COMMSCOPE®
RUCKUS®

RUCKUS IoT Controller Software Installation Guide, 1.7-5.2.1-p2

Supporting IoT Controller Release 1.7-5.2.1-p2

Part Number: 800-72817-001 Rev B
Publication Date: February 2021

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **5**
- Document Conventions 5
  - Notes, Cautions, and Safety Warnings 5
- Command Syntax Conventions 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Contacting RUCKUS Customer Services and Support 7
  - What Support Do I Need? 7
  - Open a Case 7
  - Self-Service Resources 7

About This Guide **9**
- Introduction to RUCKUS IoT Controller 9
- What's New in This Document 9

Installing RUCKUS IoT Controller on Hypervisor **11**
- System Requirements for Installing RUCKUS IoT Controller on a Hypervisor 11
  - Hardware Recommendations for the IoT Server 11
- Installing RUCKUS IoT Controller on Oracle VM VirtualBox 12
- Installing RUCKUS IoT Controller on a VMware ESXi 21
- Installing RUCKUS IoT Controller Using VMware Player 33
- Installing a KVM Guest Using virsh Commands 45
- Installing a KVM Guest Using Virtual Machine Manager 45

Installing RUCKUS IoT Controller on AWS **59**
- Installing AWS CLI 59
- Getting Access Key ID and Secret Access Key for Amazon S3 Account 60
- Importing VRIOT Image 60
- Creating RUCKUS IoT Controller EC2 Instance 61

Upgrading the Software **63**
- Upgrading the AP Firmware Using SmartZone 100 or Virtual SmartZone Controller 63
- Upgrading the RUCKUS IoT Controller 67
- Upgrading the RUCKUS IoT Controller with N+1 Configuration 68

Hot Upgrade of IoT Gateway **71**

Deploying the APs **73**
- Connecting a Set of IoT APs Using Grouping Method 73

Managing a License **75**
- Activating a License 75

Preface

- Document Conventions 5
- Command Syntax Conventions 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Contacting RUCKUS Customer Services and Support 7

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.

Convention	Description
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

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

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

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

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://training.ruckuswireless.com.

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

About This Guide

- Introduction to RUCKUS IoT Controller..... 9
- What's New in This Document..... 9

Introduction to RUCKUS IoT Controller

The RUCKUS IoT Controller is a versatile, easy-to-deploy service and management component that allows for integration of Internet of Things (IoT) devices and IoT services for a wide range of use cases. It provides a robust, secure, scalable, interoperable, and well-managed general transport between IoT devices and cloud services.

The RUCKUS IoT Controller is an open-programmable framework that exposes northbound APIs and is thereby a highly flexible IoT transport for RUCKUS partners to integrate a wide range of IoT services and solutions for the enterprise and beyond.

This guide provides information about how to install the RUCKUS IoT Controller on a supported hypervisor. Topics include the list of supported hypervisors and RUCKUS IoT Controller installation instructions using the .OVA or .qcow2 file.

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.

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

What's New in This Document

TABLE 2 Summary of New Features in RUCKUS IoT Controller Release 1.7-5.2.1-p2

Feature	Description	Location
Initialization screen is replaced.	This screen has now an option for SmartThings Service.	All the topics that relate to Installing RUCKUS IoT Controller.

Installing RUCKUS IoT Controller on Hypervisor

- System Requirements for Installing RUCKUS IoT Controller on a Hypervisor....11
- Installing RUCKUS IoT Controller on Oracle VM VirtualBox....12
- Installing RUCKUS IoT Controller on a VMware ESXi....21
- Installing RUCKUS IoT Controller Using VMware Player....33
- Installing a KVM Guest Using virsh Commands....45
- Installing a KVM Guest Using Virtual Machine Manager....45

System Requirements for Installing RUCKUS IoT Controller on a Hypervisor

The RUCKUS IoT Controller supports a number of hypervisors and requires a virtual machine (VM).

The following table lists the hypervisors (and their release versions) on which you can install the controller.

TABLE 3 Supported Hypervisors

Hypervisor	Vendor	Version
ESXi	VMware	6.0 and later
VM VirtualBox	Oracle	5.1.20 and later
VM Player	VMware	12 or later
KVM	Linux	2.11.1 or later

NOTE
For the compatible hardware for the hypervisors listed above, refer to the respective vendors website.

The virtual machine (VM) on which the controller is installed must meet the following requirements:

- The VM for the Oracle VM VirtualBox hypervisor must have a minimum of 4 vCPUs, 4 GB RAM, and Fixed 20 GB HDD.
- The VM for the VMware ESXi hypervisor must have a minimum of 4 vCPUs, 4 GB RAM, and Fixed 20 GB HDD.
- The VM for the VM Player hypervisor must have a minimum of 4 vCPUs, 4 GB RAM, and Fixed 20 GB HDD.
- The VM for the KVM hypervisor must have a minimum of 4 vCPUs, 4 GB RAM, and Fixed 20 GB HDD.
- Ports 80, 123 or NTP, 443, 1883, and 8883 must be open.

NOTE
For a high-scale deployment, RUCKUS recommends a minimum of 8 vCPUs and 8 GB RAM for the RUCKUS IoT Controller.

Hardware Recommendations for the IoT Server

The RUCKUS IoT Controller recommends the following minimum hardware requirements for the IoT Server.

- **CPU**: 4 core i7 or equivalent
- **Memory**: 32 GB
- **Hard Disk**: 1 TB

Installing RUCKUS IoT Controller on Oracle VM VirtualBox

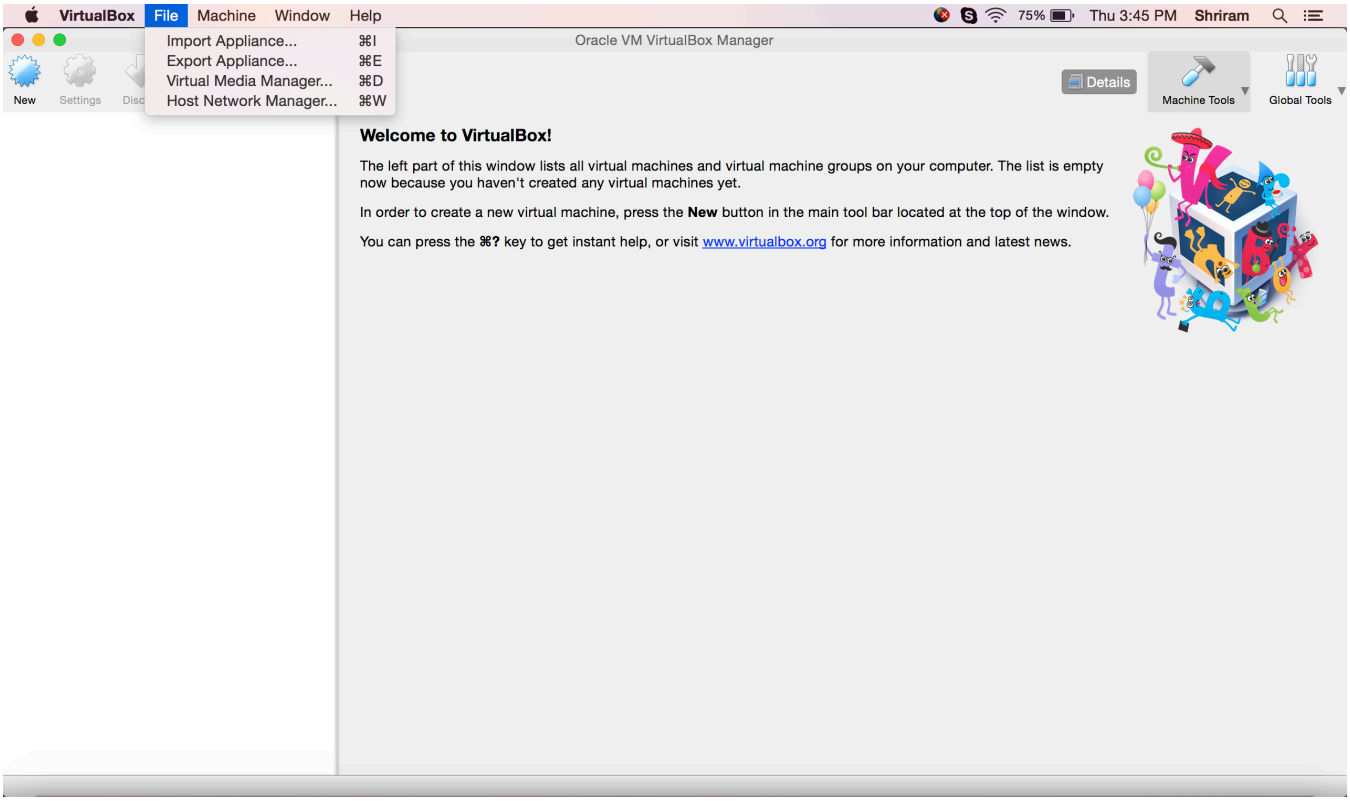
The RUCKUS IoT Controller can be installed on an Oracle VM VirtualBox using an .OVA file.

NOTE
RUCKUS IoT Controller can be installed on a Mac or a Windows 64-bit machine.

Complete the following steps to install RUCKUS IoT Controller on a Mac.

1. Download the RUCKUS IoT Controller distribution package in the .OVA file format from the RUCKUS Support website at https://support.ruckuswireless.com.
2. Open the Oracle VM VirtualBox Manager and select **File** > **Import Appliance**.

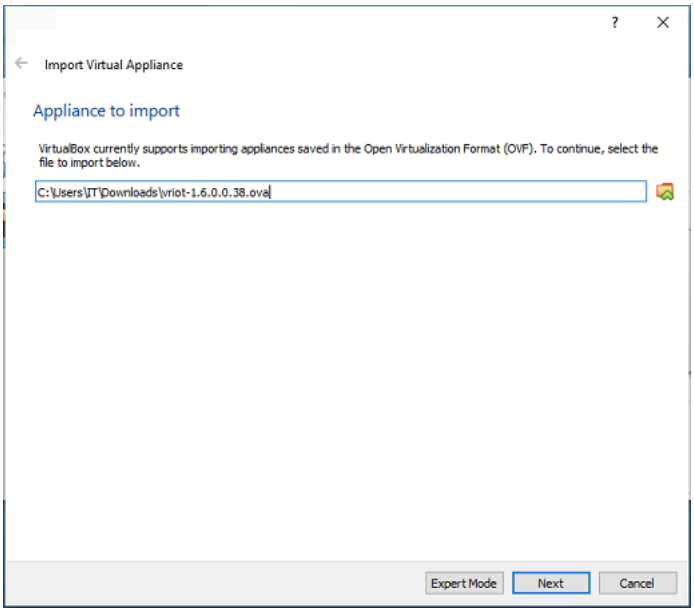
FIGURE 1 Oracle VM VirtualBox Manager



The installation begins.

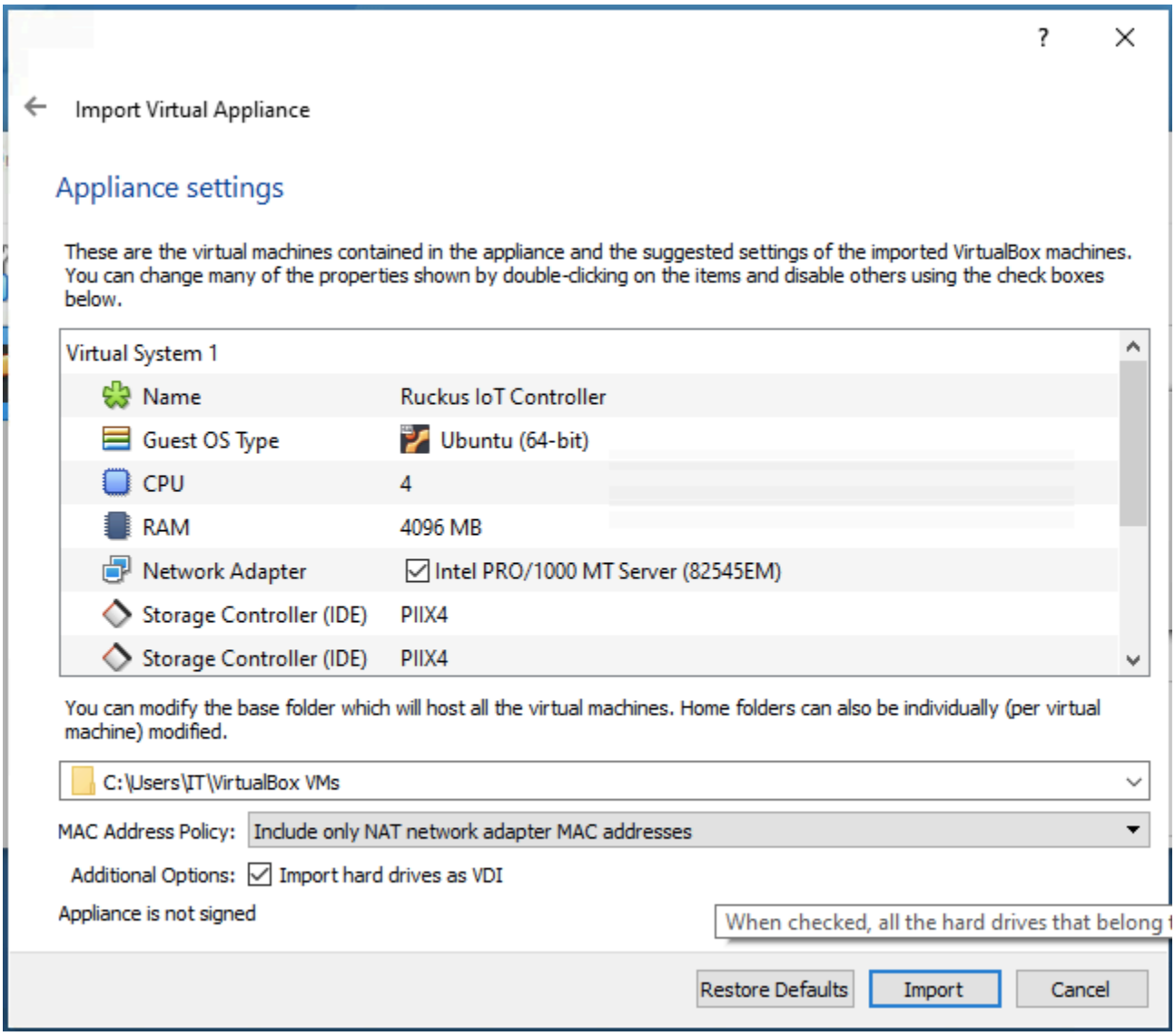
3. Import the .OVA file of the virtual appliance and click **Continue**.

FIGURE 2 Importing the Virtual Appliance



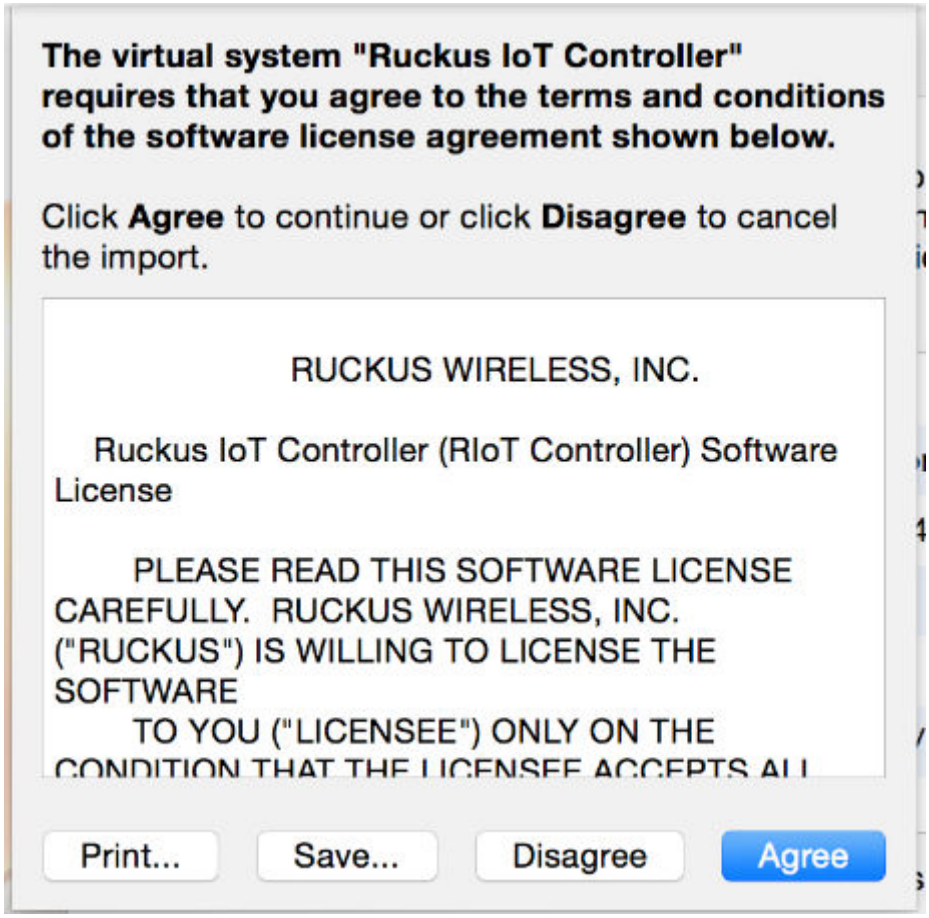
4. Confirm the appliance settings and click **Import**.

FIGURE 3 Importing the Appliance Settings



5. Accept the terms of the license agreement and click **Agree**.

FIGURE 4 License Agreement

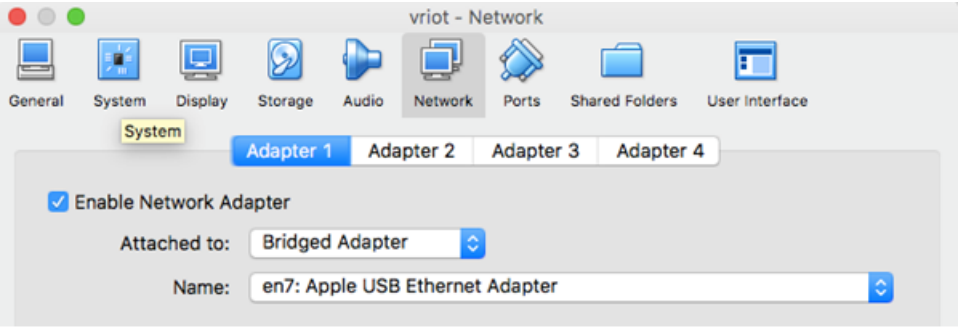


When the import has completed, the RUCKUS IoT Controller .OVA file runs in VirtualBox.

FIGURE 5 RUCKUS IoT Controller .OVA File Running in VirtualBox

6. Select **Bridged Adapter** to configure the VirtualBox interfaces.

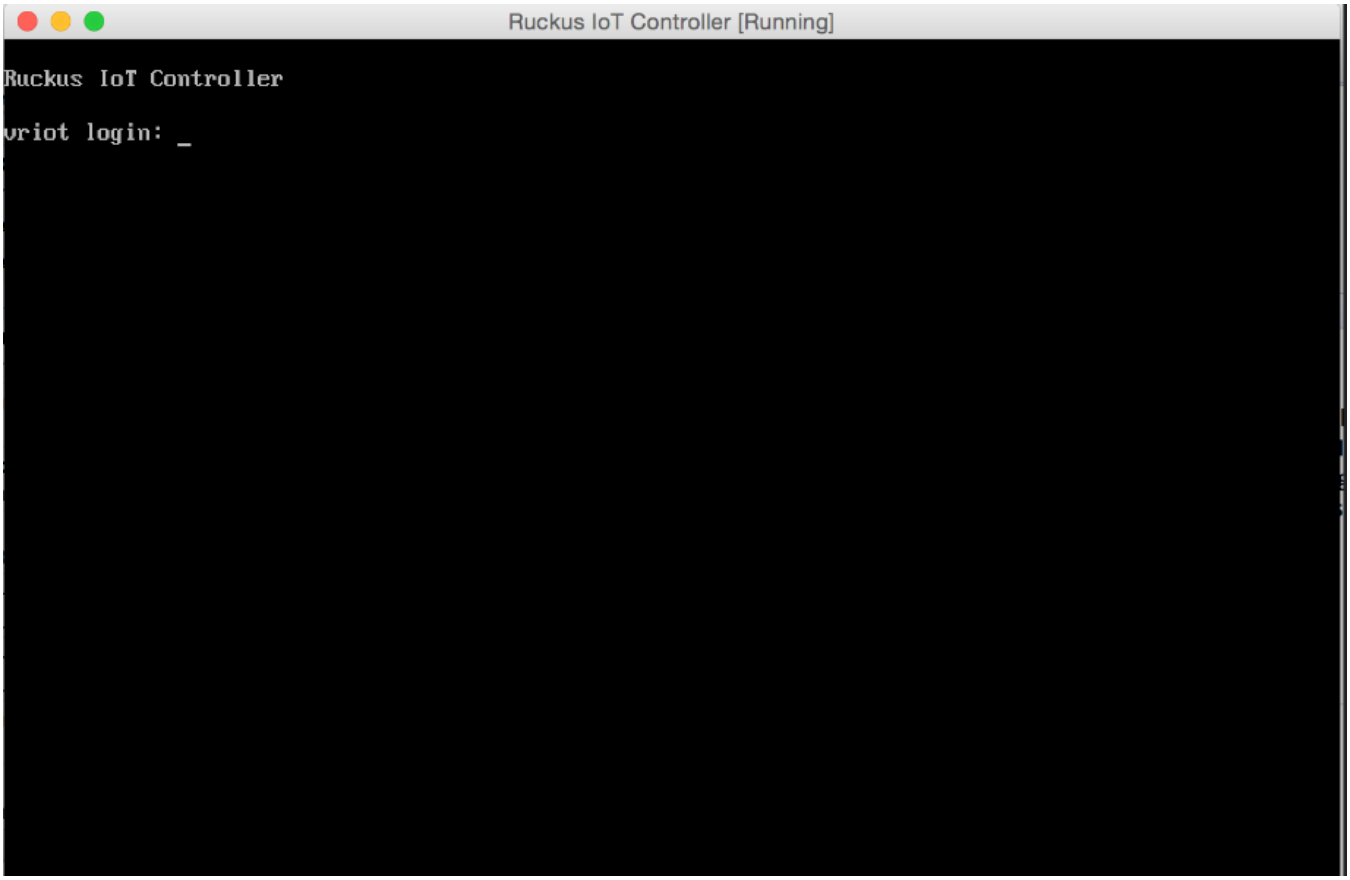
FIGURE 6 VM Interface Configuration



7. Power on the virtual machine and wait for the login prompt.

   The RUCKUS IoT Controller login prompt is displayed.

   FIGURE 7 RUCKUS IoT Controller Login Prompt

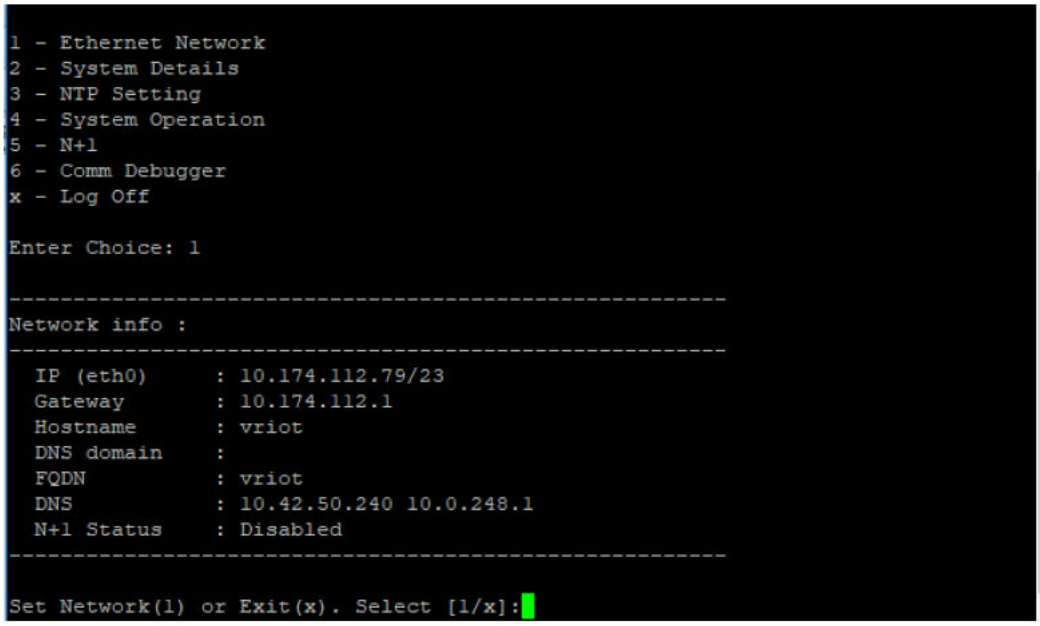


8. Enter the username and the password at the login prompt.

9. Enter **1** in the **Enter Choice** field to get the IP address of the virtual machine.

   This information is needed to access the RUCKUS IoT Controller **Initialization** page.

