attempt to resolve “RuckusController” and “zonedirector” without a domain name from the DNS server as the FQDN of controller's control interface.

You have completed registering the controller with the DNS server.

Method 4: Configure DHCP Option 43 on the DHCP Server

Another method for the AP to discover the controller on the network automatically is to configure the DHCP server on the network. To do this, you will need to configure DHCP Option 43 (043 Vendor Specific Info) with the IP address of the controller on the network. When an AP requests an IP address from the DHCP server, the DHCP server will send a list of controller IP addresses to the AP. If there are multiple controller devices on the network, the AP will automatically select a controller to register with from this list of IP addresses.

DHCP Option 43 enables the DHCP server on your network to provide the controller's server address – either IP address or FQDN– (specifically, the IP address assigned to the controller's control plane or cluster plane interface) to DHCP clients, including APs that are connected to the network.

The procedure for configuring DHCP option 43 varies, depending on the DHCP server that you are using. Refer to the documentation provided with your DHCP server software for information on how to configure DHCP option 43.

NOTE: The following procedure describes how to configure DHCP option 43 on a Linux server (Fedora). If your DHCP server is running on a different platform, refer to the DHCP server documentation for the relevant instructions.

CAUTION! If you have a ZoneDirector controller on the network and you do not want APs to be managed by this ZoneDirector controller, you must disable auto approval on the ZoneDirector web interface. Log on to the ZoneDirector web interface, and then go to *Configure* > *Access Points* > *Access Points Policies* page, and then clear the **Approval** check box.

Follow these steps to configure DHCP option 43 on a Linux server.

1. Log on to your DHCP server via a console terminal (for example, PuTTY).
2. Go to **`/etc`** directory.
3. Run **`vi dhcpd.conf`**. This command opens the DHCP configuration file for editing.

4 At the beginning of the DHCP configuration file, insert the following lines:

```
option VendorInfo.WSG_sub6 code 6=text;
option VendorInfo.WSG_sub3 code 3=text;

option VendorInfo.WSG_sub6 "<Controller IP>";
option VendorInfo.WSG_sub3 "<Controller IP>";
```

For example, if you only have one controller on the network and its IP address is 120.0.0.3, then these lines in the DHCP configuration file should look like in Figure 50Sample DHCP Option 43 configuration.

Figure 50. Sample DHCP Option 43 configuration

```
option space VendorInfo;
option VendorInfo.WSG code 6 = text;
option VendorInfo.ZD code 3 = text;
option VendorInfo.WSGD code 7 = text;

Vendor-option-space VendorInfo;
option VendorInfo.WSG "120.0.0.3";
```

If you have a two-node controller cluster on the network, use a comma to separate the control interface IP addresses in option VendorInfo.WSG, for example:

```
option VendorInfo.WSG "120.0.0.3,120.0.0.4"
```

where 120.0.0.3 is the control interface IP address of the first controller and 120.0.0.4 is the control interface IP address of the second controller.

5 Save the DHCP configuration file.

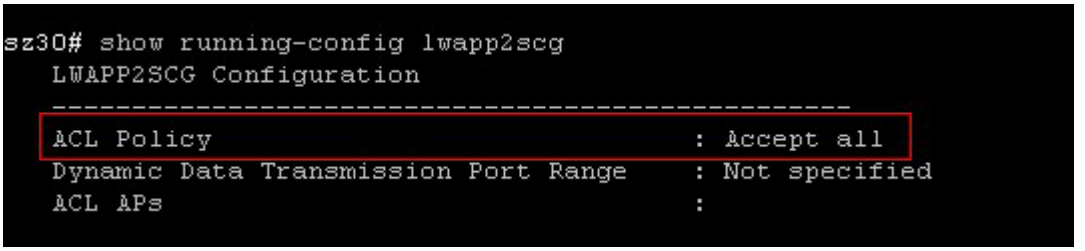
6 Restart the DHCP server to apply the new settings.

7 Verify that the LWAPP2SCG application is enabled on the controller. To verify, log on to the controller's CLI, and then enter the following command:

`show running-config lwapp2scg`

If LWAPP2SCG is enabled, the value for `ACL Policy` should show as `Accept all`.