   FIGURE 8 Displaying the IP Address



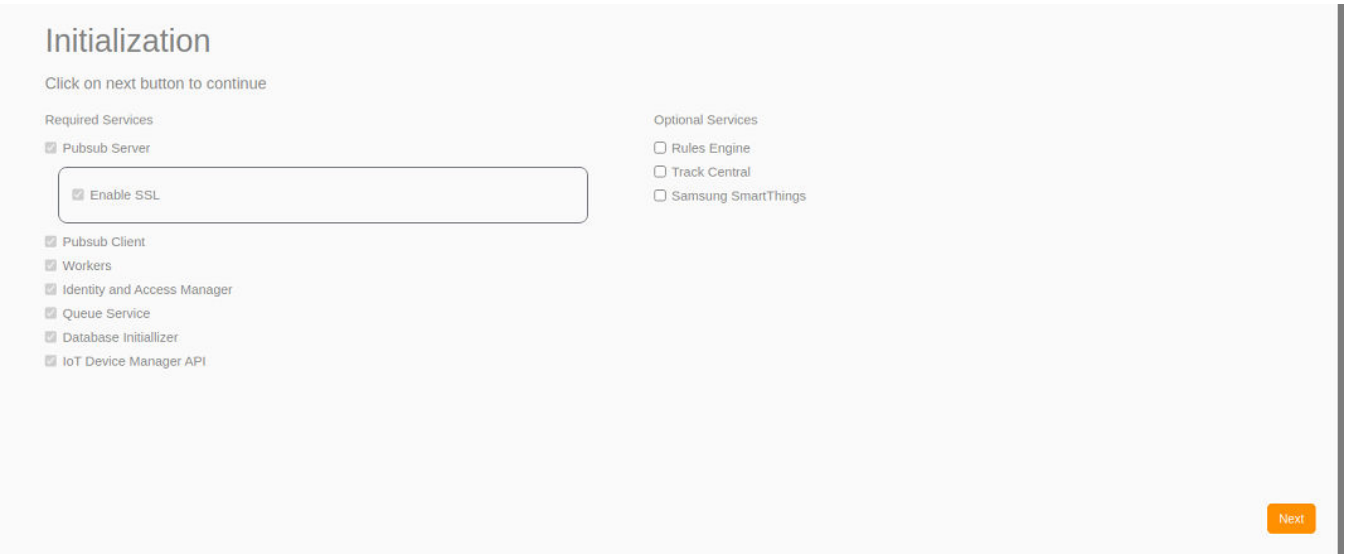
   To configure N+1 on the RUCKUS IoT Controller, enter **5** in the **Enter Choice** field. Refer to "Configuring N+1" in the *RUCKUS IoT Controller Configuration Guide* to complete this configuration.

10. Open a web browser on your host machine and enter the IP address of the VM in the address bar.

    HTTP and HTTPS on ports 80 and 443 are supported.

    The **Initialization** page is displayed.

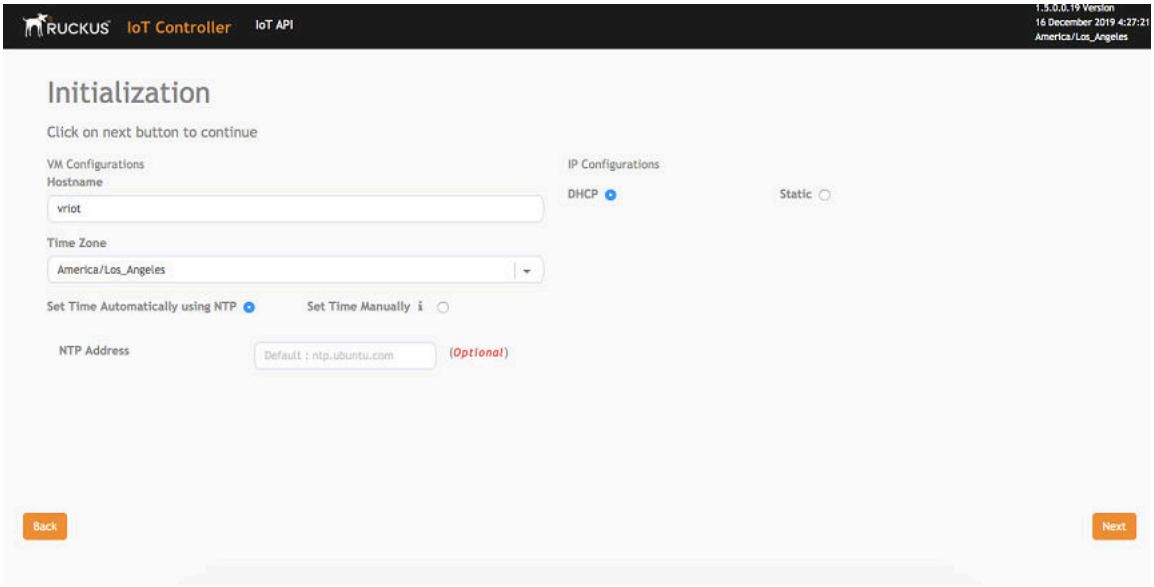
    FIGURE 9 Intialization Page



11. Select the required services and click **Next**.

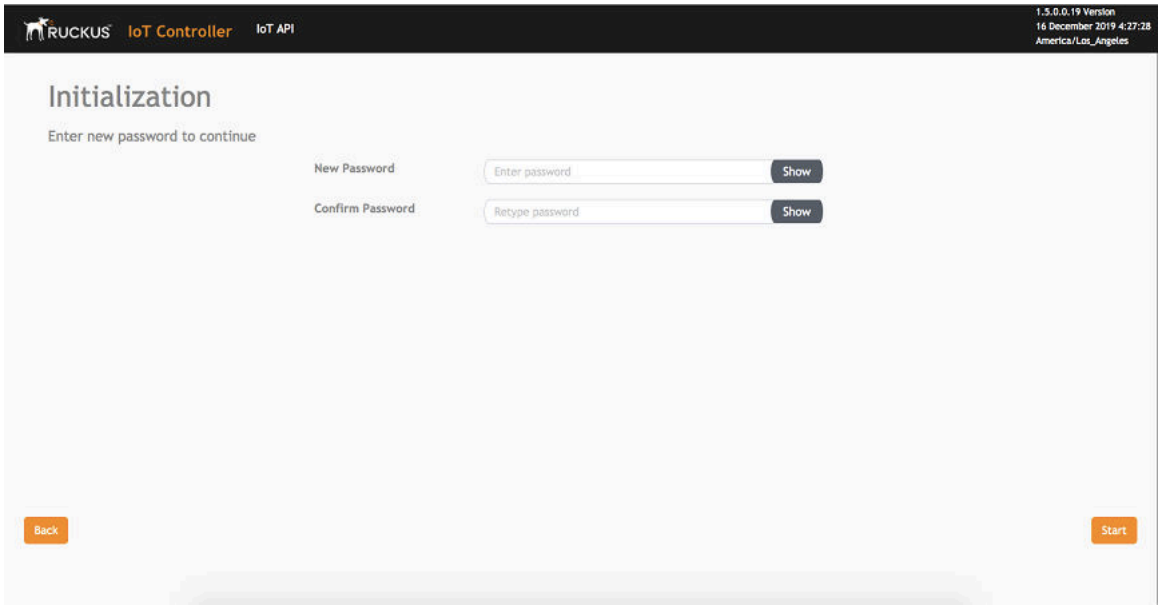
12. Confirm the configuration information and click **Next**.

FIGURE 10 Initial VM and IP Configurations



The **RUCKUS IoT Controller Initialization** page is displayed.

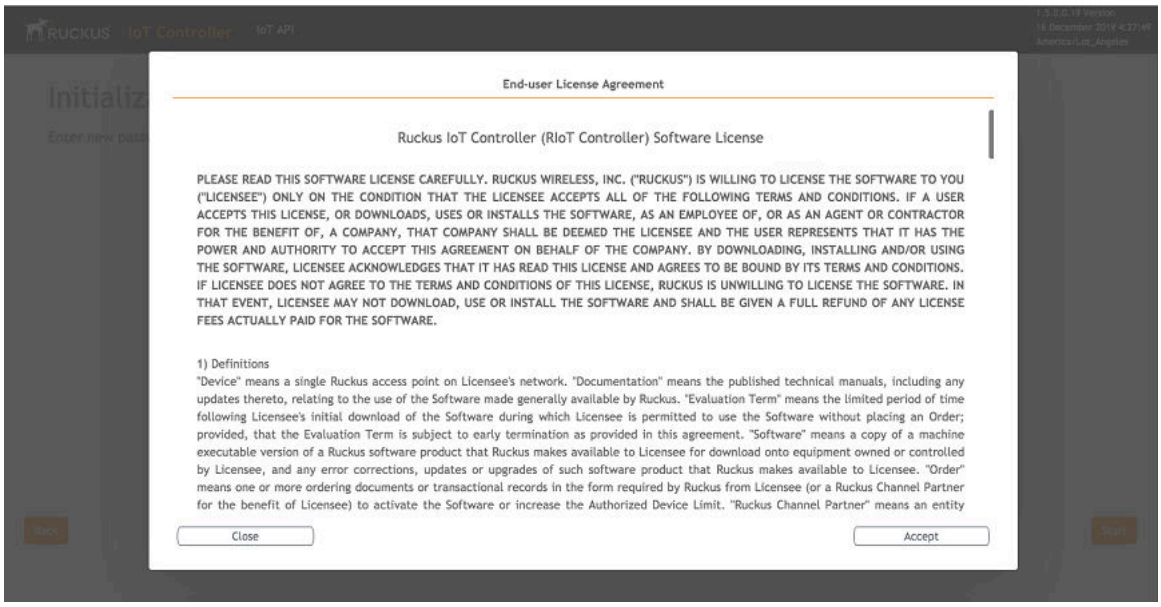
FIGURE 11 Confirming the Password



13. Enter a new password and re-enter the new password in the **Confirm Password** field. Click **Start**.

14. The **End-user License Agreement** page is displayed. Click **Accept** to accept the RUCKUS IoT Controller license.

FIGURE 12 End-user License Agreement Page



You are ready to configure and start the RUCKUS IoT Controller services. Refer to the *RUCKUS IoT Controller Configuration Guide* for more information.

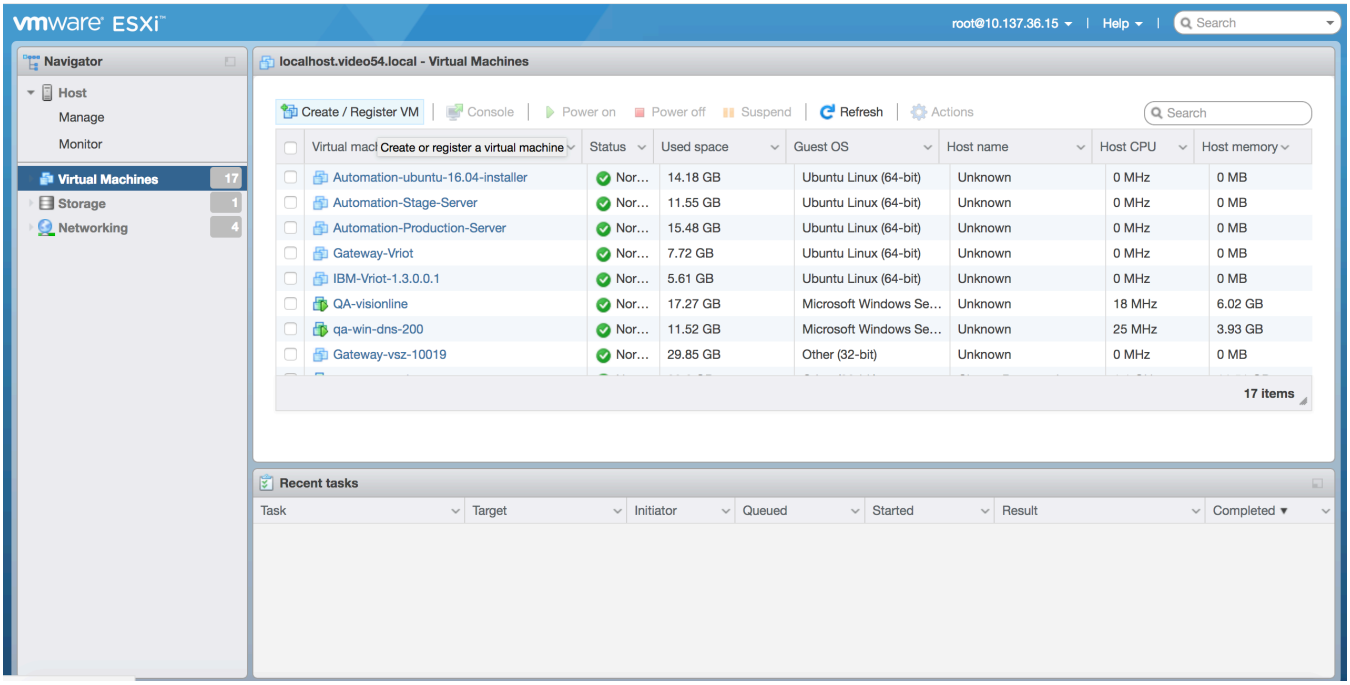
Installing RUCKUS IoT Controller on a VMware ESXi

The RUCKUS IoT Controller can be installed on a VMware ESXi hypervisor using an .OVA file.

1. Download the RUCKUS IoT Controller distribution package in the .OVA file format from the RUCKUS Support website at https://support.ruckuswireless.com.

2. Open VMware ESXi and select **Virtual Machines** from the **Navigator** pane.

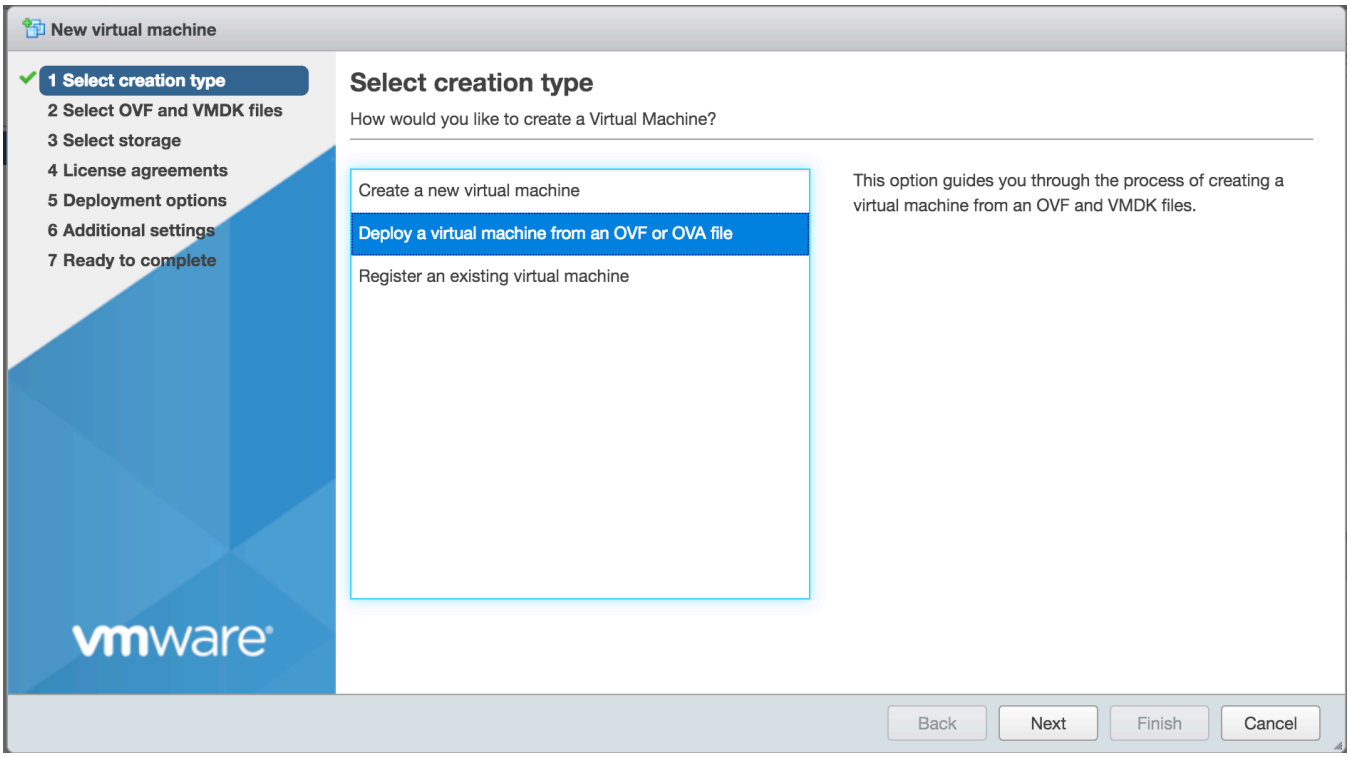
FIGURE 13 Creating or Registering Virtual Machines



3. Click **Create/Register VM**.

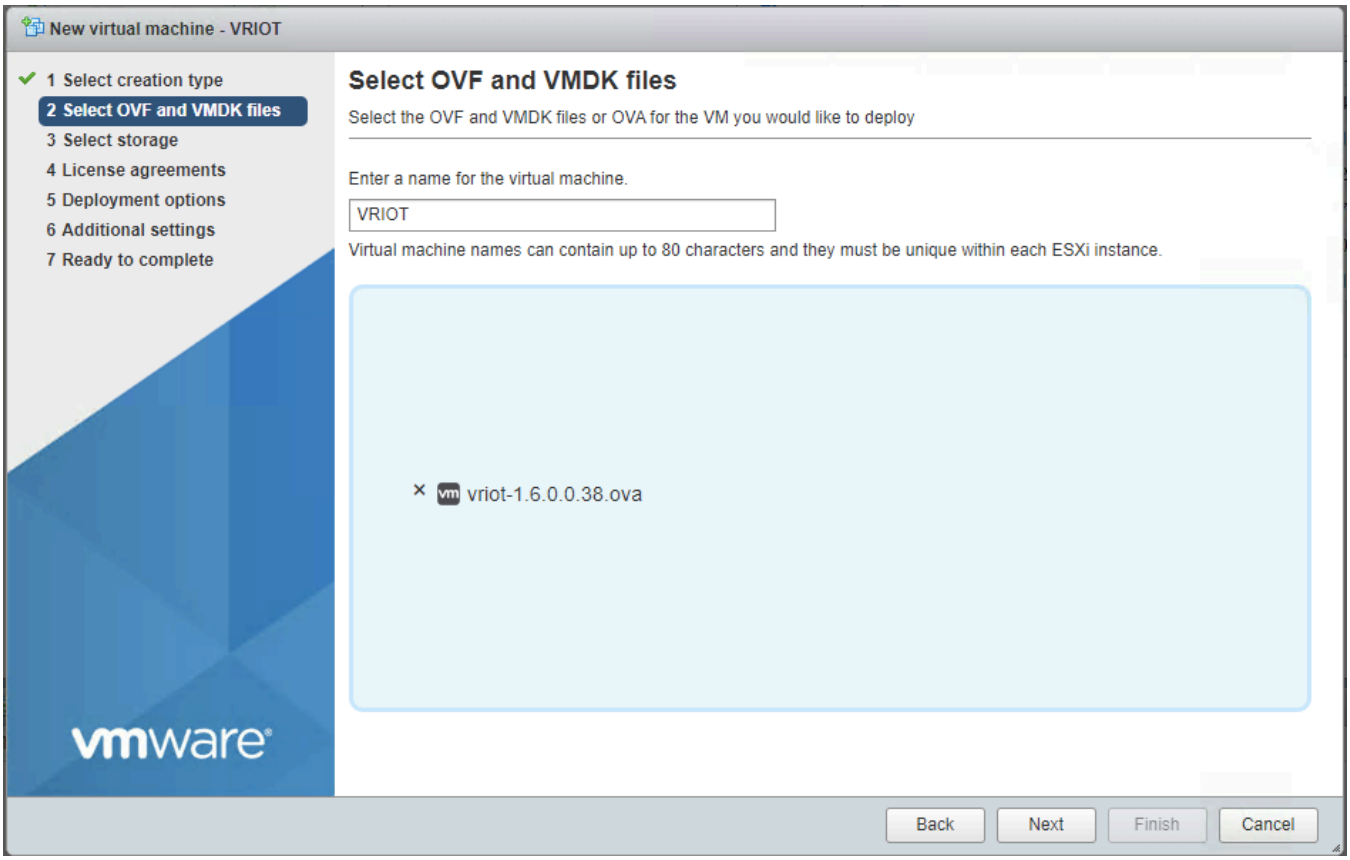
4. On the **New virtual machine** page, click **Select creation type**, and select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.

FIGURE 14 Select Creation Type Page



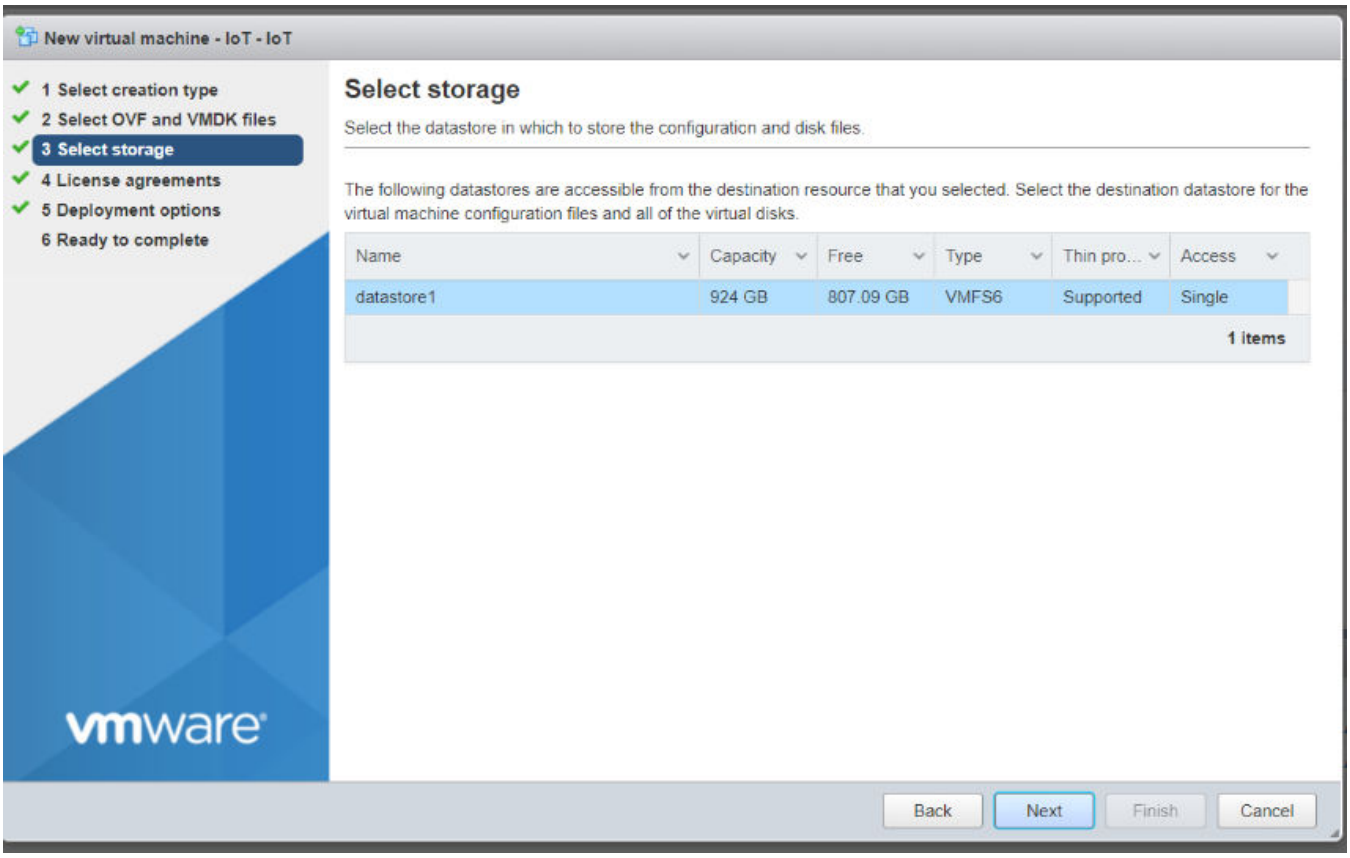
5. Click **Select OVF and VMDK files**, enter a name for the virtual machine, and select the OVF file. Click **Next**.

FIGURE 15 Select OVF and VMDK Files Page



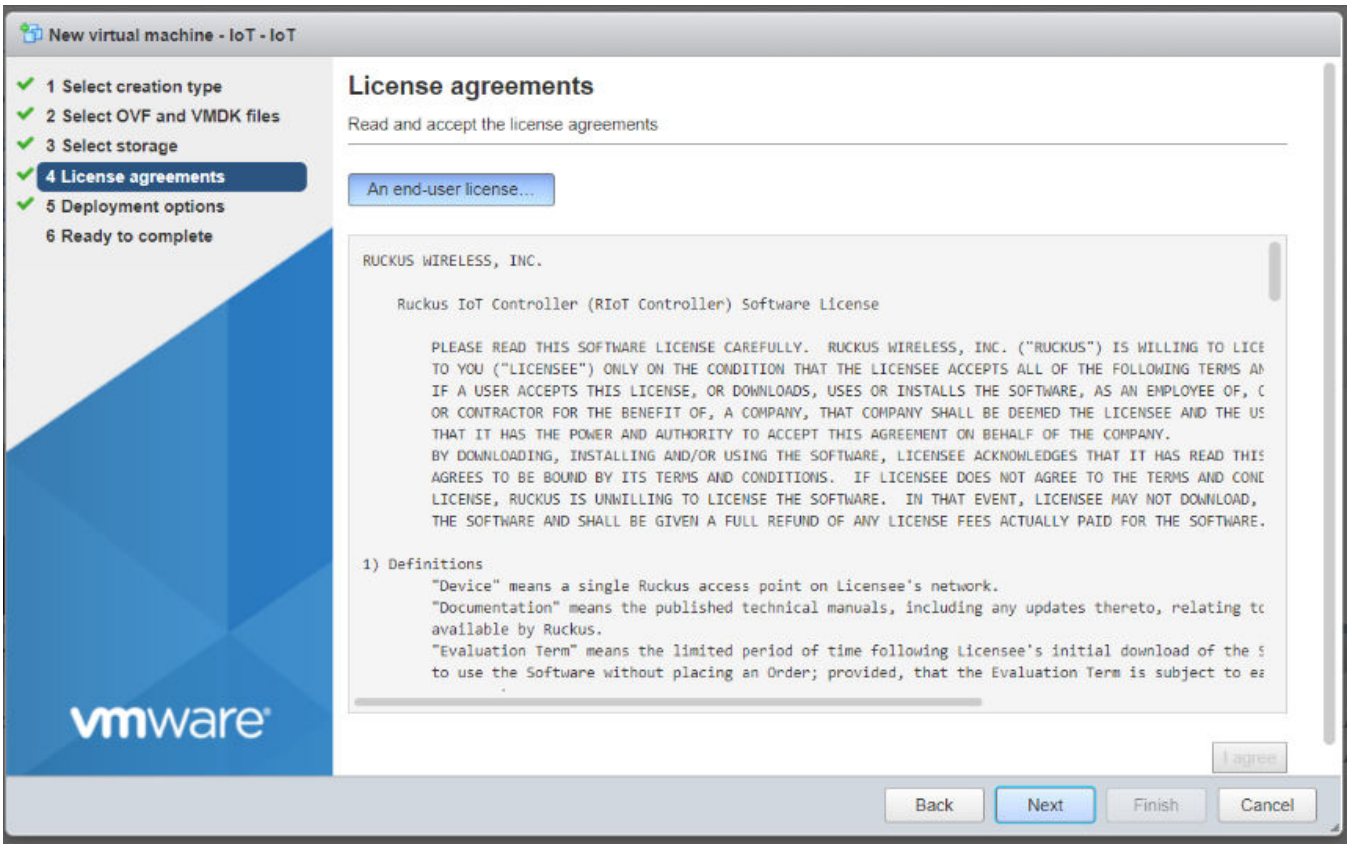
6. Click **Select storage**, and select the datastore in which you want to save the configuration and disk files. Click **Next**.

FIGURE 16 Select Storage Page



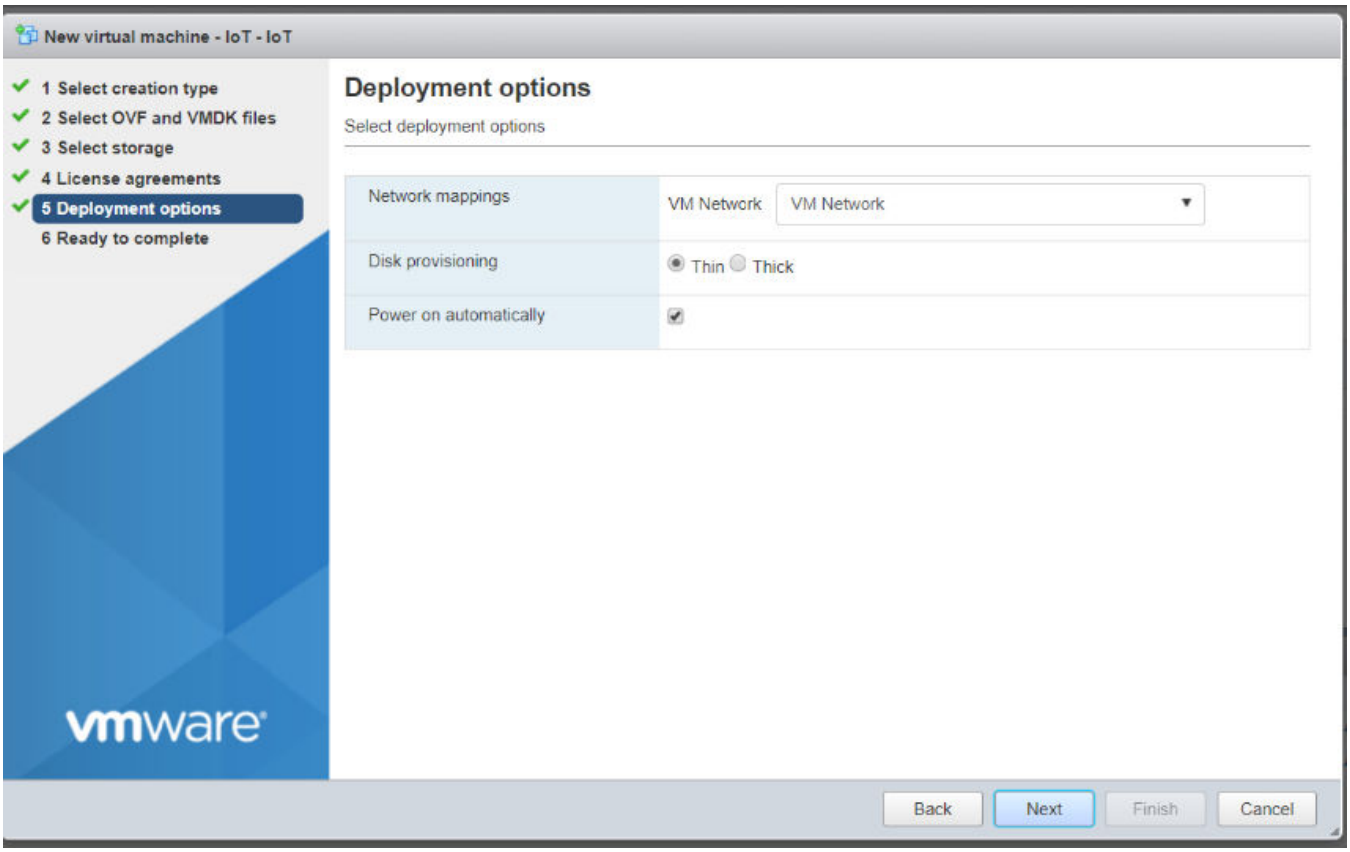
7. Click **License agreements** to accept the terms and conditions of the software license and click **Agree**.

FIGURE 17 License Agreements Page



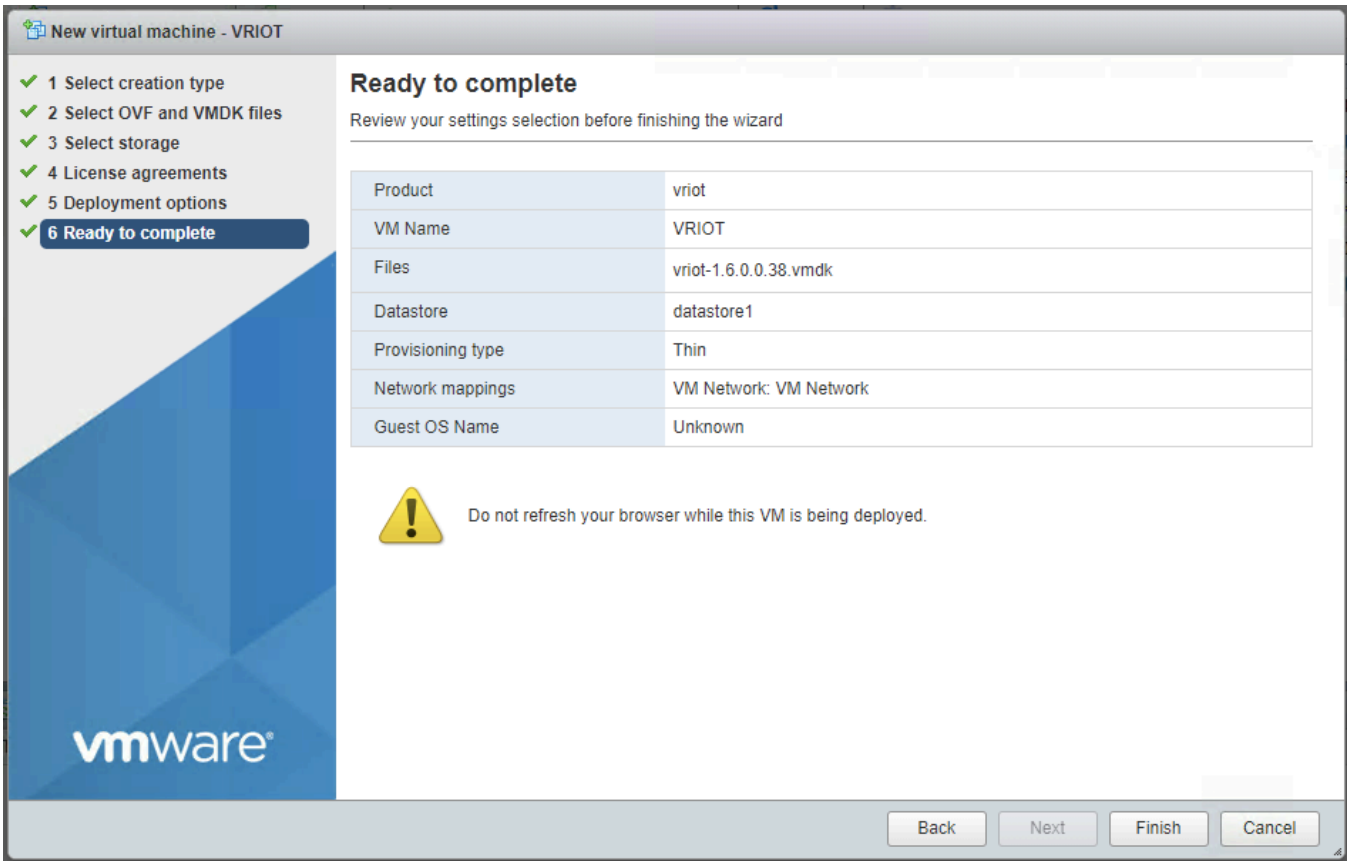
8. Click **Deployment options**, and select the **Network mappings** and **Disk provisioning**. Click **Next**.

FIGURE 18 Deployment Options Page



9. Click **Ready to complete** and review the settings. Click **Finish**.

FIGURE 19 Ready to Complete Page



The RUCKUS IoT Controller login prompt is displayed.

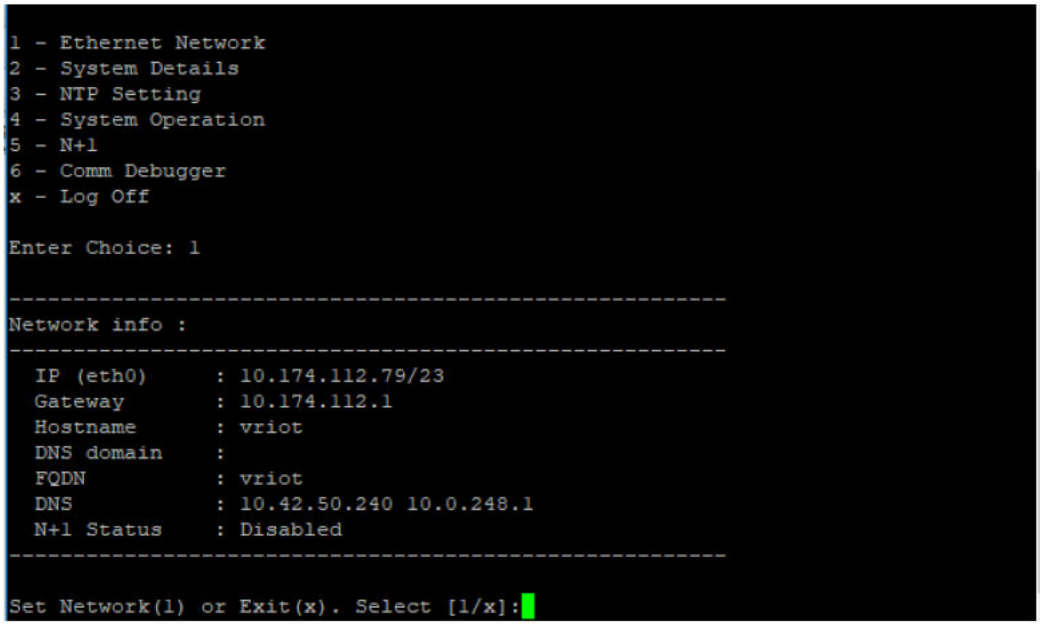
FIGURE 20 RUCKUS IoT Controller Login Prompt

10. Log in to the virtual machine using the username and password.

11. Enter **1** in the **Enter Choice** field to get the IP address of the virtual machine.

    This information is needed to access the RUCKUS IoT Controller **Initialization** page.

    FIGURE 21 Displaying the IP Address



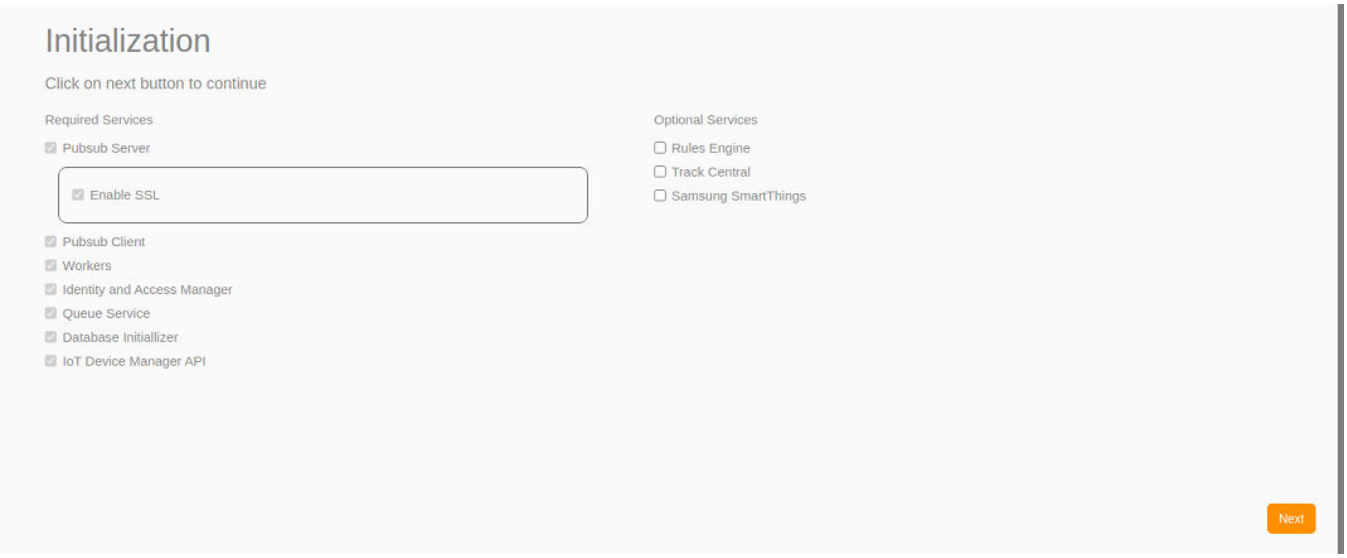
    To configure N+1 on the RUCKUS IoT Controller, enter **5** in the **Enter Choice** field. Refer to "Configuring N+1" in the *RUCKUS IoT Controller Configuration Guide* to complete this configuration.

12. Open a web browser on your host machine and enter the IP address of the VM in the address bar.

    HTTP and HTTPS on ports 80 and 443 are supported.

    The **Initialization** page is displayed.

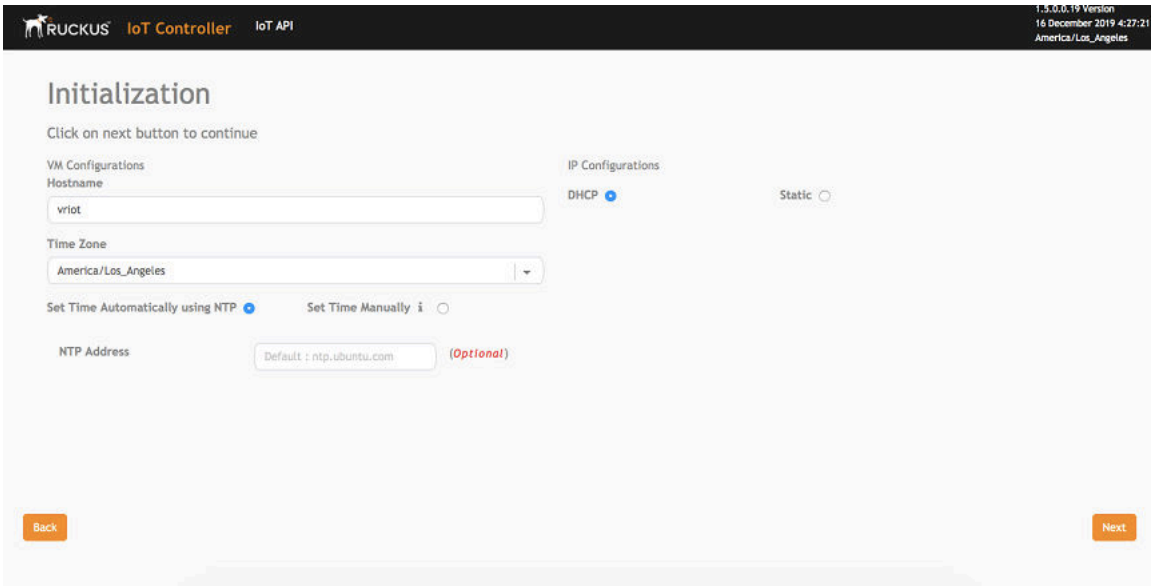
    FIGURE 22 Intialization Page



13. Select the required services and click **Next**.

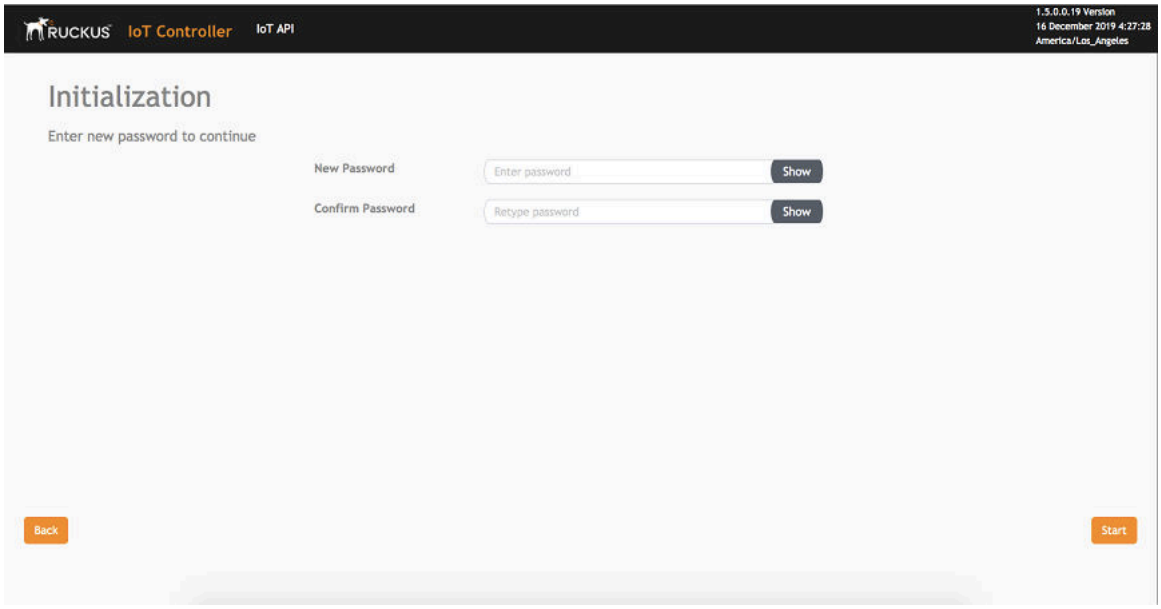
14. Confirm the configuration information and click **Next**.

FIGURE 23 Initial VM and IP Configurations



The **RUCKUS IoT ControllerInitialization** page is displayed.

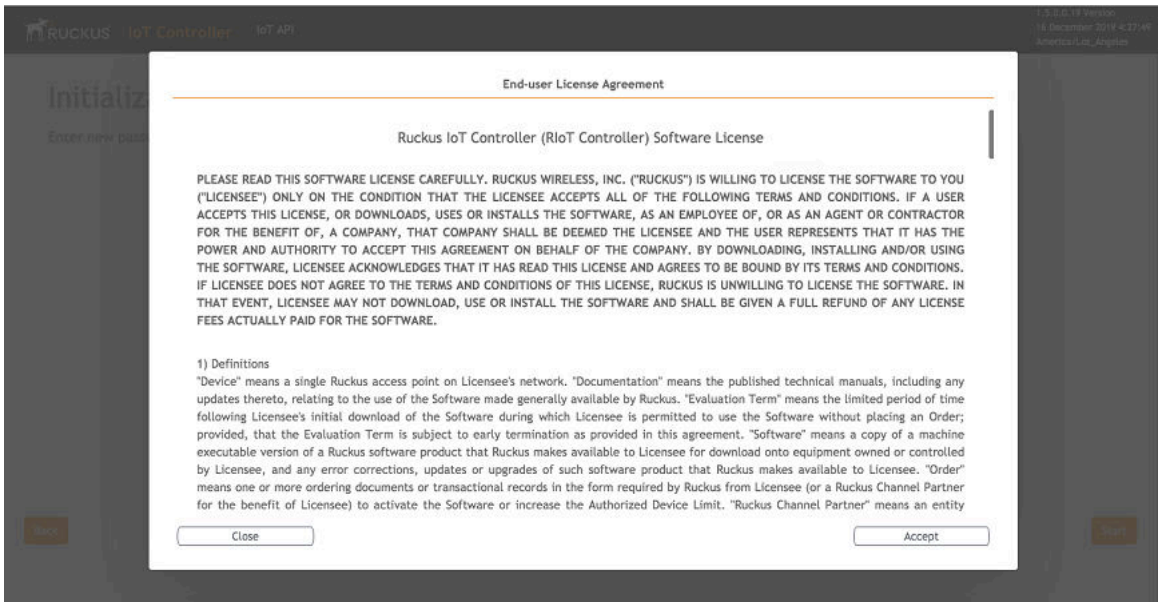
FIGURE 24 Confirming the Password



15. Enter a new password and re-enter the new password in the **Confirm Password** field. Click **Start**.

16. The **End-user License Agreement** page is displayed. Click **Accept** to accept the RUCKUS IoT Controller license.

FIGURE 25 End-user License Agreement Page



You are ready to configure and start the RUCKUS IoT Controller services. Refer to the *RUCKUS IoT Controller Configuration Guide* for more information.

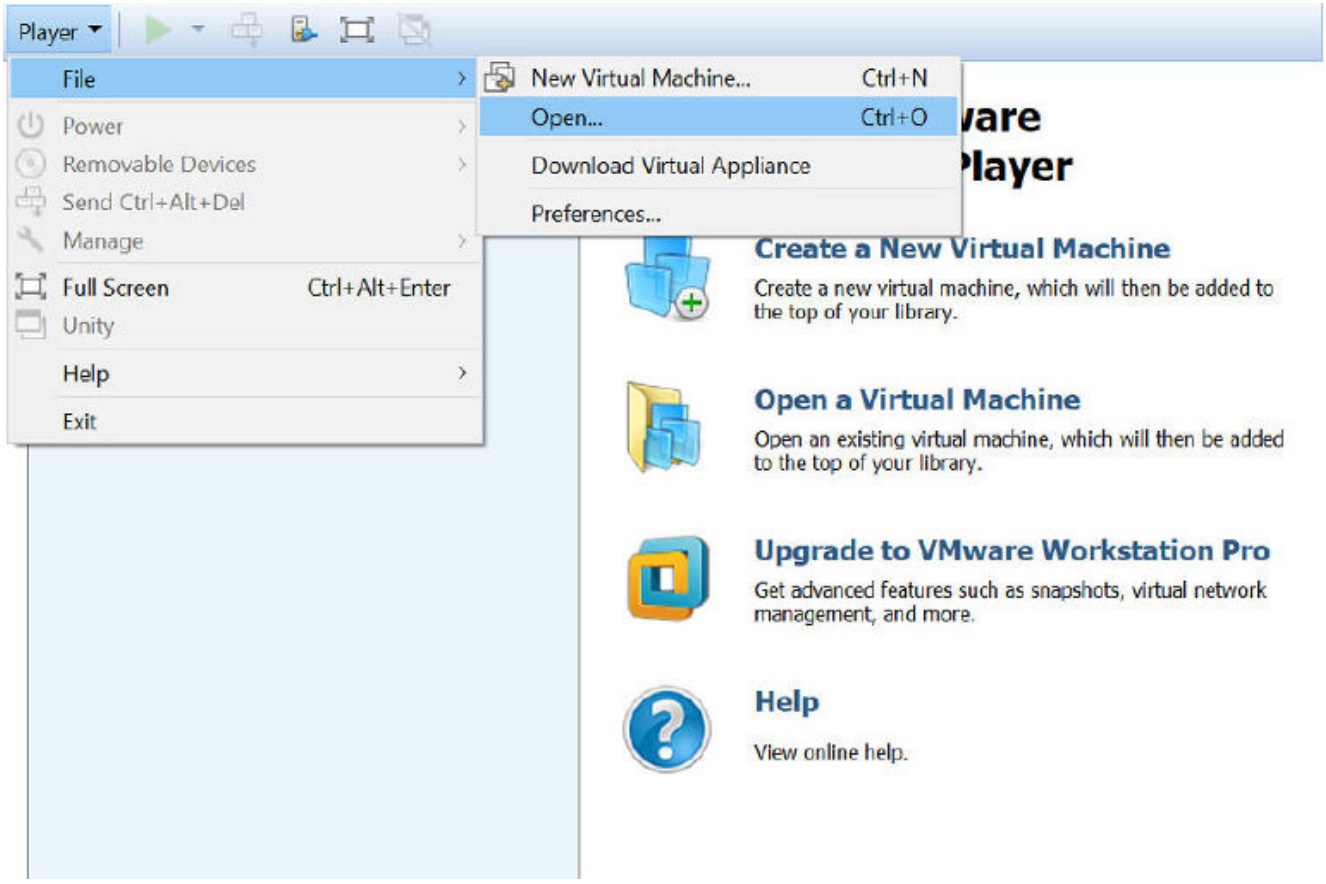
Installing RUCKUS IoT Controller Using VMware Player

The RUCKUS IoT Controller can be installed on a virtual machine using VMware Player.

1. Download the RUCKUS IoT Controller distribution package in the .OVA file format from the RUCKUS Support website at https://support.ruckuswireless.com.
2. Open VMware Player.