Figure 51. “Accept all” indicates that LWAPP2SCG is enabled



If LWAPP2SCG is disabled, do the following to enable it:

a Enter **`config`**.

b Enter **`lwapp2scg`**.

c Enter **`policy`**.

d Enter one of the following commands:

- **`accept {MAC`**
- **`address}`**: Enter this command if you only want specific APs to be managed by the controller. See Figure 53.
- **`accept-all`**: Enter this command if you want all APs that discover the controller to be managed by it.

Figure 52. Options that appear after you enter the “policy” command

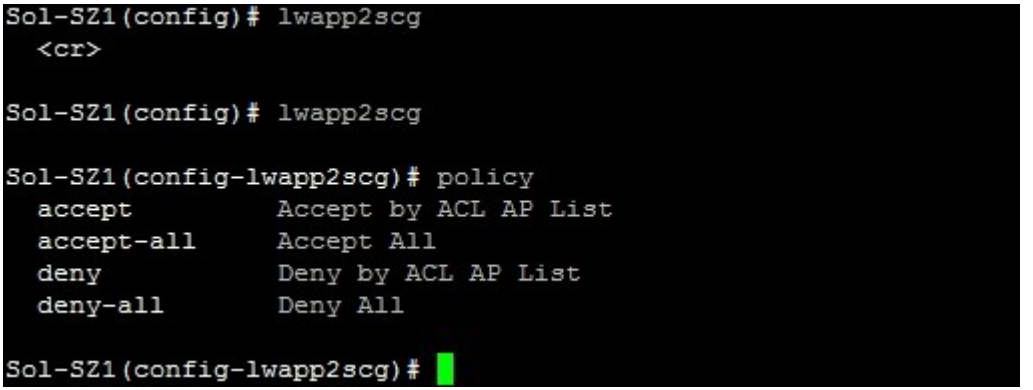
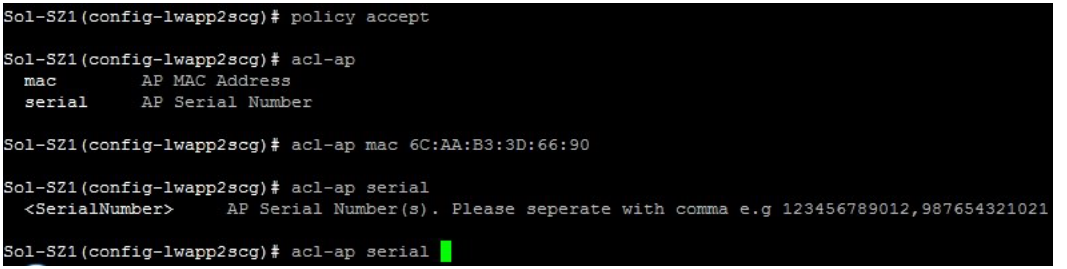


Figure 53. Enter accept {MAC address} if you only want specific APs to be managed by the controller



8 Reset the AP to factory default settings, and then connect it to a network subnet where it can communicate with the controller.

9 Reboot the AP.

After the AP reboots, it will obtain an IP address and the IP address of its parent controller from the DHCP server. Once the AP registers with the controller, it will download and install the latest SCG-AP firmware.