3. From the **Player** menu, select **File** > **Open**, and select the .OVA file for the RUCKUS IoT Controller.

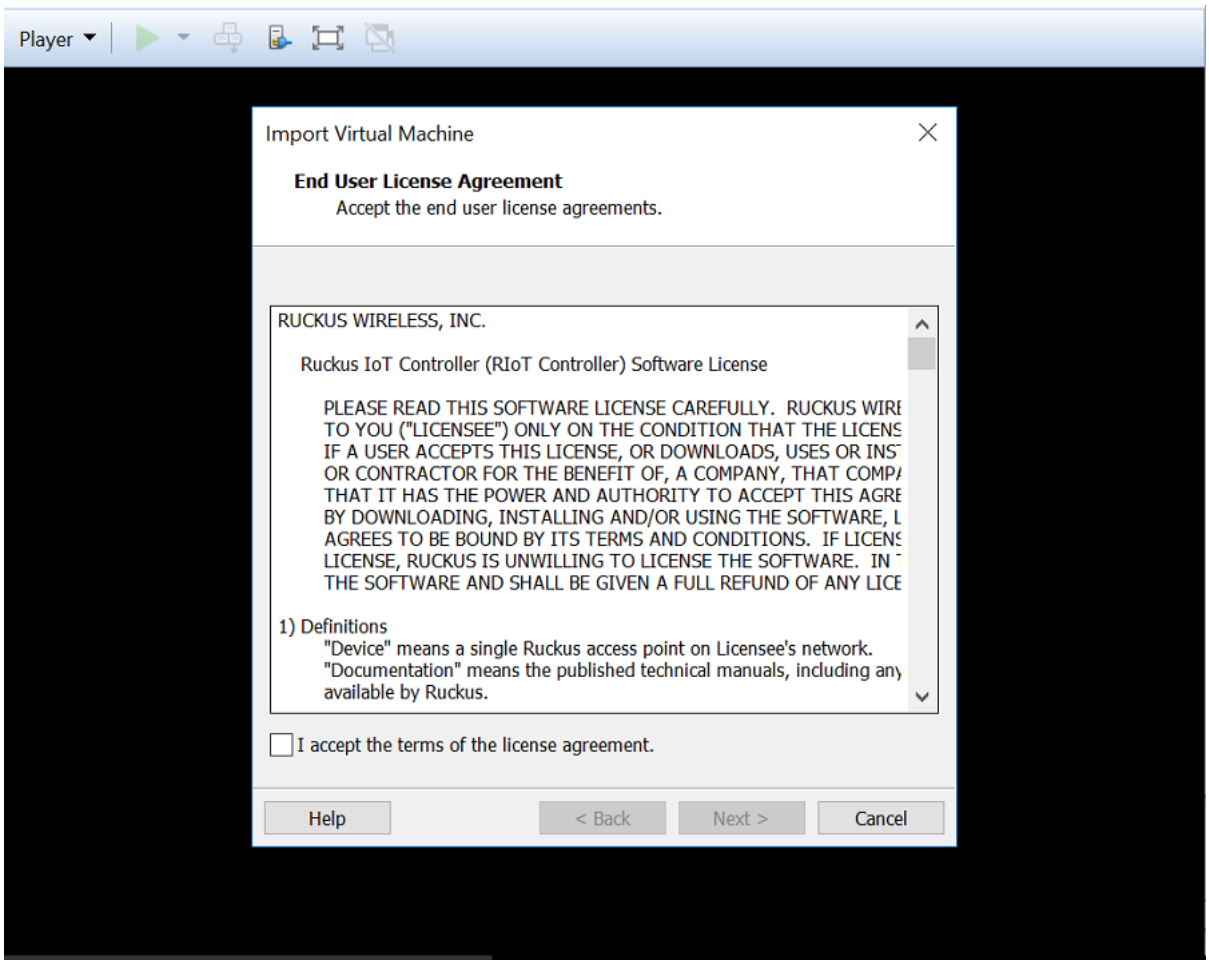
FIGURE 26 Selecting the .OVA File



The installation begins.

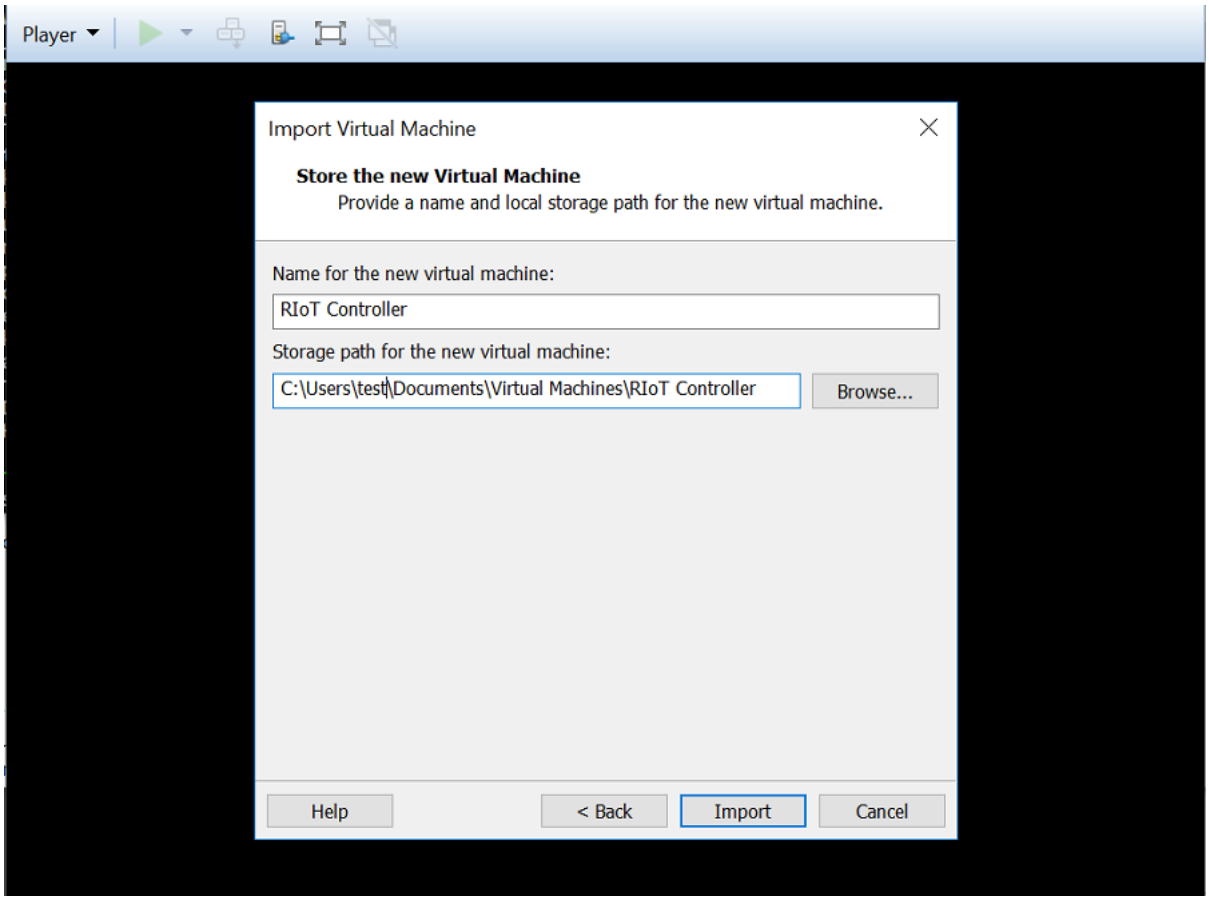
4. Accept the terms of the end user license agreement and click **Next**.

FIGURE 27 End User License Agreement



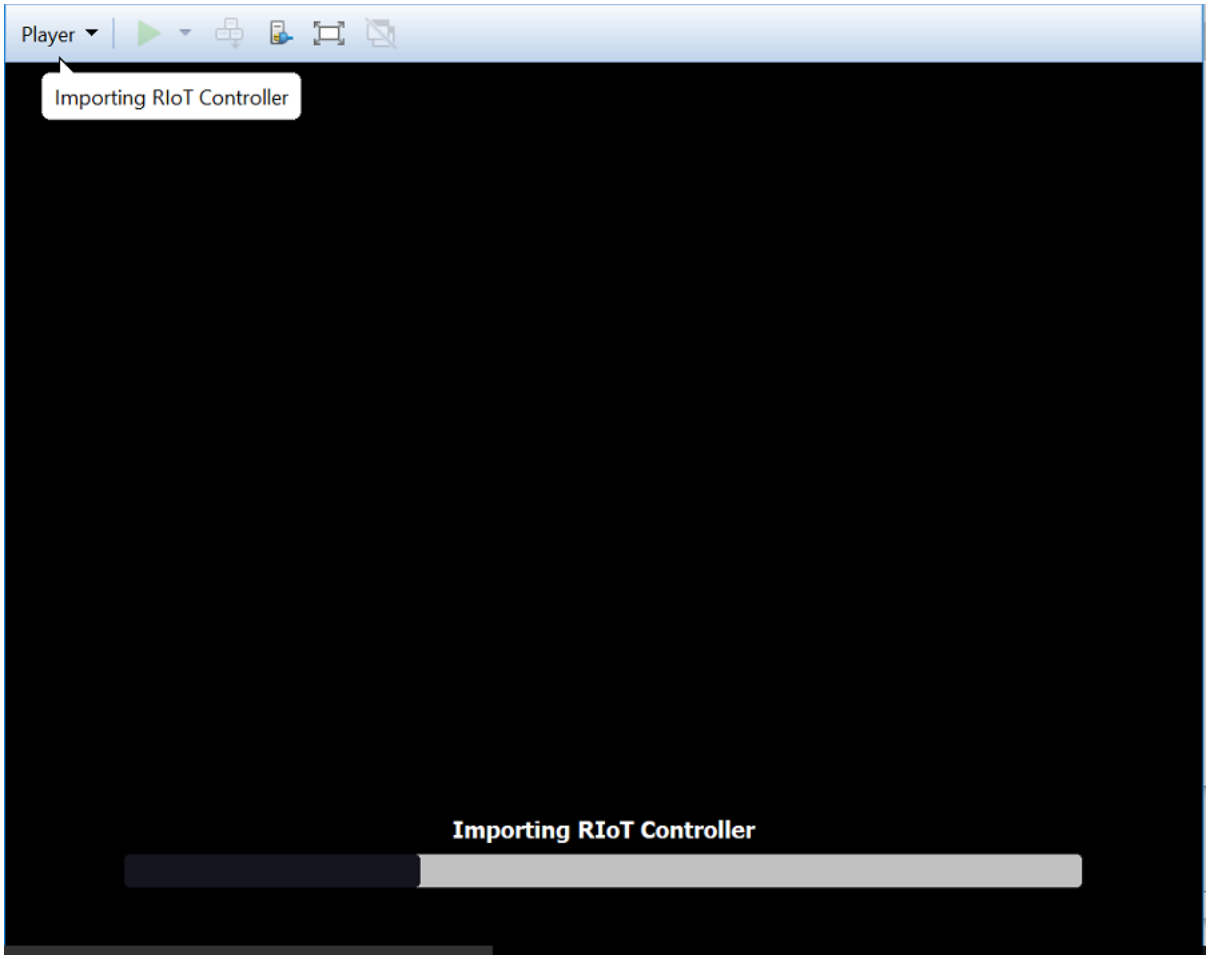
5. Enter a name and storage path for the virtual machine and click **Import**.

FIGURE 28 Naming the Virtual Machine



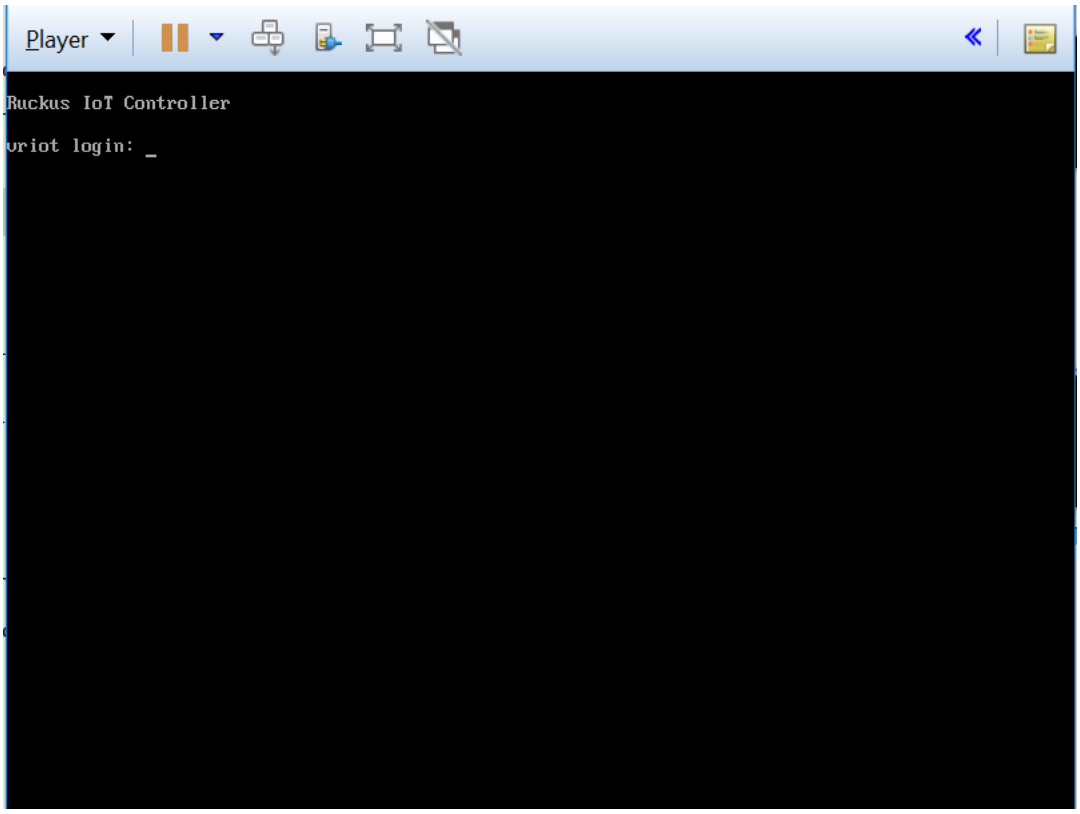
VMware Player begins importing the RUCKUS IoT Controller.

FIGURE 29 Importing the RUCKUS IoT Controller



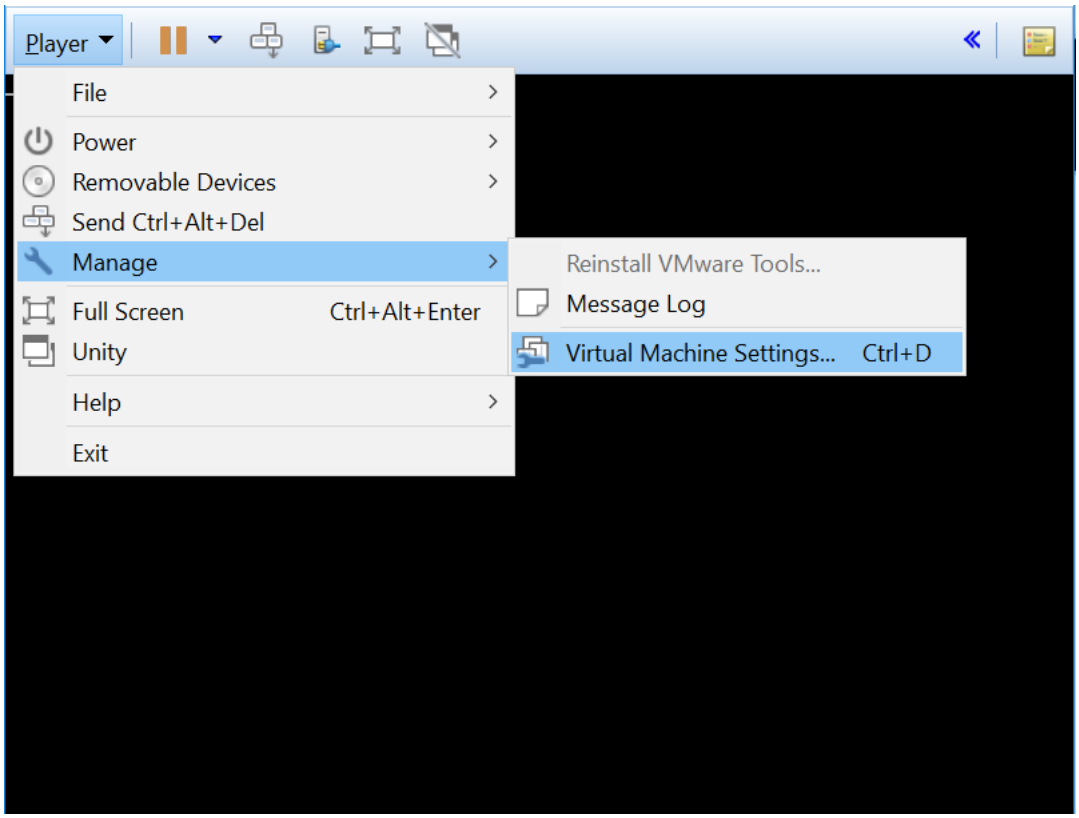
6. Log in to the RUCKUS IoT Controller using the username and password.

FIGURE 30 RUCKUS IoT Controller Login Prompt



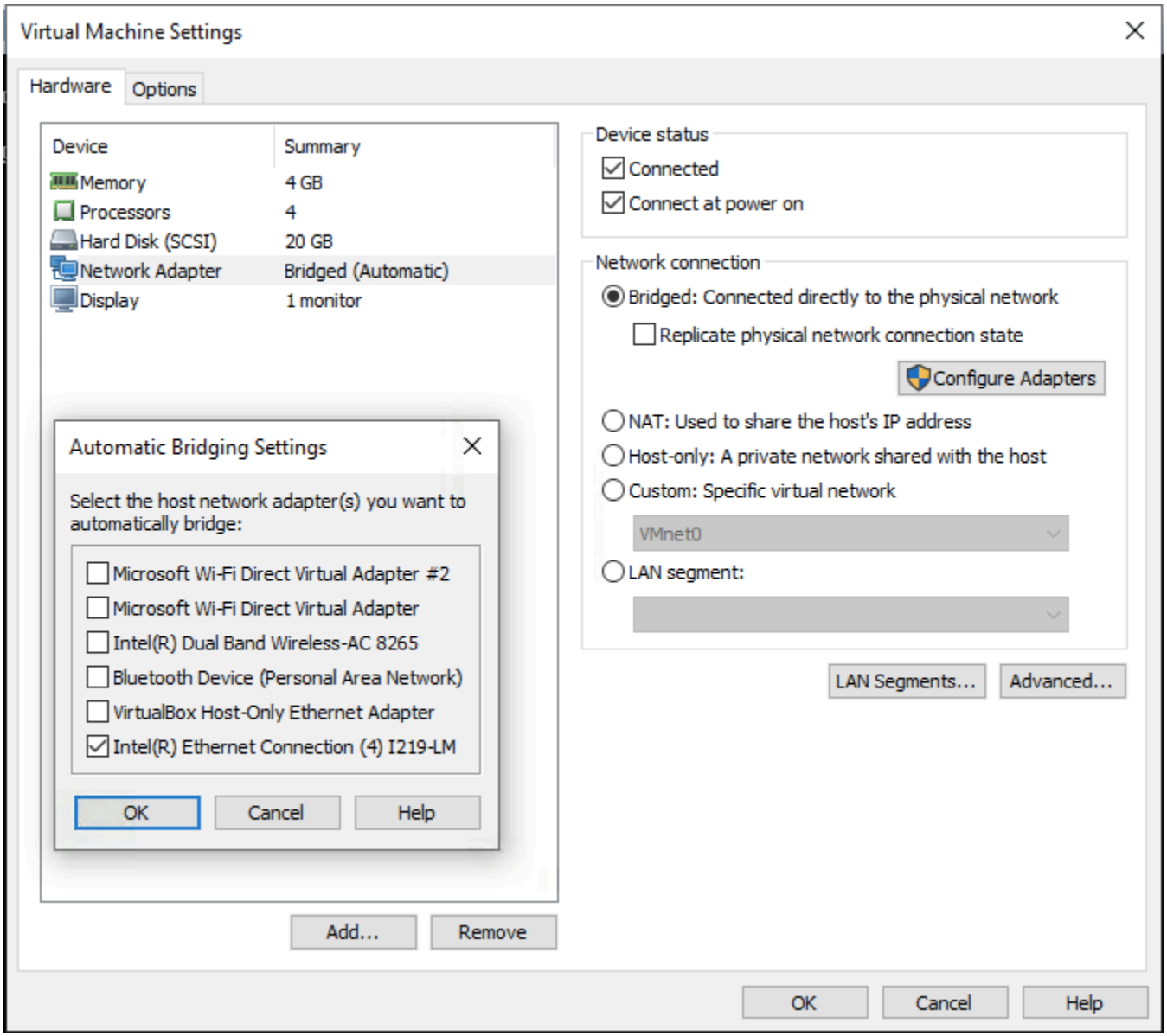
7. From the **Player** menu, select **Manage** > **Virtual Machine Settings** to open the settings for the virtual machine.

FIGURE 31 Opening the Virtual Machine Settings



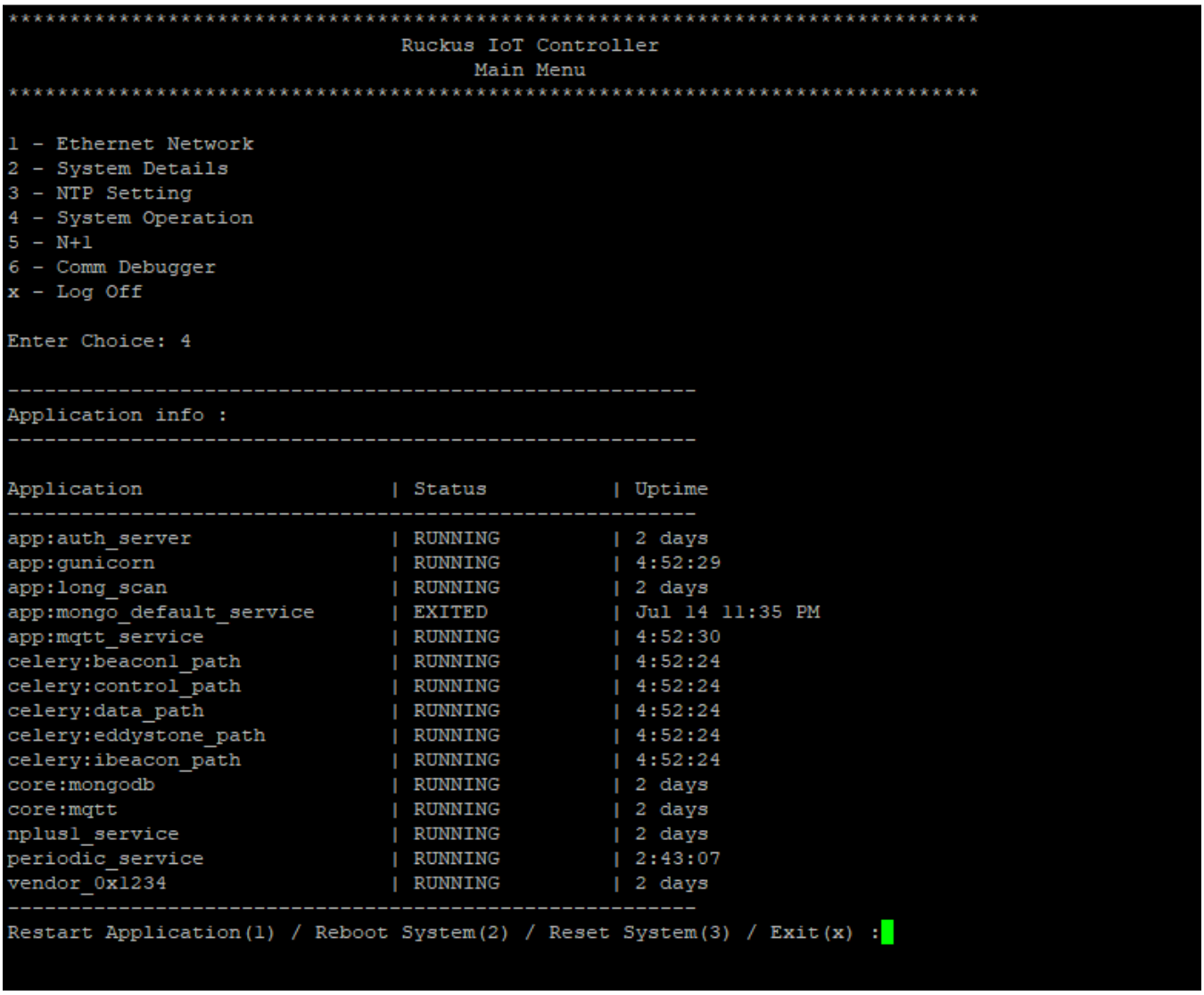
8. Click the **Bridged** network connection and select the appropriate host network adapter for automatic bridging. Click **OK**.

FIGURE 32 Virtual Machine Settings Page



9. In the RUCKUS IoT Controller Main Menu, enter **4** in the **Enter Choice** field to perform system operation on the controller. To restart the system, enter **1**. To reboot the system, enter **2** in the **Enter Choice** field.