You have completed

Method 5: Manually Configure the Controller Address on the AP's Web Interface

1 Log on to the AP's web interface.

2 Go to the Administration > Management page.

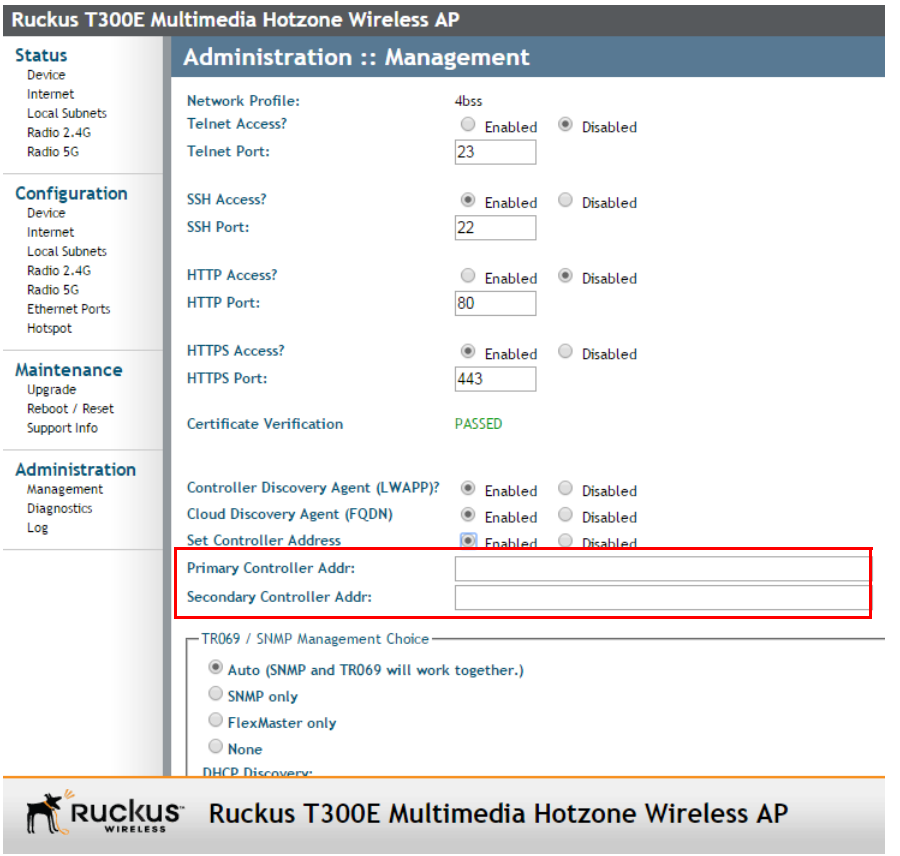
3 In *Primary Controller Address*, type the IP address of the controller that you want to manage the AP.

4 In Secondary Controller Address, type the IP address of a backup controller that you want to manage the AP if the primary controller is unavailable.

5 Click **Apply**.

You have completed manually configuring the controller's IP address on the AP's web interface.

Figure 54. Set the IP addresses of the primary and secondary controllers that you want to manage the AP



What to Do Next

For more information on configuring and managing the controller, refer to the *Virtualized SmartCell Gateway Administrator Guide for RuckOS 3.0*, which is available for download on the Ruckus Wireless Support website at http://support.ruckuswireless.com.

NOTE: For a complete list of documentation that is available for this SZ release, refer to the *Release Notes*.

Index

Numerics

802.11d 79

A

AAA server 65
ACLs 73
Administrator Guide 84
AES 76
AP zone 61, 73
authentication options 75

B

background scanning 63
backup RADIUS 65

C

client fingerprinting 79
cluster name 51, 52
cluster setting 51
controller name 52
country code 62
creating a new cluster 51

D

description file 8
DHCP Option 43 79
DHCP Option 82 79
DHCP server 80
disable WLAN 79
Dynamic VLAN 78

E

encryption algorithm 76
encryption options 75
ESSID 74
ESXi 8

F

firmware version 53

G

gateway 9

H

hide SSID 78
hotspot 65
hotspot service 67
hypervisors 8

I

inactivity timeout 79
interface settings 9
IP address 9

J

joining a cluster 52

K

KVM 8

L

Linux 8
logging on 58

M

management interface 58
manifest file 8
max clients 79
mesh settings 62

N

netmask 9
NTP server 52

O

OVA 8

P

passphrase 77
primary DNS server 9
proxy ARP 79

R

RADIUS 65
RADIUS Accounting 65
rate limiting 78
recommended system resources 10
registration rule 70
  priority 72
rule priority 72

S

setup wizard 46
software version 53
SSID
  hiding 78
staging zone 61

T

TKIP 76

V

virtual machine
  recommended system resources 10
virtual machine state file 8
VLAN 78
VMWare 8
vSCG
  required disk space 11
vSphere client 11

W

Web interface 58
WEP key 77
WEP-128 76
WEP-64 76
WLAN
  disabling 79
WLAN name 74
WLAN settings 73
WLAN usage 74
WPA 76

WPA2 76
WPA-Mixed 76

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com