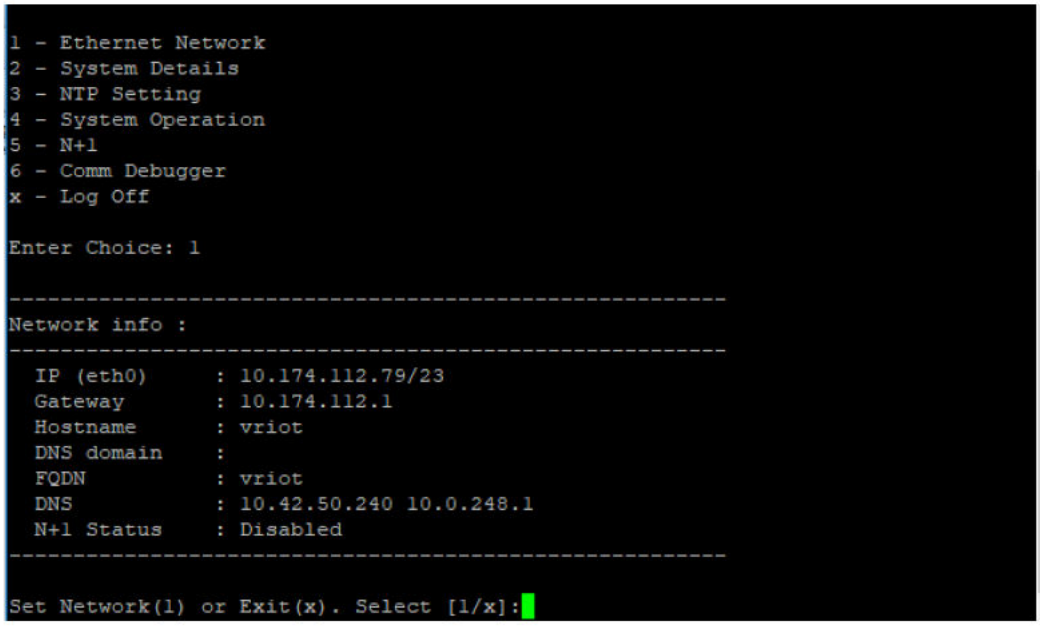
FIGURE 33 Rebooting RUCKUS IoT Controller



10. Enter **1** in the **Enter Choice** field to get the IP address of the virtual machine.

    This information is needed to access the RUCKUS IoT Controller**Initialization** page.

    FIGURE 34 Displaying the IP Address



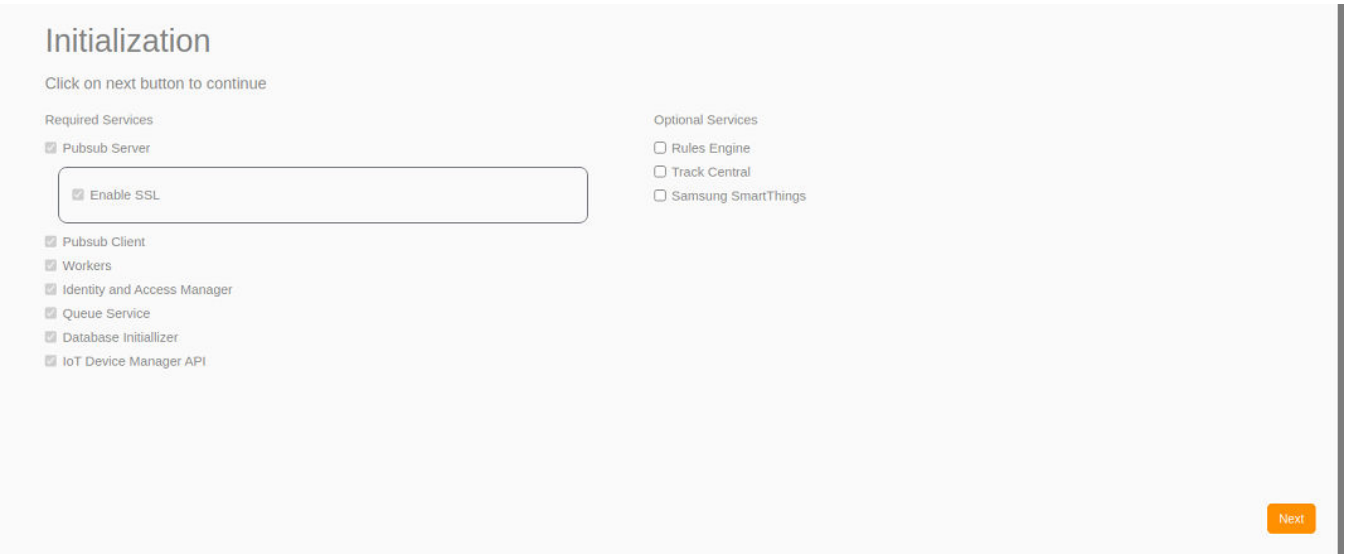
    To configure N+1 on the RUCKUS IoT Controller, enter **5** in the **Enter Choice** field. Refer to "Configuring N+1" in the *RUCKUS IoT Controller Configuration Guide* to complete this configuration.

11. Open a web browser on your host machine and enter the IP address of the VM in the address bar.

    HTTP and HTTPS on ports 80 and 443 are supported.

    The **Initialization** page is displayed.

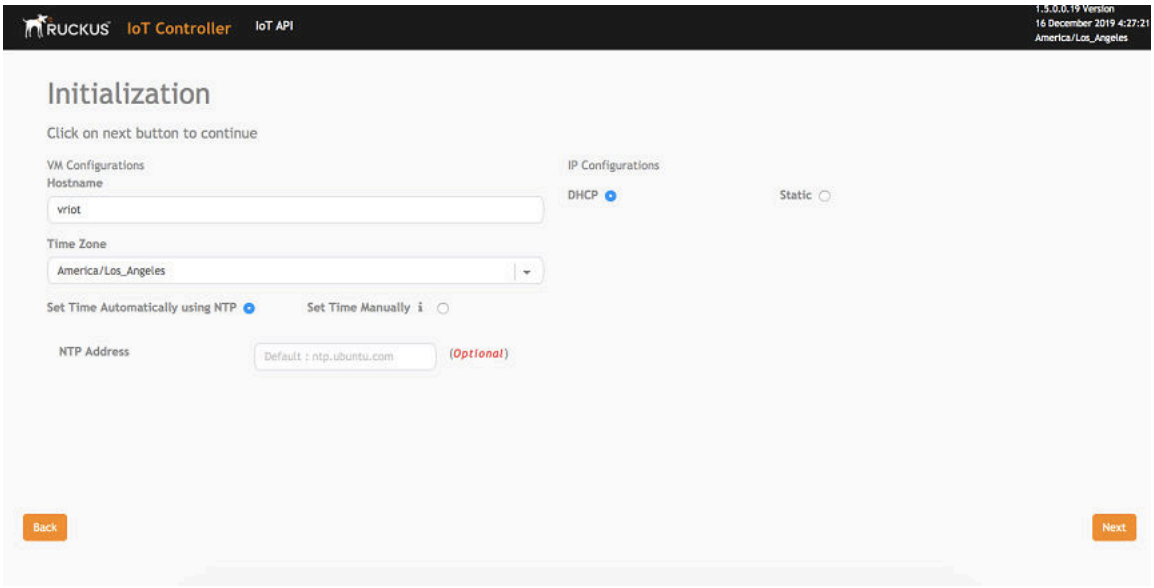
    FIGURE 35 Intialization Page



12. Select the required services and click **Next**.

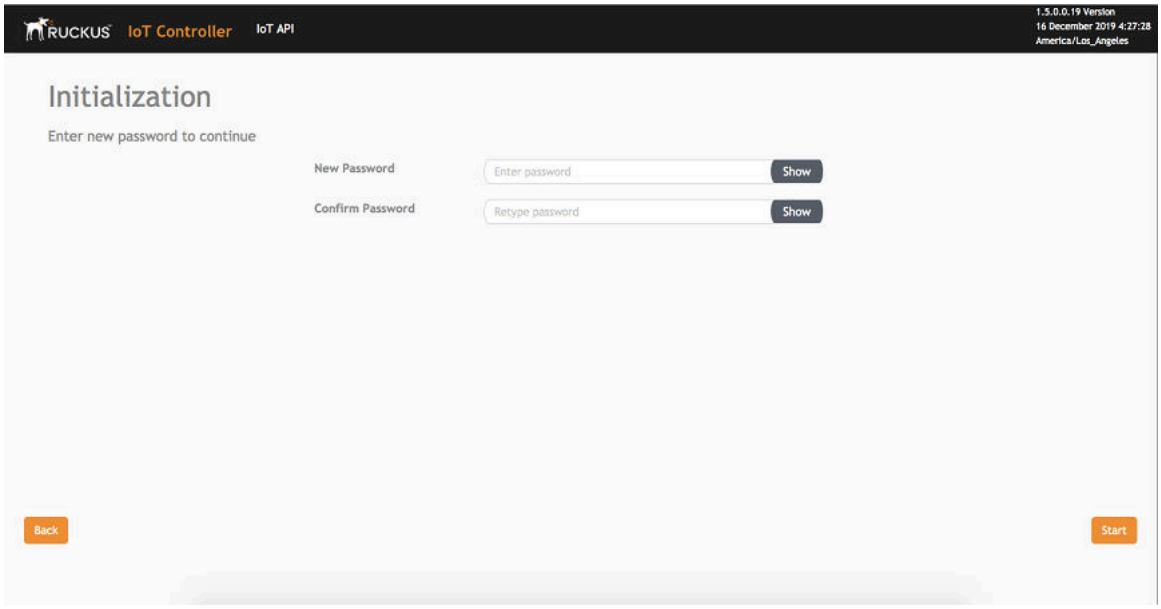
13. Confirm the configuration information and click **Next**.

FIGURE 36 Initial VM and IP Configurations



The **RUCKUS IoT ControllerInitialization** page is displayed.

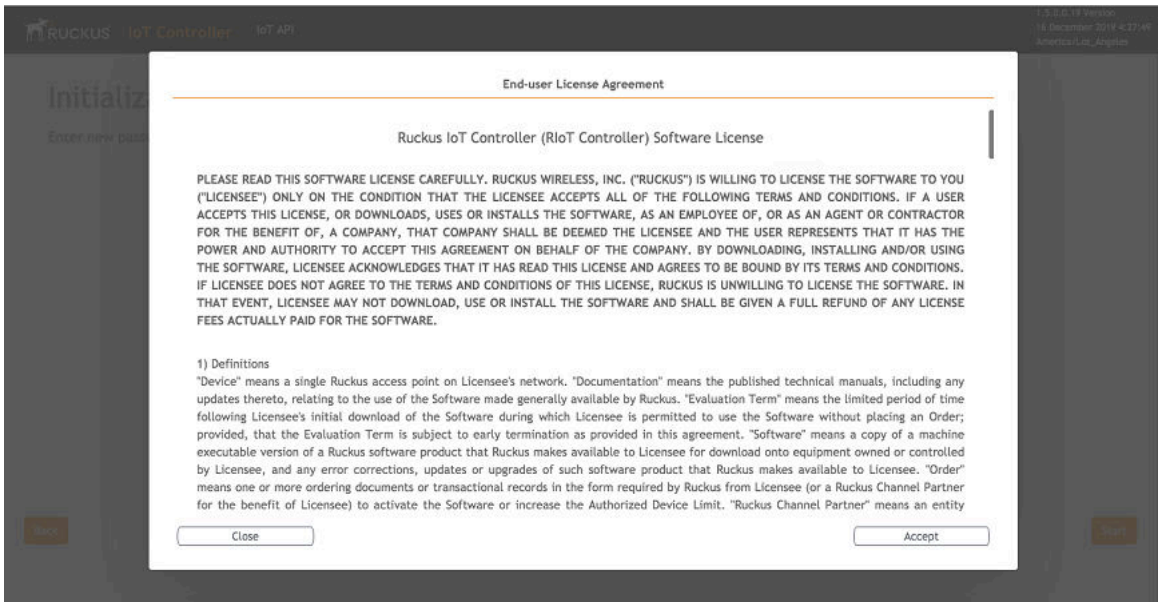
FIGURE 37 Confirming the Password



14. Enter a new password and re-enter the new password in the **Confirm Password** field. Click **Start**.

15. The **End-user License Agreement** page is displayed. Click **Accept** to accept the RUCKUS IoT Controller license.

FIGURE 38 End-user License Agreement Page



You are ready to configure and start the RUCKUS IoT Controller services. Refer to the *RUCKUS IoT Controller Configuration Guide* for more information.

Installing a KVM Guest Using virsh Commands

The RUCKUS IoT Controller can be installed on the KVM Guest using virsh commands.

1. Use the **tar -xvf vriot-qcow2-1.6.0.0.x.tar** command to extract the vriot-qcow2-1.6.0.0.x.tar file.
2. Use the **sudo mv vriot-1.6.0.0.x.qcow2 /var/lib/libvirt/images/** command to move the qcow2 image to the libvirt images path..
3. Use the **virsh define vriot-1.6.0.0.x.xml** command to define the VM.

   NOTE
   You must edit the XML file to add it to the network interface

4. Use the **virsh start Ruckus-IoT-Controller** command to start the virtual machine (VM).
5. Use the **virsh console Ruckus-IoT-Controller** command to obtain console access to the VM.

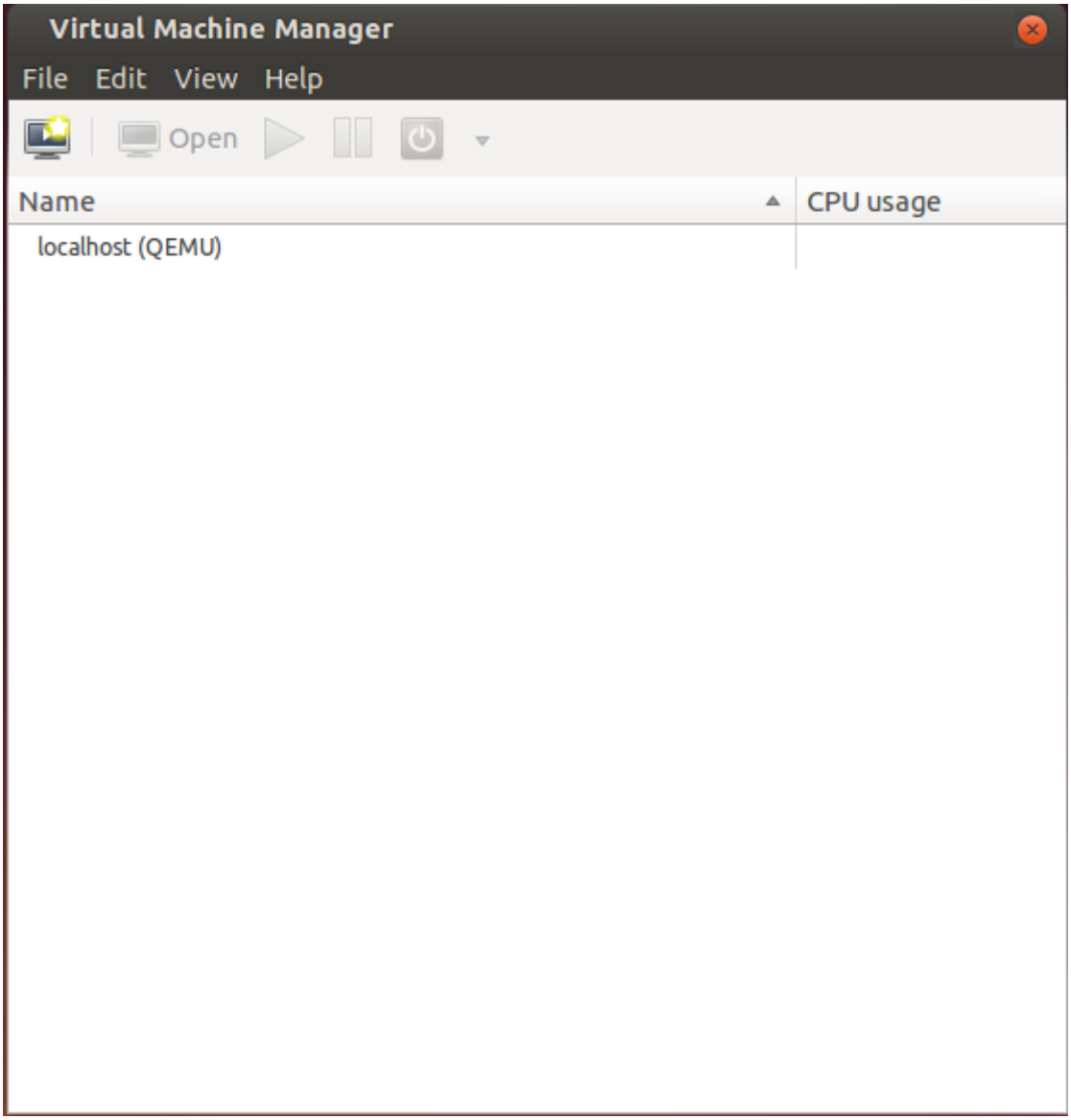
Installing a KVM Guest Using Virtual Machine Manager

The RUCKUS IoT Controller can be installed on a KVM guest using Virtual Machine Manager.

1. Download the RUCKUS IoT Controller distribution package in the .tar file format from the RUCKUS Support website at https://support.ruckuswireless.com.
2. Use the **tar -xvf filename.tar** command to obtain the qcow2 image file and template file.

3. Open the Virtual Machine Manager.
4. From the **Virtual Machine Manager** menu, select **File** > **Create a New Virtual Machine**.

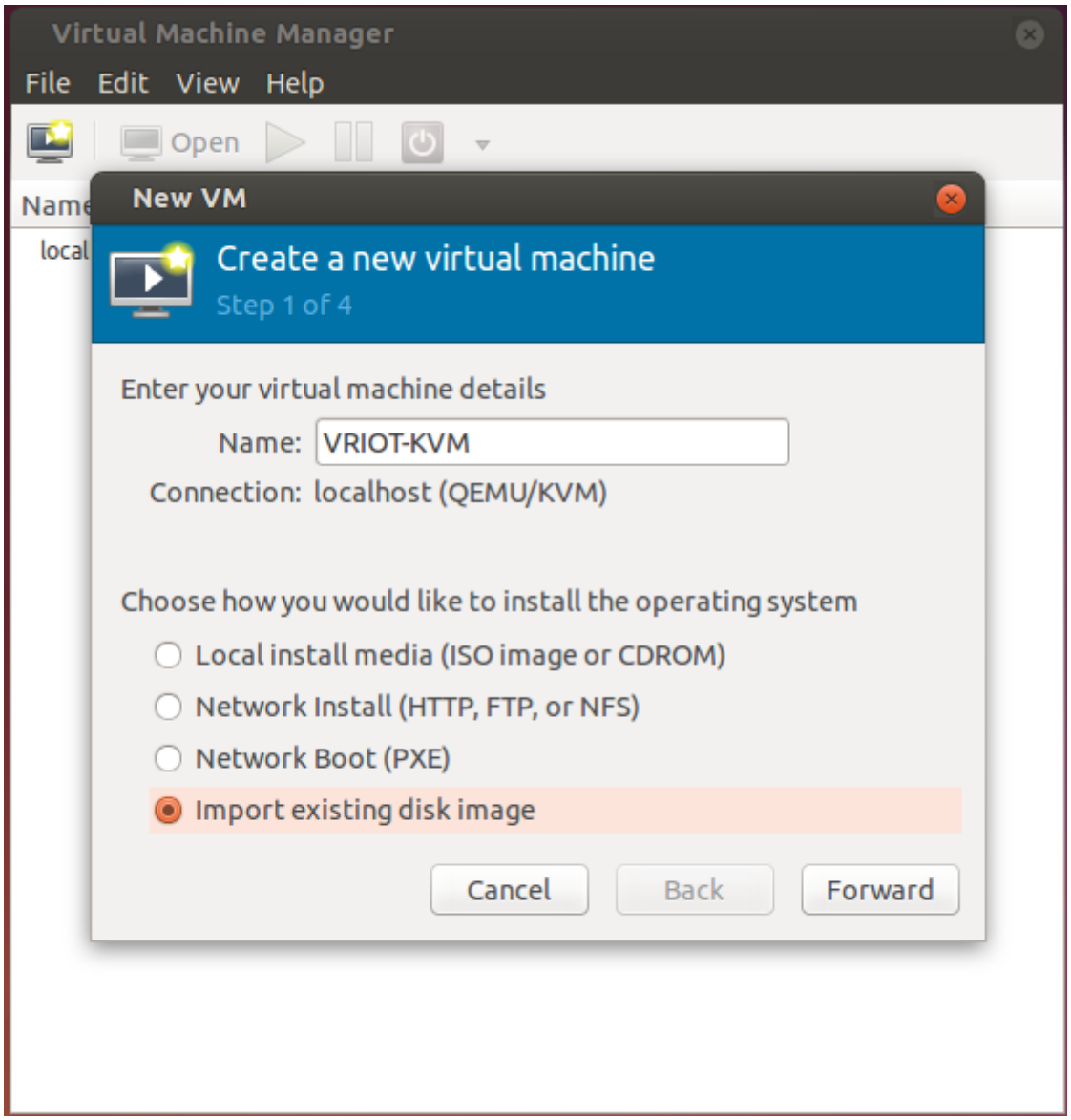
FIGURE 39 Virtual Machine Manager Menu



The **New VM** dialog box is displayed.

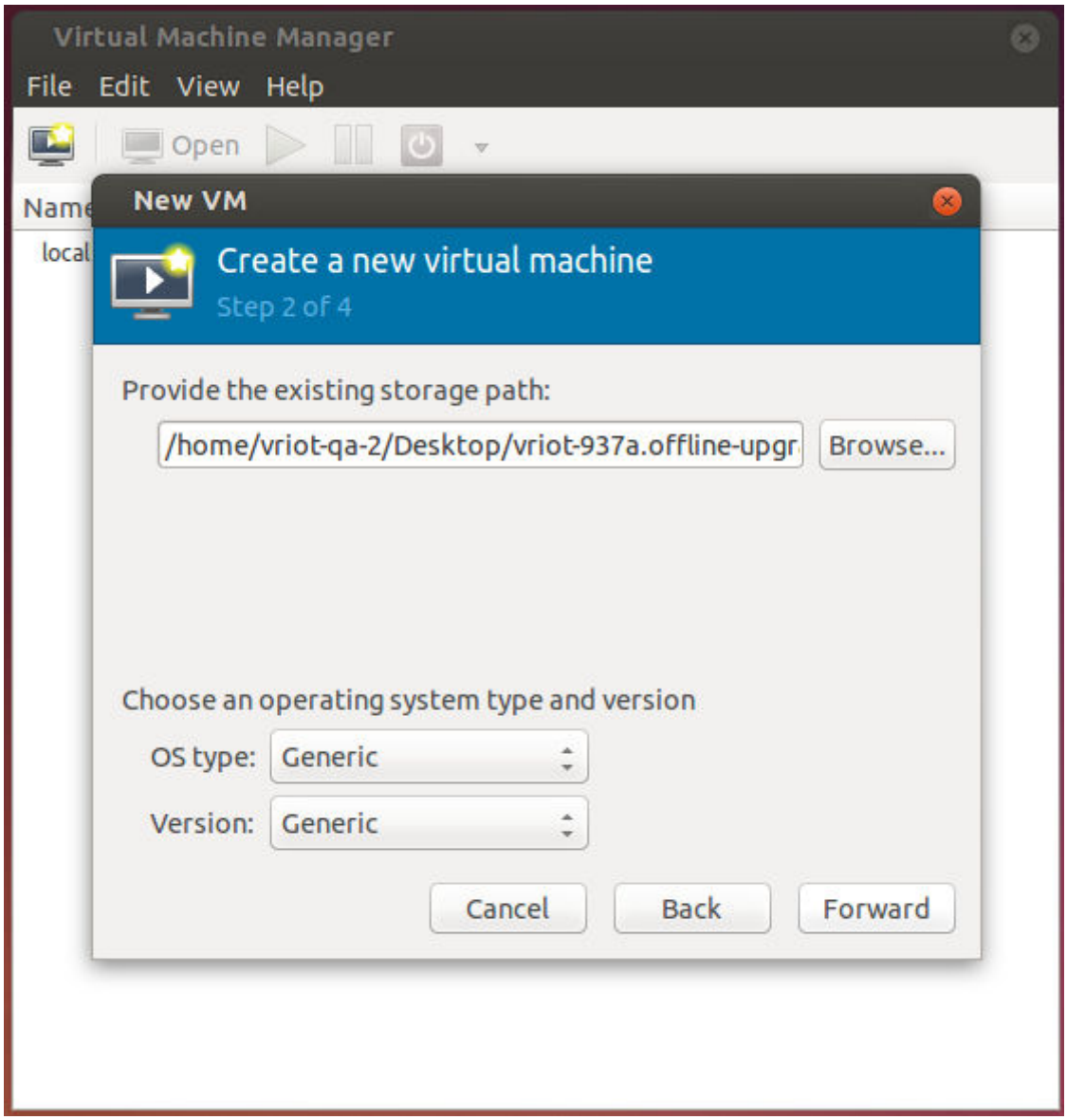
5. Enter the name of the virtual machine, select **Import existing disk image**, and click **Forward**.

FIGURE 40 New VM Dialog Box Step 1



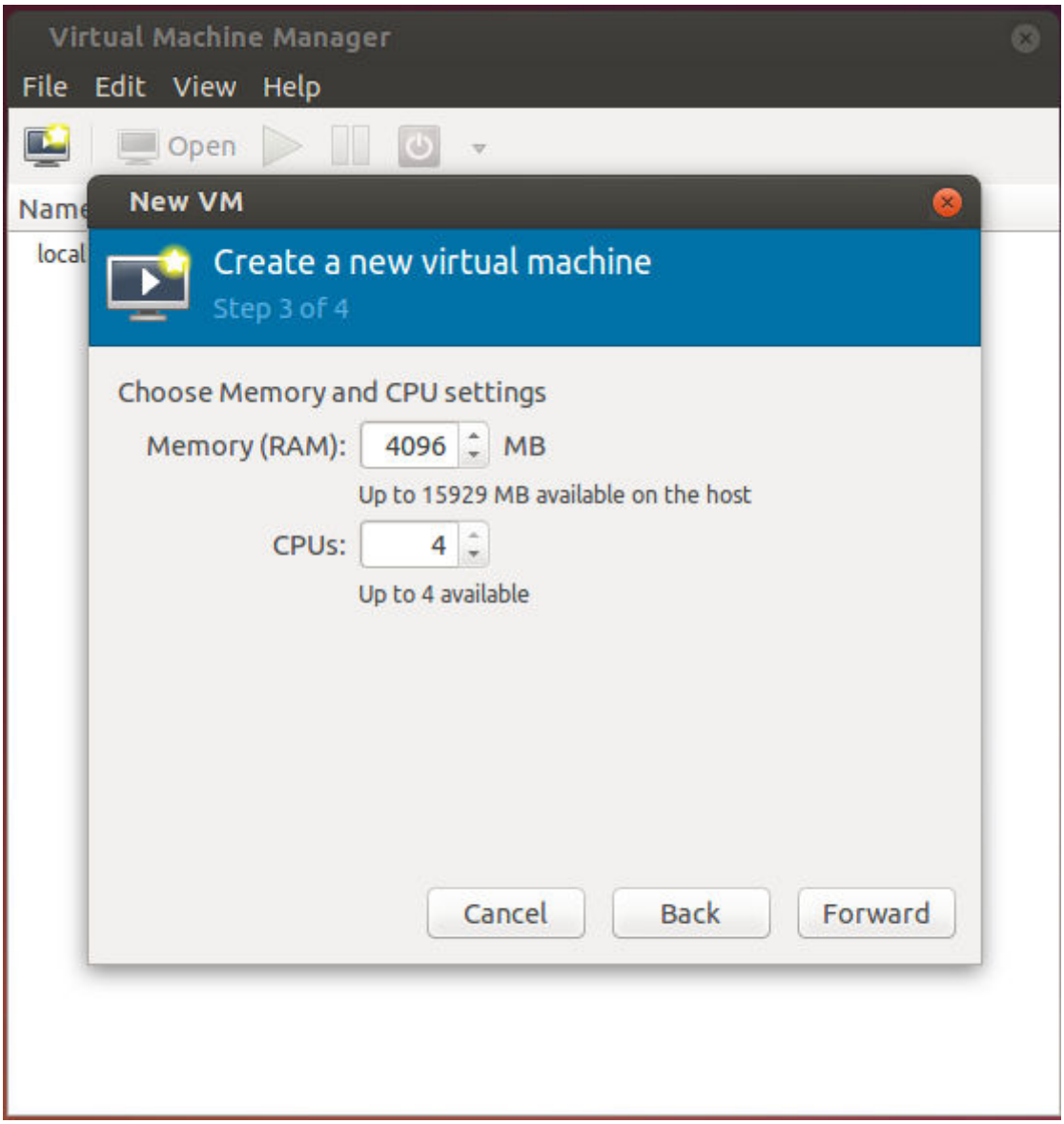
6. Enter the path of the .qcow image, the operating system type, and the version number, and click **Forward**.

FIGURE 41 New VM Dialog Box Step 2



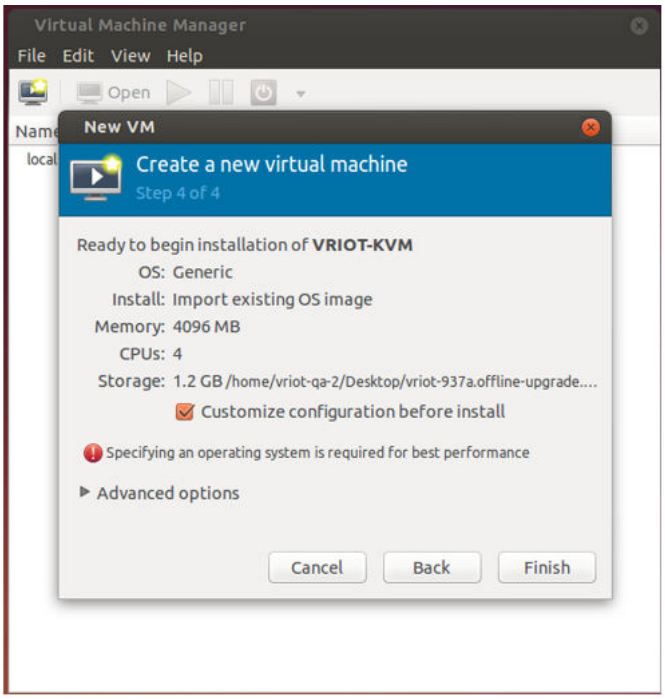
7. Select the memory size of RAM (in MB) and the number of central processing units (CPUs) for the virtual machine, and click **Forward**.

FIGURE 42 New VM Dialog Box Step 3



8. Select **Customize configuration before install**, and click **Finish**.

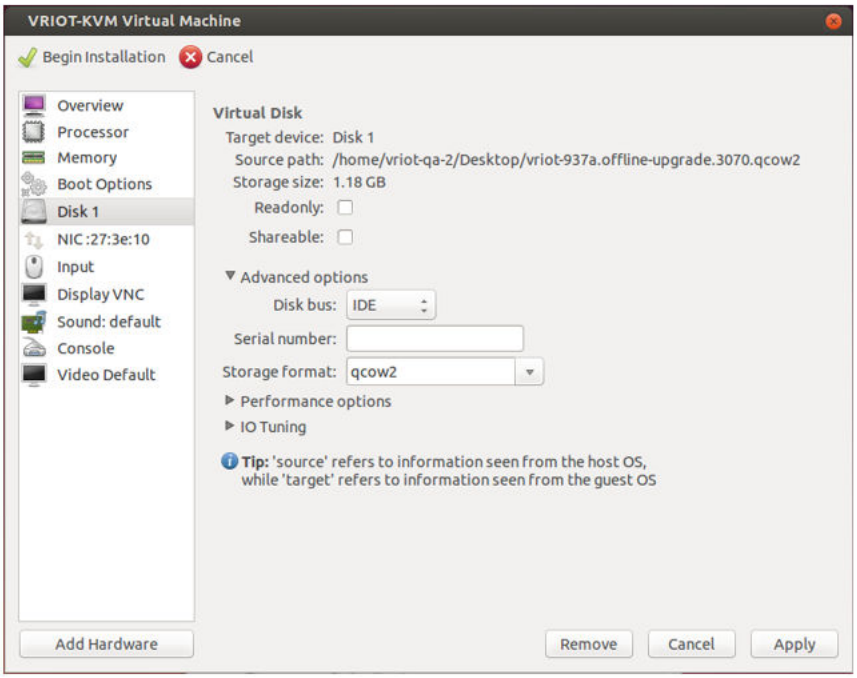
FIGURE 43 New VM Dialog Box Step 4



The RUCKUS IoT Controller installation on the virtual manager begins.

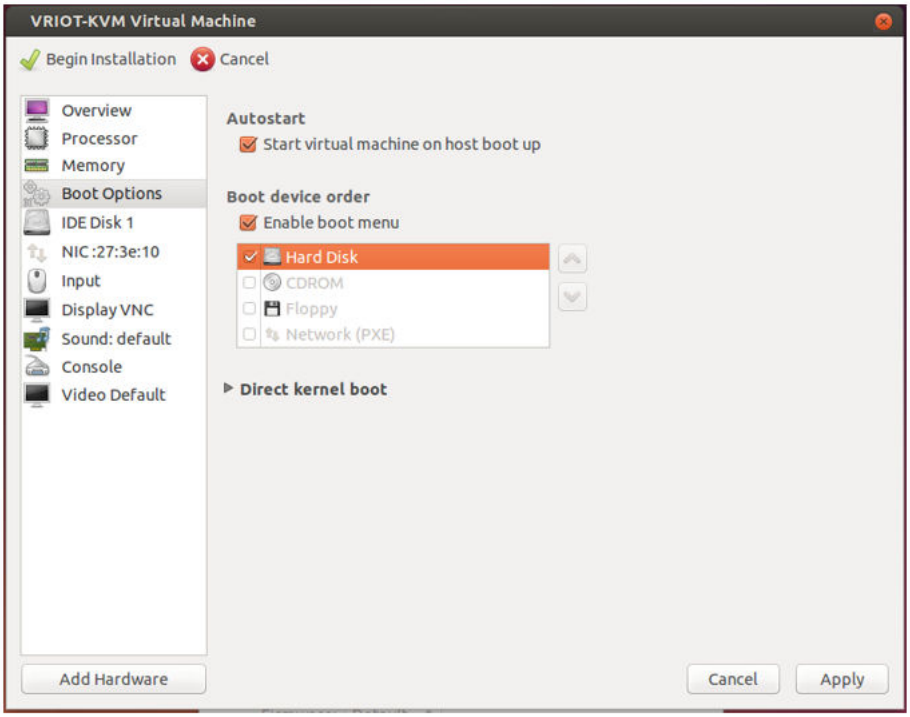
9. After the installation has completed, open the Virtual Machine Manager. Select **Disk** in the left pane and information about the disk is displayed. Expand **Advanced options** and ensure that the disk bus is **IDE** and the storage format is **qcow2**.

FIGURE 44 Virtual Disk Configuration



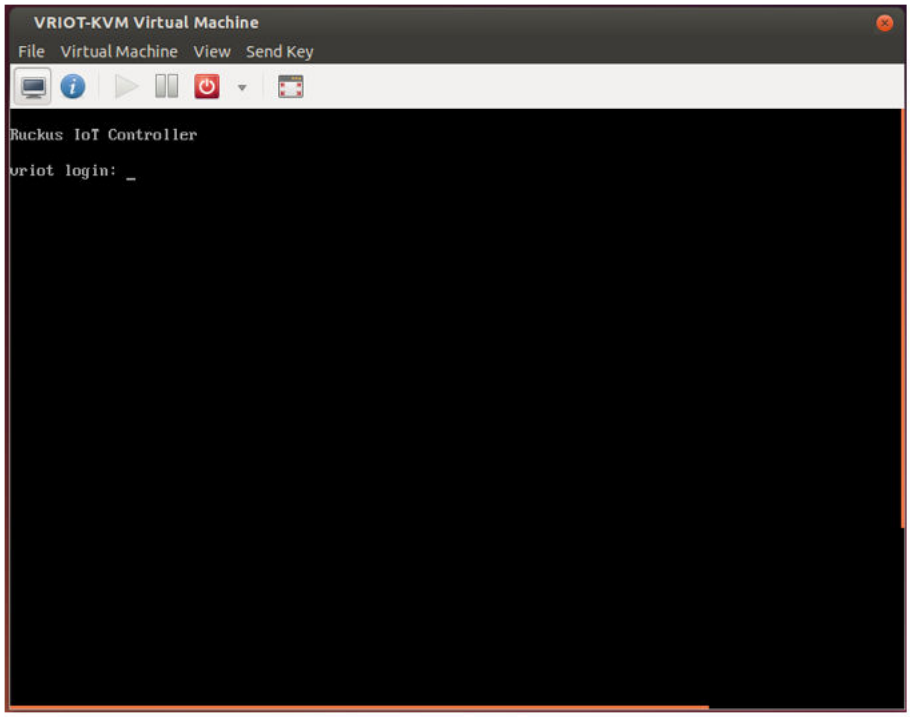
10. Select **Boot Options** in the left pane. Ensure that **Start virtual machine on host boot up** and **Enable boot menu** are selected. Select **Hard Disk** and click **Apply**.

FIGURE 45 Boot Options Configuration



11. Log in to the RUCKUS IoT Controller using the username and password.

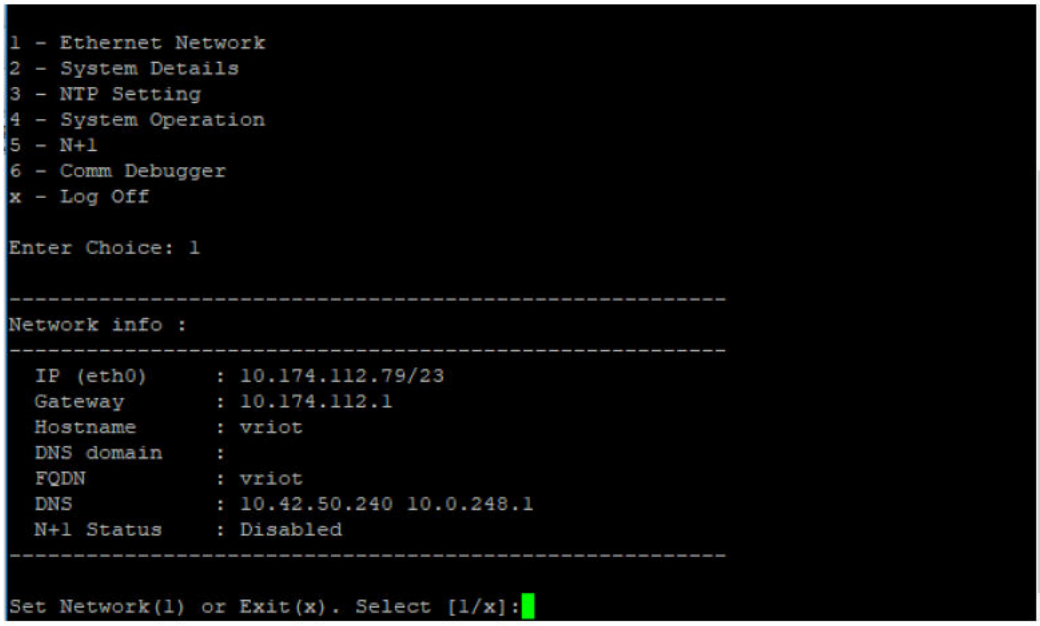
FIGURE 46 RUCKUS IoT Controller Login Prompt



12. Enter **1** in the **Enter Choice** field to get the IP address of the virtual machine.

    This information is needed to access the RUCKUS IoT Controller **Initialization** page.

    FIGURE 47 Displaying the IP Address



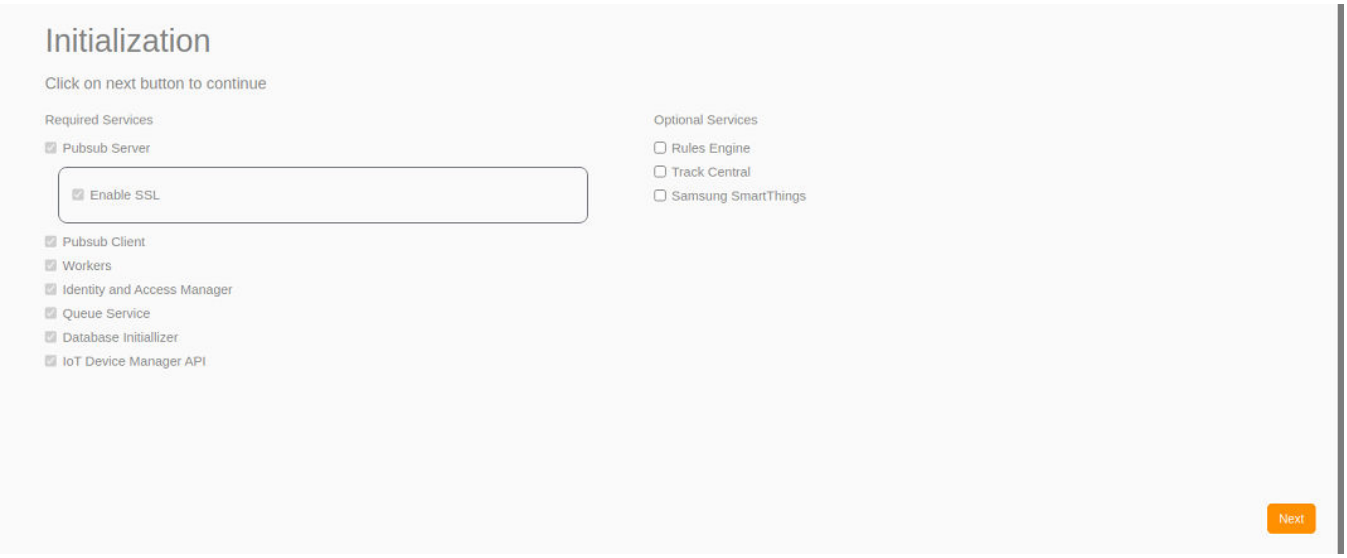
    To configure N+1 on the RUCKUS IoT Controller, enter **5** in the **Enter Choice** field. Refer to "Configuring N+1" in the *RUCKUS IoT Controller Configuration Guide* to complete this configuration.

13. Open a web browser on your host machine and enter the IP address of the VM in the address bar.

    HTTP and HTTPS on ports 80 and 443 are supported.

    The **Initialization** page is displayed.

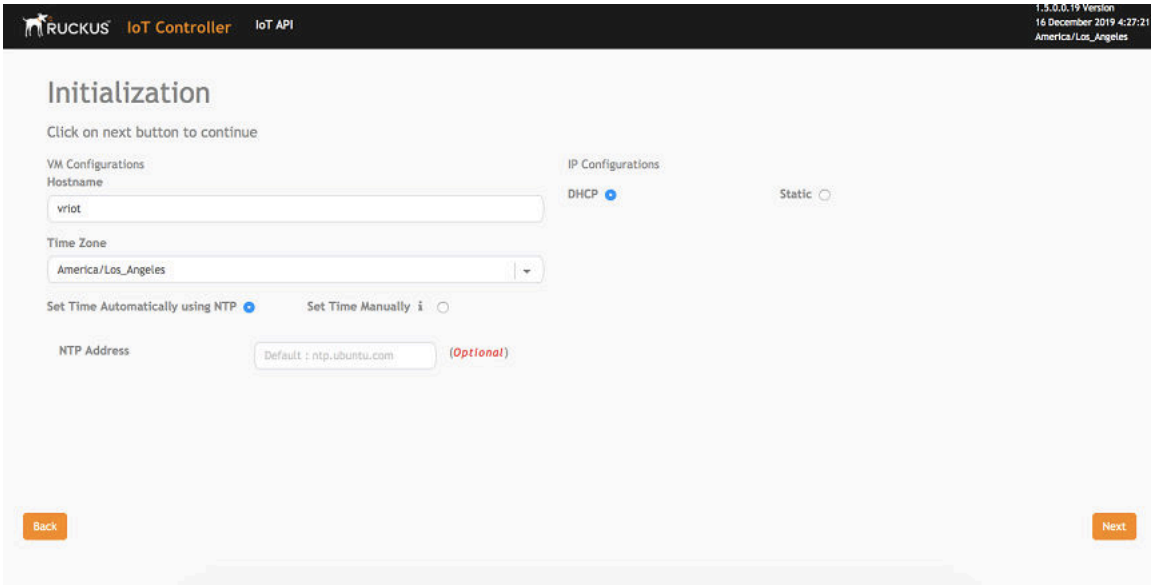
    FIGURE 48 Intialization Page



14. Select the required services and click **Next**.

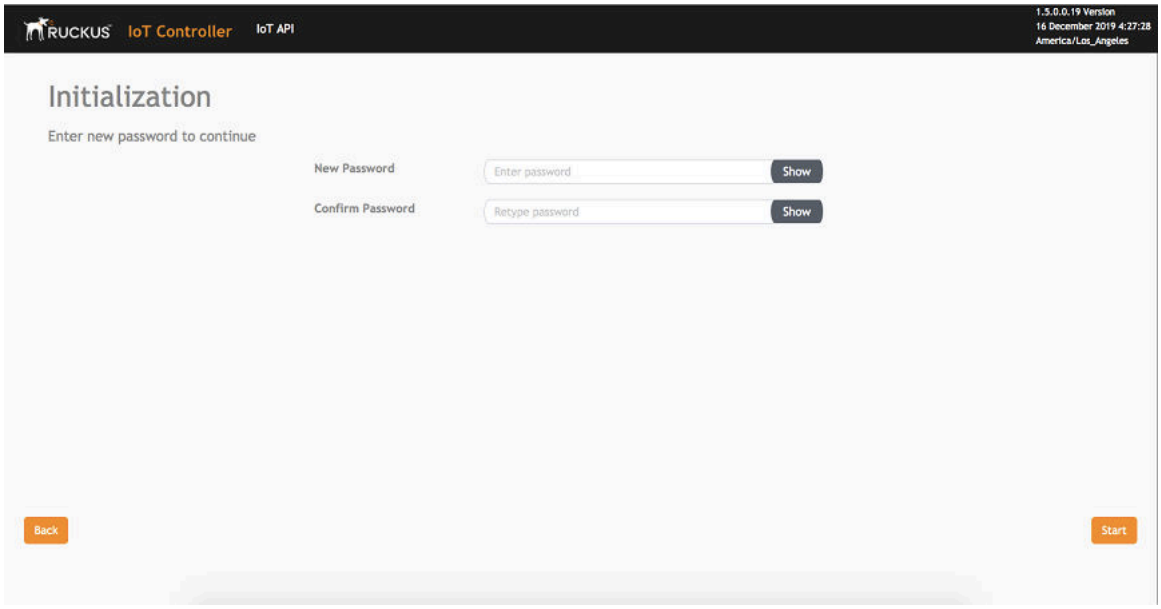
15. Confirm the configuration information and click **Next**.

FIGURE 49 Initial VM and IP Configurations



The **RUCKUS IoT ControllerInitialization** page is displayed.

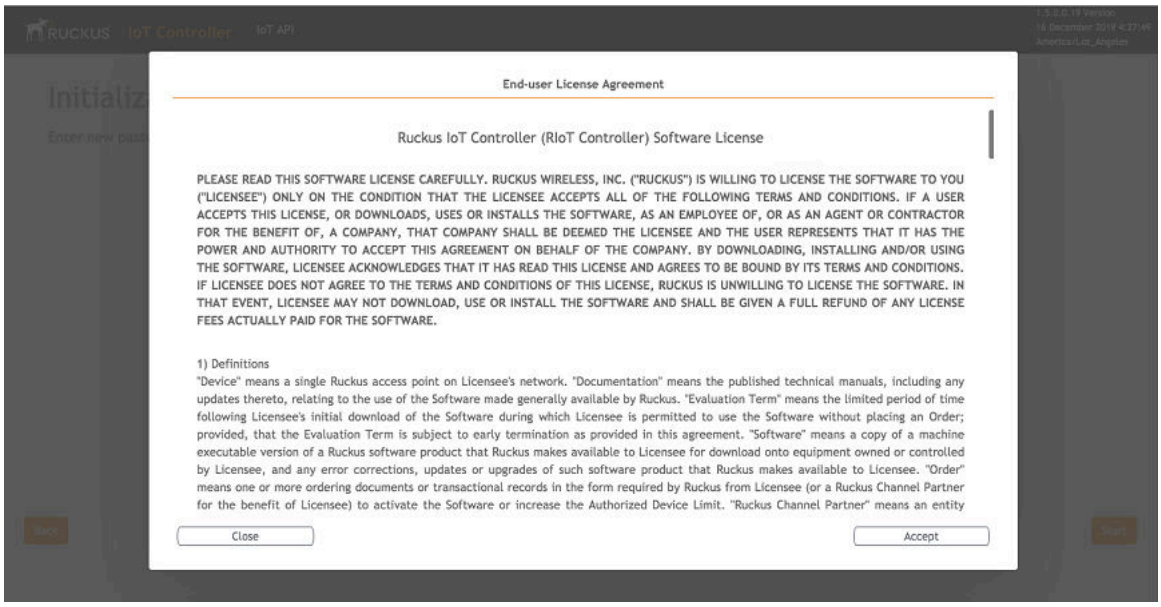
FIGURE 50 Confirming the Password



16. Enter a new password and re-enter the new password in the **Confirm Password** field. Click **Start**.

17. The **End-user License Agreement** page is displayed. Click **Accept** to accept the RUCKUS IoT Controller license.

FIGURE 51 End-user License Agreement Page



You are ready to configure and start the RUCKUS IoT Controller services. Refer to the *RUCKUS IoT Controller Configuration Guide* for more information.

Installing RUCKUS IoT Controller on AWS

- Installing AWS CLI 59
- Getting Access Key ID and Secret Access Key for Amazon S3 Account 60
- Importing VRIOT Image 60
- Creating RUCKUS IoT Controller EC2 Instance 61

Installing AWS CLI

Ensure that you have created an account with AWS and have the login details for the same.

1. Install pip by executing the below command.

```
curl-O https://bootstrap.pypa.io/get-pip.py

sudo python27 get-pip.py
```

2. Install AWS CLI using pip:

```
#pip install awscli --upgrade -user
```

3. Verify that the AWS CLI installed correctly by using the below command.

```
# aws --version
```

4. Test the installation by using the command.

```
# aws help
```

5. To set up AWS CLI you need to get your access and secret key identifier. Follow the instructions and find your identifier keys.
6. Use the following command to configure CLI :

```
# aws configure
AWS Access Key ID [None]: xxx
AWS Secret Access Key [None]: xxx
Default region name [None]: us-west-2
Default output format [None]: json
```

7. The default region should be the same as the bucket region. Refer to Table for the mapping details.In addition refer to you can also refer to latest version.

Region Name	Region
us-west-2	US West (Oregon)

Getting Access Key ID and Secret Access Key for Amazon S3 Account

To obtain the Access Key ID, and Secret Access Key for Amazon S3 account, follow the steps below.

1. In the AWS web interface, navigate to **Dashboard** > **Identity & Access Management.**

   The **Identity & Access Management** (IAM) page is displayed.
2. From the navigation menu, click **Users**.
3. Select the **IAM User Name**.
4. Click **User Actions**, and then click **Manage Access Keys**.
5. Click **Create Access Key**.

   The keys appear as **Access Key ID** example : AKIAIOSFODNN7EXAMPLE and **Secret Access Key** example: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
6. Click **Download Credentials**, and store the keys in a secure location.

Importing VRIOT Image

Follow the below steps to import VRIOT image into Amazon Web Service (AWS) shared AMI.

1. Create a JSON file called import.json using the following commands. Replace the bucket name with the storage bucket name that you created.

   In this example the VRIOT image file name is seen as vriot-1.6.0.0.16.ova.

   ```
   {
       "Description": "Import vriot",
       "DiskContainers": [
           {
               "Description": "vriot-1.6.0.0.16",
               "UserBucket":{
                 "S3Bucket":"vriot",
                 "S3Key": "qa-1.6.0.0/1.6.0.0.16/vriot-1.6.0.0.16.ova"
   }
   } ]
   }
   ```

   S3 Bucket info can be fetched with following command
2. To access the details of S3 bucket,enter the below command.

   ```
   aws s3api list-buckets --query "Buckets[].Name"
   ```

3. Execute the following command to attach the policy to the role created.

   ```
   # aws ec2 import-image --cli-input-json file://import.json
   ```

4. The system displays the below response.


```
{
    "Description": "Import vriot",
    "ImportTaskId": "import-ami-0f662ebae1a3c5ed4",
    "Progress": "2",
    "SnapshotDetails": [
        {
            "DiskImageSize": 0.0,
            "UserBucket": {
                "S3Bucket": "vriot",
                "S3Key": "qa-1.6.0.0/1.6.0.0.16/vriot-1.6.0.0.16.ova"
            }
        }
    ],
    "Status": "active",
    "StatusMessage": "pending"
}
```


5. Verify the status of the imported VRIOT image by executing the below command. Ensure to enter the correct import task identifier.

```
.# aws ec2 describe-import-image-tasks --import-task-ids "import-ami-0f662ebae1a3c5ed4"
```

6. Observe the below converting status response. Check the status until the converting is complete. The estimated time for conversion is 30 minutes.


```
{
    "ImportImageTasks": [
        {
            "Architecture": "x86_64",
            "Description": "Import vriot",
            "ImportTaskId": "import-ami-0f662ebae1a3c5ed4",
            "LicenseType": "BYOL",
            "Platform": "Linux",
            "Progress": "39",
            "SnapshotDetails": [
                {
                    "DeviceName": "/dev/sda1",
                    "DiskImageSize": 2428570624.0,
                    "Format": "VMDK",
                    "Status": "completed",
                    "UserBucket": {
                        "S3Bucket": "vriot",
                        "S3Key": "qa-1.6.0.0/1.6.0.0.16/vriot-1.6.0.0.16.ova"
                    }
                }
            ],
            "Status": "active",
            "StatusMessage": "booting",
            "Tags": []
        }
    ]
}
```

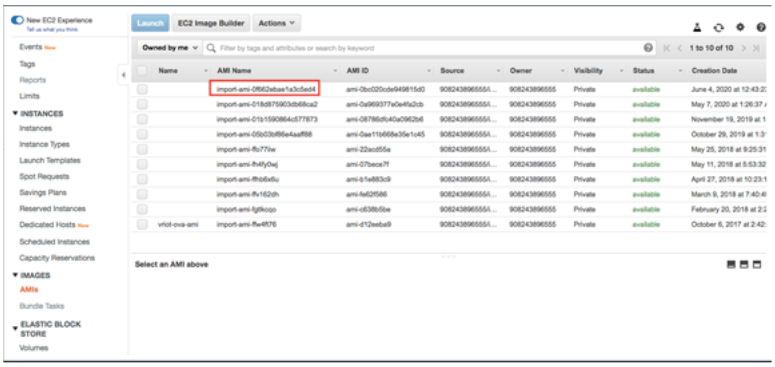

Creating RUCKUS IoT Controller EC2 Instance

To create a RUCKUS IoT Controller instance on Amazon Web Service (AWS), follow the below steps.

1. From Amazon Web Service, click **Compute** > **EC2**

2. Navigate to **Images** > **AMIs** to ensure that the imported Amazon Machine Image (AMI) exists.

FIGURE 52 Creating EC2 Instance



3. Navigate to **Network & Security** > **Security Groups** > **Create Security Group.**

   The Security group acts as a virtual firewall that controls the traffic for one or more instances.

4. Define the **Setup group name**, **Description**, **Ports** and the **Firewall rule**.

   The table lists the common service ports.

5. Navigate to **Instances** and click on **Launch Instances**.

Upgrading the Software

- Upgrading the AP Firmware Using SmartZone 100 or Virtual SmartZone Controller....63
- Upgrading the RUCKUS IoT Controller....67
- Upgrading the RUCKUS IoT Controller with N+1 Configuration.... 68

Upgrading the AP Firmware Using SmartZone 100 or Virtual SmartZone Controller

You can upgrade the existing AP firmware using a SmartZone 100 controller or Virtual SmartZone.

Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process has completed successfully. If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server.

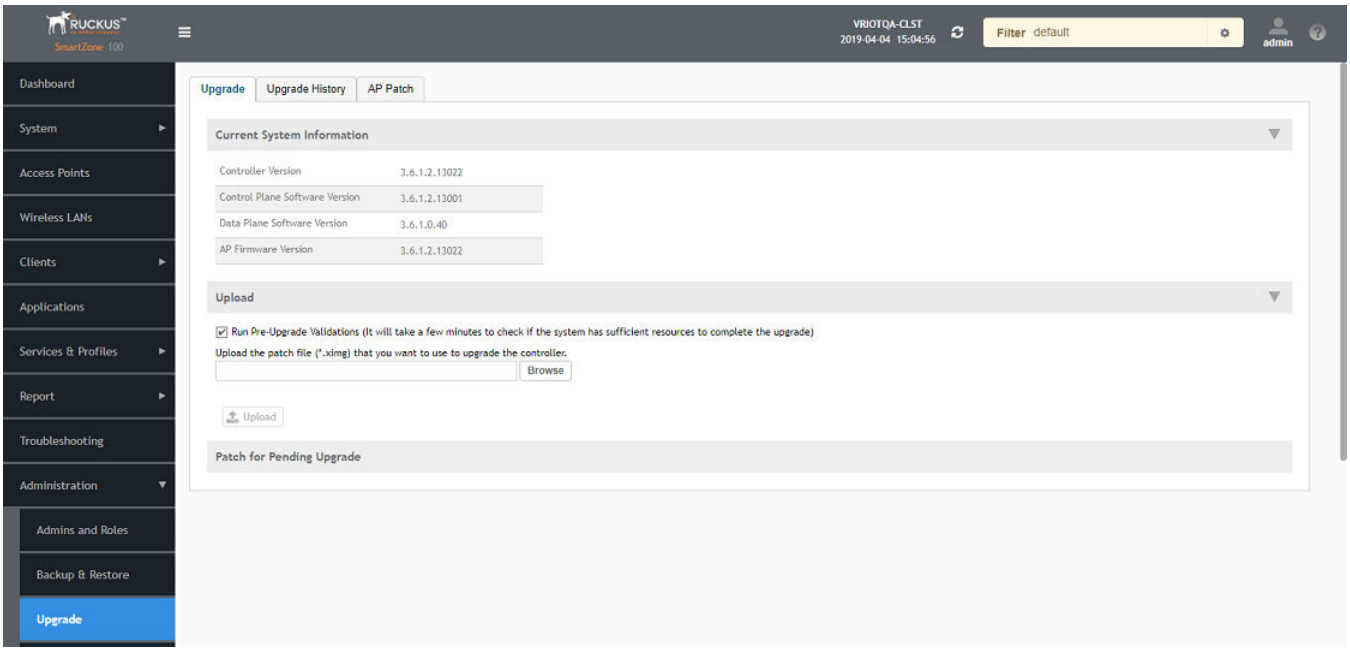
NOTE
RUCKUS strongly recommends backing up the SmartZone 100 controller cluster before performing an upgrade. If the upgrade process fails for any reason, you can use the latest backup file to restore the controller cluster.

NOTE
Before beginning the upgrade, you must obtain a valid controller software upgrade file from RUCKUS Support or an authorized RUCKUS reseller.

1. Copy the software upgrade file that you received from RUCKUS to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.

2. From the SmartZone 100 user interface, click **Administration** > **Upgrade**.

FIGURE 53 SmartZone 100 User Interface



3. Select the **Upgrade** tab.

   Under **Current System Information**, the controller version information is displayed.

   NOTE
   The **Upgrade History** tab displays information about previous cluster upgrades.

4. Under **Upload**, select **Run Pre-Upgrade Validations** to verify if the data migration was successful. This option allows you to verify data migration errors before performing the upgrade.

   NOTE
   You can still upgrade even if there are data migration errors.

5. Click **Browse** to select the .ximg patch file.
6. Click **Upload** to upload the controller configuration to the configuration in the patch file.

   The controller uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file. If data migration was unsuccessful, the following error is displayed:

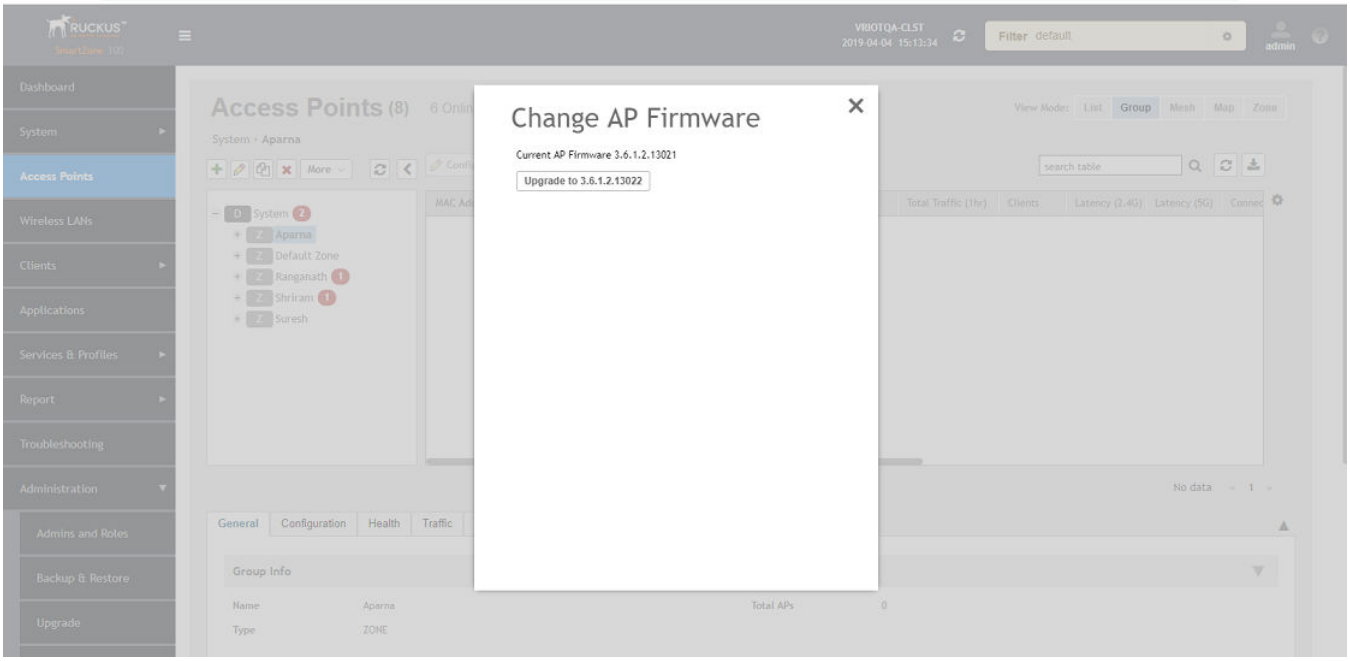
   ```
   Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.
   ```

7. If the controller configuration upload was successful, perform one of the following steps:
   - Click **Upgrade** to start the upgrade process without backing up the current controller cluster or its system configuration.
   - Click **Backup & Upgrade** to back up the controller cluster and system configuration before performing the upgrade.

   When the upgrade (or backup-and-upgrade) process is complete, the controller logs you out of the web interface automatically. When the controller login page displays again, you have completed upgrading the controller.

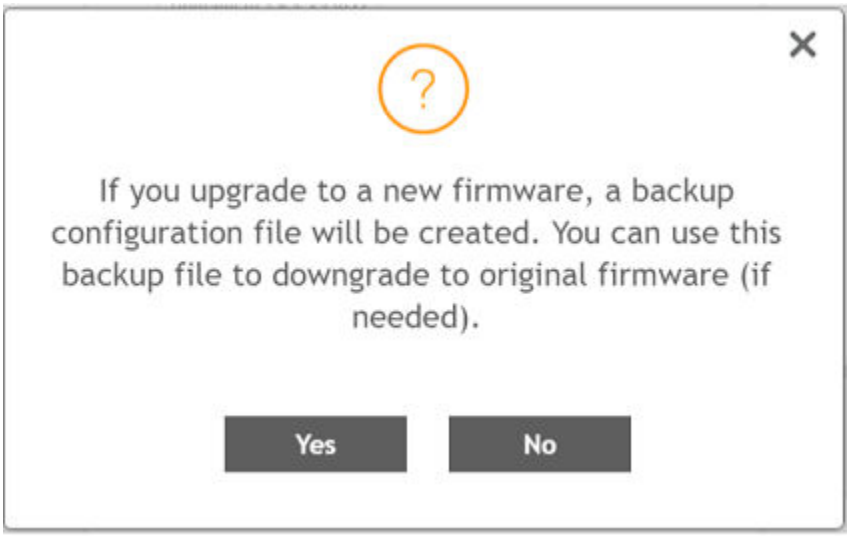
8. From the Smartzone 100 user interface, click **Access Points**.
9. Select the zone from the list, click **More**, and select **Change AP Firmware** from the list. The **Change AP Firmware** dialog box is displayed. The current AP firmware version is displayed.

FIGURE 54 Changing the AP Firmware



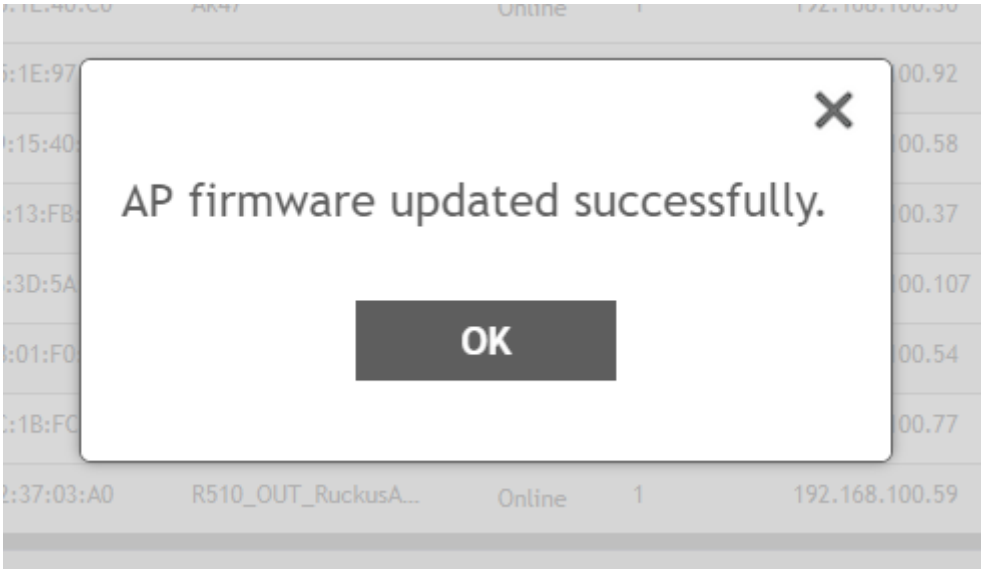
10. Click **Upgrade** to upgrade to the new firmware version.

FIGURE 55 Upgrading to New Firmware



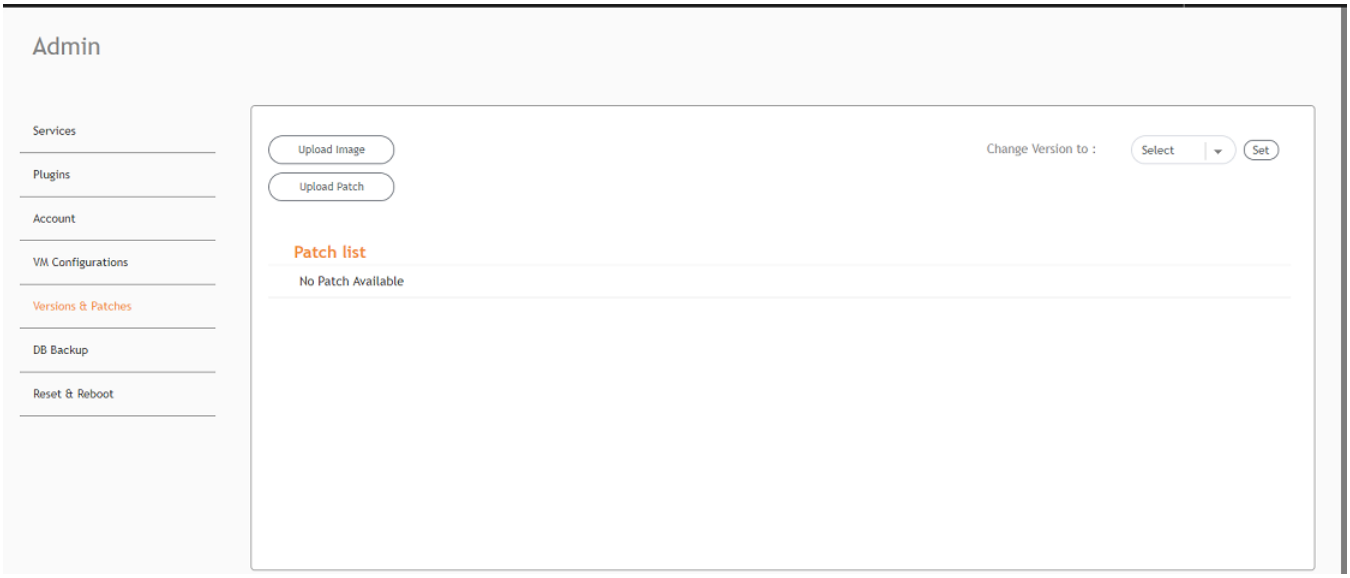
11. Click **Yes**. A confirmation message is displayed stating that the firmware version was updated successfully.

FIGURE 56 Update Successful Confirmation Message



12. Click **OK**.
13. Open the RUCKUS IoT Controller. From the **Admin** tab, click **Versions and Patches**.

FIGURE 57 Uploading an Image



14. Click **Upload Image** and select the tar.gz image.
15. From the **Change Version to** list, select the image, and click **Set**.

The RUCKUS IoT Controller is upgraded successfully to the new build.

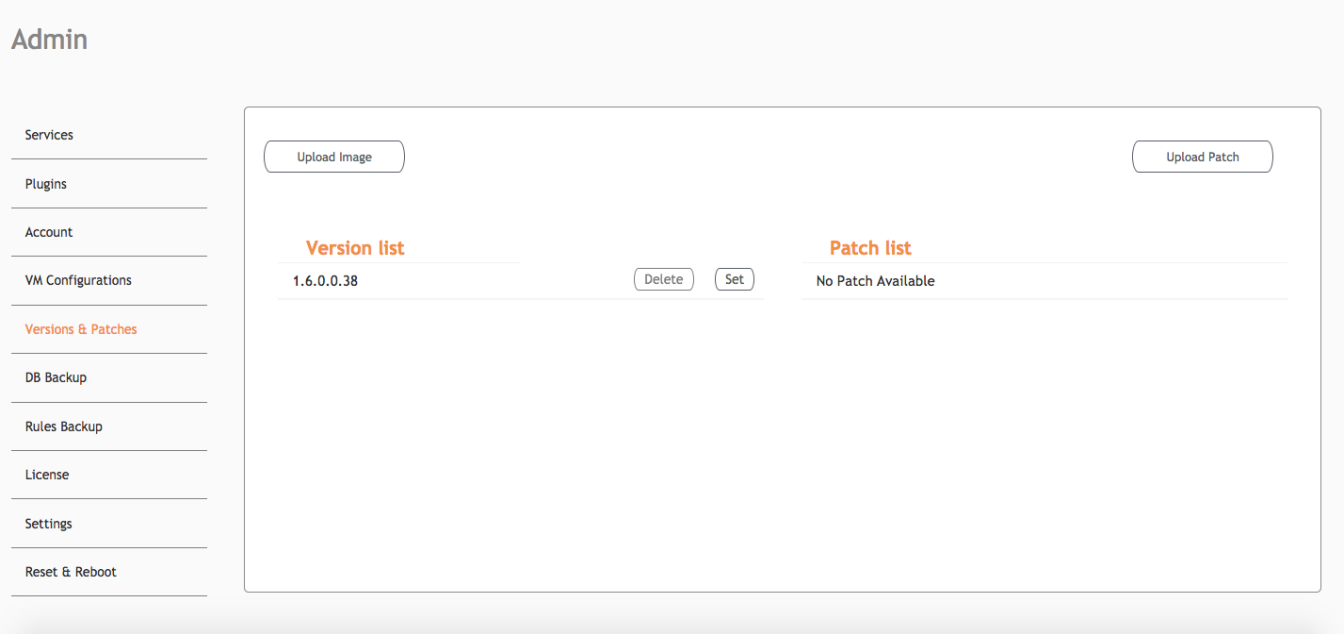
Upgrading the RUCKUS IoT Controller

Previous versions of RUCKUS IoT Controller supported a hard disk size of 8 GB. To use the latest version of the controller, the hard disk size must be increased from 8 GB to 20 GB Fixed. After the hard disk size is increased, you can upgrade the RUCKUS IoT Controller software.

Complete the following steps to upgrade the RUCKUS IoT Controller software.

1. From the main menu, click **Admin** .

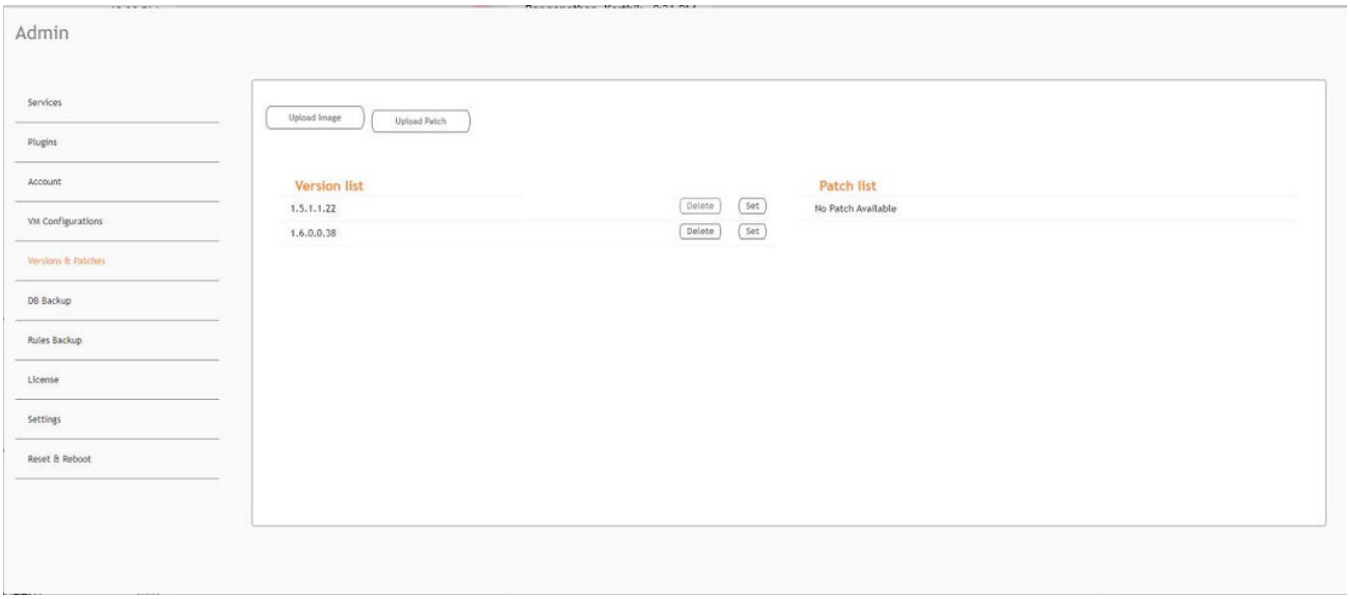
   FIGURE 58 Upgrading RUCKUS IoT Controller



2. In the left navigation pane, click **Versions & Patches**.

3. Click **Upload image** to upgrade to the next version of release as shown below.

FIGURE 59 Uploading the latest build



4. Select the latest version (1.6.0.0.38) from the **Version list** and click **Set**.
5. After the controller is upgraded with the newer version, it will automatically logout.
6. Login back to the controller.

NOTE
Support for downgrade is not provided. Downgrade from 1.6.0.0 to a lower version is not supported.

Upgrading the RUCKUS IoT Controller with N+1 Configuration

To upgrade the primary and secondary RUCKUS IoT Controller with N+1 Configuration, perform the following steps.

1. Upgrade the SmartZone to the supported version.

NOTE
Refer to Upgrading the AP Firmware Using SmartZone 100 or Virtual SmartZone Controller on page 63 for more information.

2. Disable the N+1 configuration if previously configured.

NOTE
Refer to "Disabling the N+1 Feature" in the RUCKUS IoT Controller Configuration Guide.

3. Upgrade AP Firmware using SmartZone 100 or Virtual SmartZone Controller.

   NOTE
   Refer to Upgrading the AP Firmware Using SmartZone 100 or Virtual SmartZone Controller on page 63 for more information.

4. Upgrade the RUCKUS IoT Controller software.

   NOTE
   Refer to Upgrading the RUCKUS IoT Controller on page 67 for more information.

5. Upload the licenses to the controllers.

   Refer to Activating a License on page 75 for more information.

6. Re-configure the N+1 feature.

   Refer to "Configuring the N+1 feature" in the RUCKUS IoT Controller Configuration Guide for more information.

Hot Upgrade of IoT Gateway

The Hot Upgrade of IoT Gateway supports offline upgrade of AP IoT Bundle from IoT Controller. If the controller is running in a current IoT image, then the system makes sure the APs IoT version is upgraded/downgraded to the current system image. If there is any IoT version mismatch in the AP and controller, then a warning message is displayed in the IoT AP page.

The offline upgrade for an AP is observed under the following scenario.

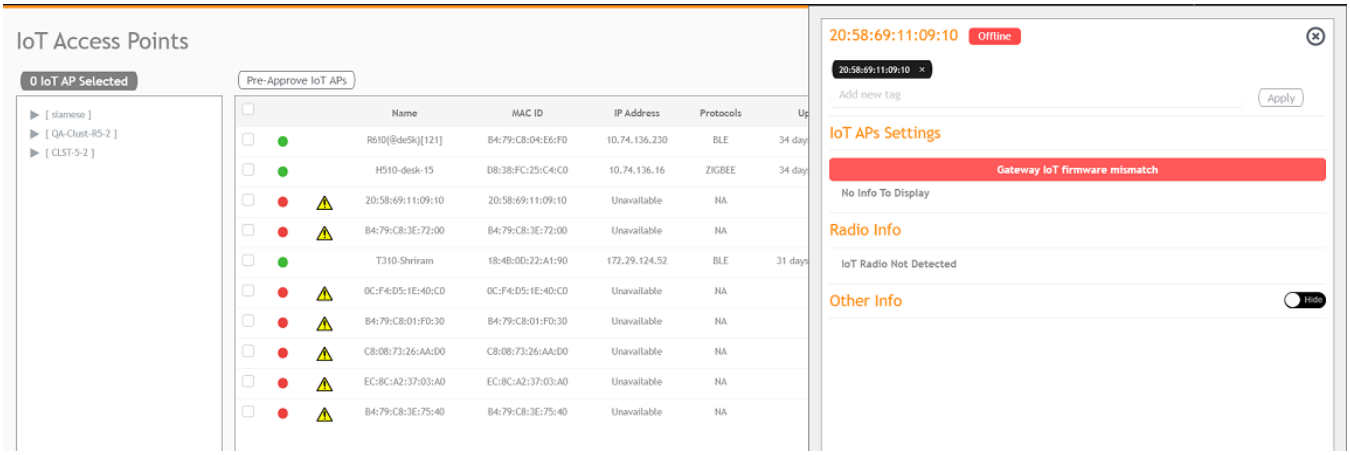
1. From the main menu, click **IoT APs** tab.

   The **IoT Access Points** page is displayed.

2. Click an IoT AP.

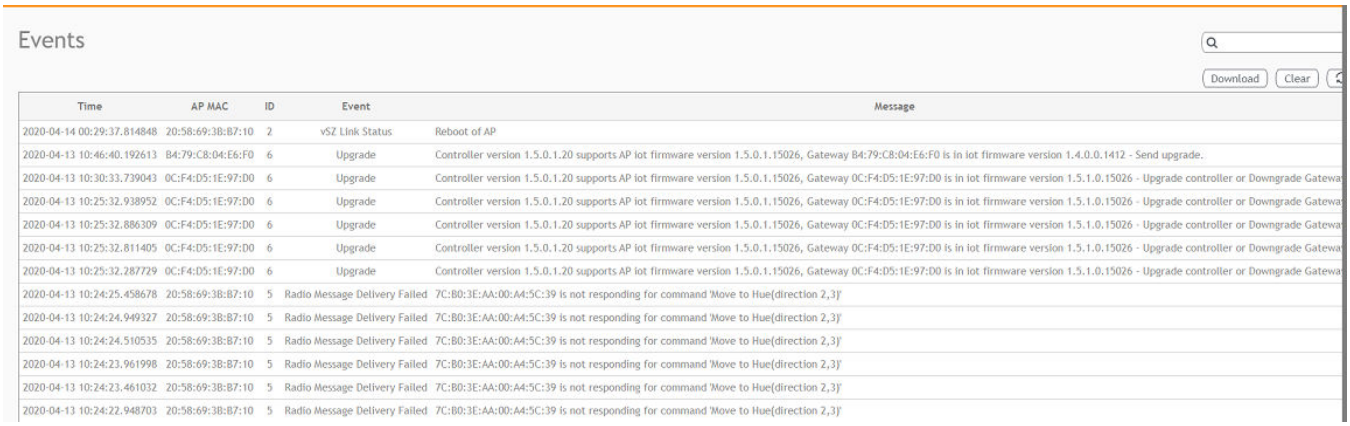
   NOTE
   If there is any mismatch in the IoT version of AP and controller then the following warning message is displayed, " Gateway IoT firmare mismatch".

FIGURE 60 Viewing IoT APs



3. To know more about the warning, click **Events** tab.

FIGURE 61 Displaying Events



Deploying the APs

- Connecting a Set of IoT APs Using Grouping Method..... 73

Connecting a Set of IoT APs Using Grouping Method

There are two methods to determine the set of IoT APs to connect with the IoT Controller.

1. Isolate the IoT APs and non-IoT APs at Layer 2 (VLAN) or Layer3 (IP) subnets. In this case, DHCP Option 43 Sub-Option 21 can be configured for networks with APs meant to connect with a particular IoT Controller. Syntax of Sub-Option 21 is the same as with Sub-Option 6 for WiFi Controller.
2. If network topology cannot be used for grouping, e.g., as a result of customer's network topology policies, the second method to use is static configuration method:
   - Disable IOT process on all APs.
   - Enable IoT process only on IoT Enabled APs.
   - Set their IoT Controller IP address

This can be done through vSZ AP CLI Script. For example, in vSZ we create a zone for the group of IoT enabled APs which we need to connect with a particular IoT Controller. Then we apply a vSZ AP CLI script to that zone which enables IoT (set iotg-enable 1) and sets the IoT Controller IP address with the AP CLI command (set iotg-mqtt-brokerip <IP>).

Managing a License

- Activating a License..... 75

Activating a License

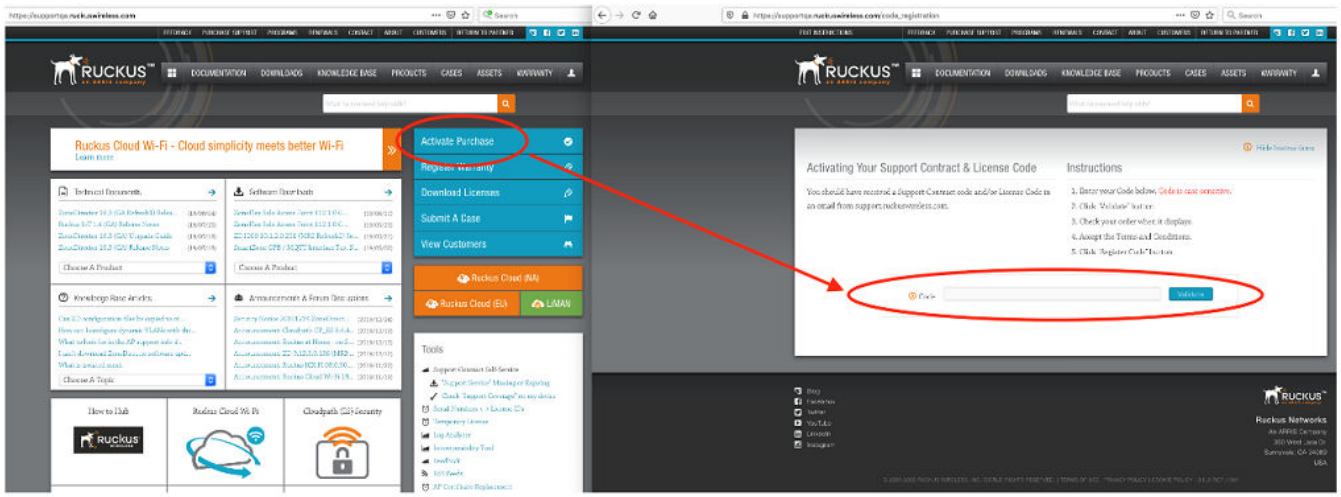
RUCKUS IoT Controller is a licensed product. After purchasing RUCKUS IoT Controller, an email message is sent to you containing an activation code. Clicking the activation code directs you to the RUCKUS Support website. After the code is validated and attached to a device (the IoT Controller serial number), the license can be downloaded from the website.

Complete the following steps to activate the license.

NOTE
In the N+1 setup ensure that individual licenses are installed on both primary and secondary respectively.

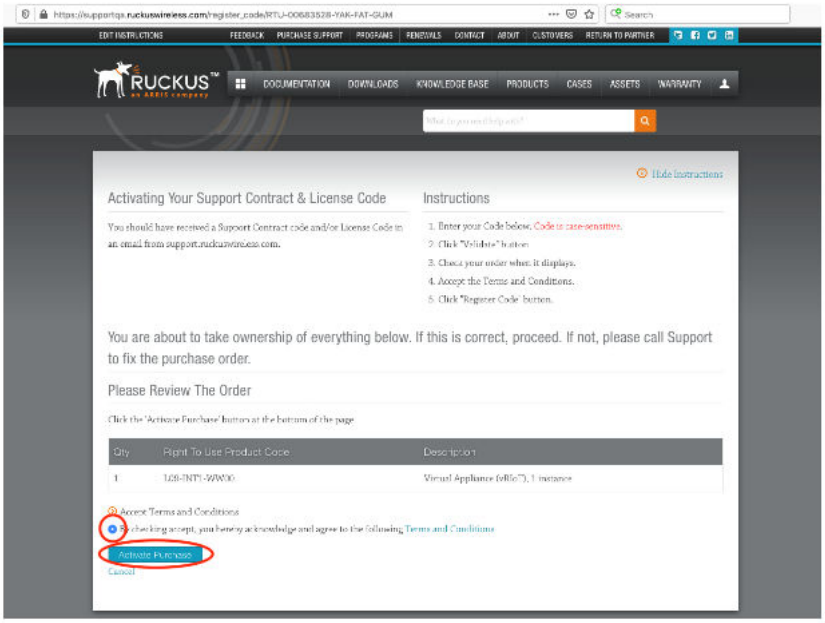
1. Click the activation code in the activation email message. You are redirected to the Ruckus Support website support.ruckuswireless.com. Log in to the website using your credentials.
2. Click **Activate Purchase**. The **Activating Your Support Contact & License Code** page is displayed. In the **Code** field, enter your activation code, and click **Validate**.

FIGURE 62 Validating the License Code



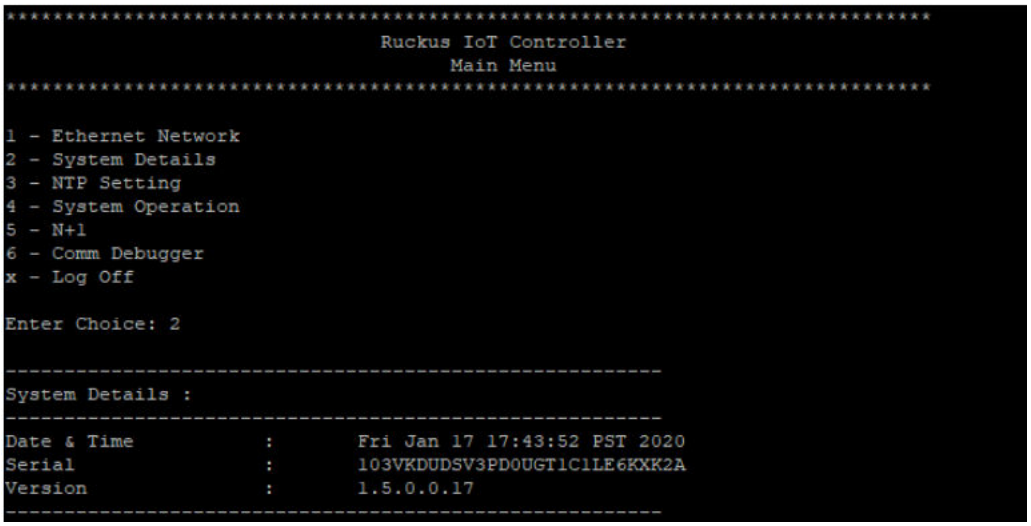
3. After the successful validation of the license code, accept the Terms and Conditions, and click **Activate Purchase**.

FIGURE 63 Activating Your Support Contract and License Code



4. Obtain the RUCKUS IoT Controller serial number in one of the two ways.
   - Obtain the RUCKUS IoT Controller serial number using the RUCKUS IoT Controller console.
     a. Log in to the console of RUCKUS IoT Controller.
     b. In the RUCKUS IoT Controller Main Menu, enter **2** in the **Enter Choice** field to get the system details.

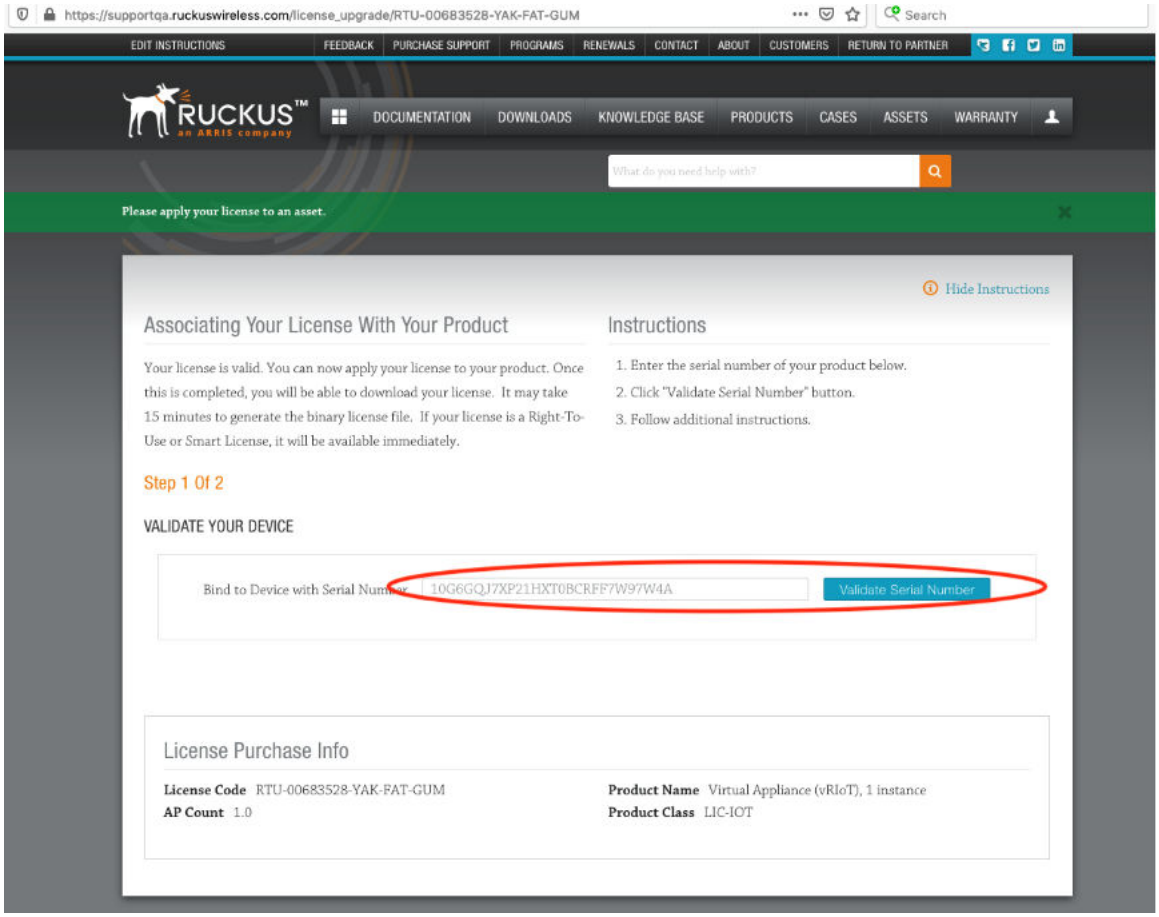
FIGURE 64 RUCKUS IoT Controller Main Menu



   - To obtain the RUCKUS IoT Controller serial number using the RUCKUS IoT Controller user interface, refer the topic " Uploading RUCKUS IoT Controller License" in the RUCKUS IoT Controller Configuration guide.

5. On the **Associating Your License With Your Product** page, enter the RUCKUS IoT Controller serial number, and click **Validate Serial Number** to activate the license.

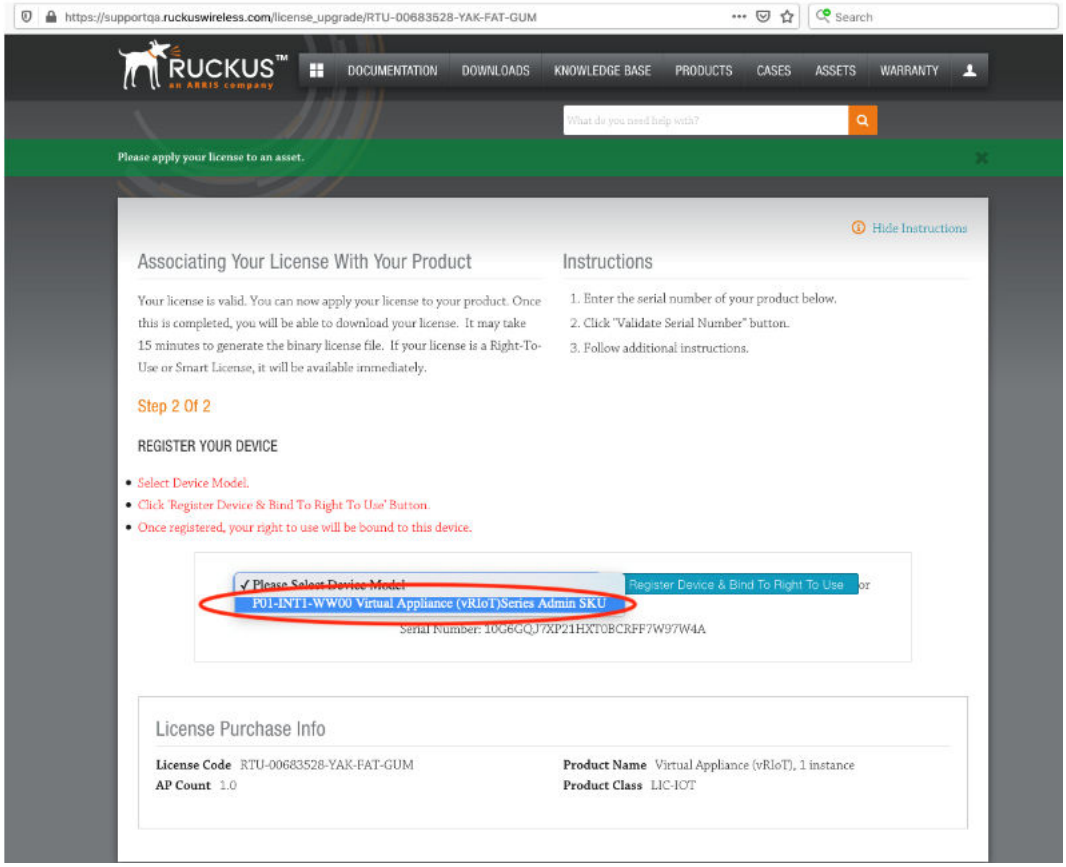
FIGURE 65 Associating the License with the Product



After successful validation, the registration page is displayed.

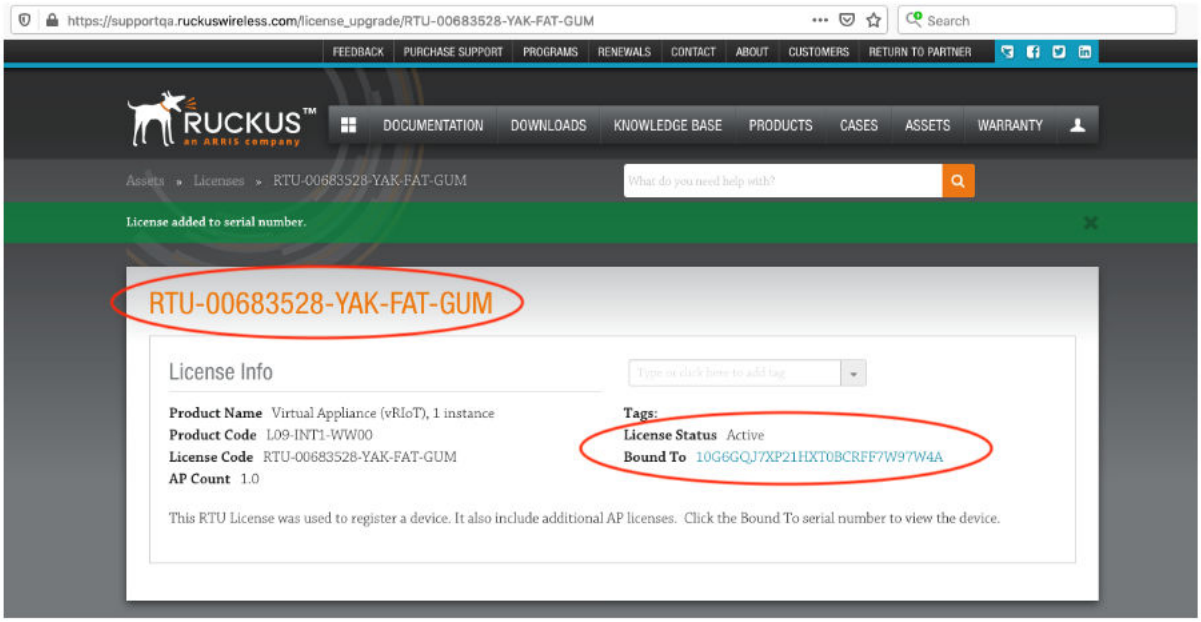
6. Select the P01-INT1-WW00 device model number and click **Register Device & Bind To Right To Use**.

FIGURE 66 Registering the Device



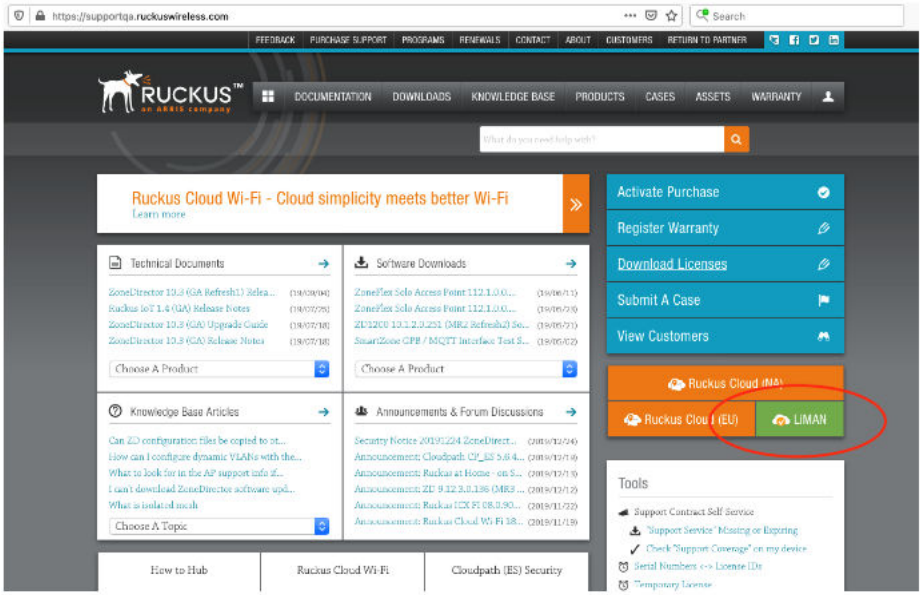
Your license information is displayed.

FIGURE 67 License Information



7. Return to the RUCKUS Support website support.ruckuswireless.com, and click **LiMAN**.

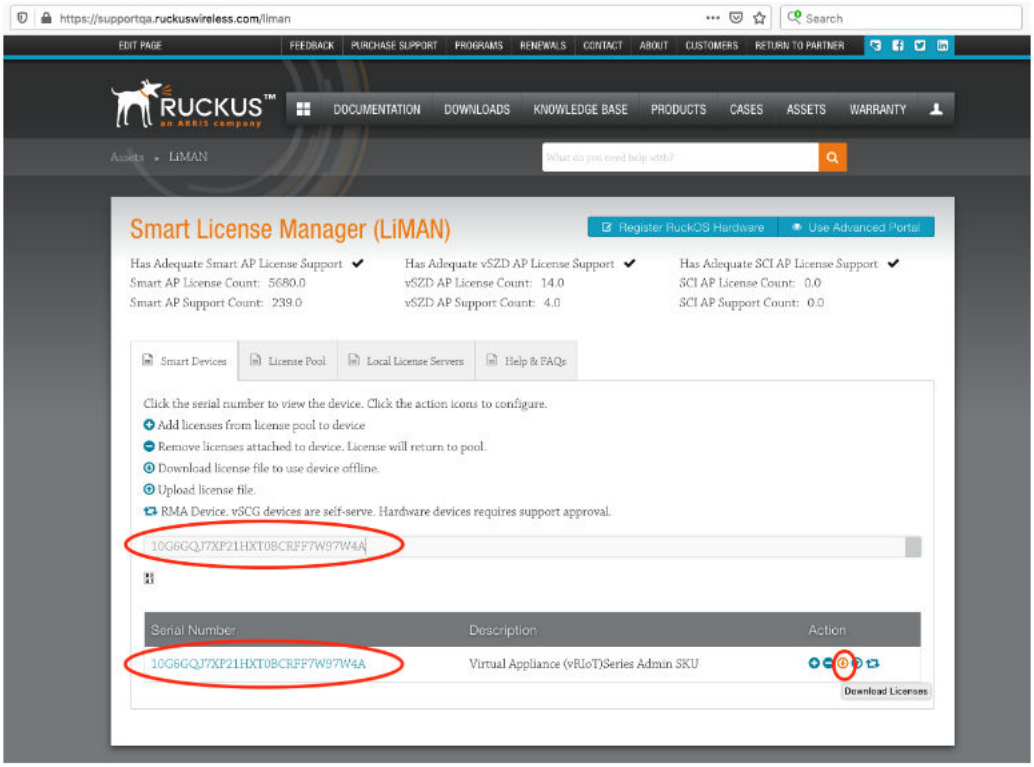
FIGURE 68 Accessing Smart License Manager (LiMAN)



8. In the **Smart License Manager** (**LiMAN**) page, enter the serial number of the controller, and click the **Download Licenses** button.

   NOTE
   The license must be uploaded to the controller.

FIGURE 69 Downloading the License



COMMSCOPE®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com