



SDN OneController Installation and User Guide

Copyright © 2015 Extreme Networks All rights reserved.

Legal Notice

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made. The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, 95134

Table of Contents

Preface.....	4
Conventions.....	4
Providing Feedback to Us.....	5
Getting Help.....	5
Related Publications.....	6
Chapter 1: OneController Overview.....	7
SDN Overview.....	7
OneController Overview.....	8
OneController Models.....	10
Chapter 2: Installing and Setting Up OneController.....	11
Installing OneController.....	11
Installing Additional Features.....	24
Reverting to the Factory Default Settings.....	29
Chapter 3: Getting Started.....	30
Logging On to the OneController GUI.....	30
Shutting Down or Rebooting OneController.....	31
Chapter 4: OneController Administration.....	33
User Accounts.....	33
Backing Up and Restoring Configurations and Logs.....	36
Upgrading OneController.....	49
Changing System Settings.....	54
Chapter 5: Networking.....	62
Viewing Network Topology.....	62
Setting Static Routes.....	63
Using OneController Interfaces.....	64
Using OpenFlow.....	64
Chapter 6: Diagnostics.....	71
OneController Reports and Logs.....	71
Network Diagnostics Overview.....	74
Creating TAC Diagnostic Files.....	77

Preface

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons





Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
<code>Screen displays</code>	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by ExtremeXOS software, which are the following:

- BlackDiamond® X series switch
- BlackDiamond 8800 series switches

- Cell Site Routers (E4G-200 and E4G-400)
- Summit® family switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the ExtremeXOS command documentation. In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines.

Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the "switch."

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at InternalInfoDev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network

- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Related Publications

Extreme SDN Documentation

- [*OneC-A-600 Quick Reference*](#)
- [*OneController Install and User Guide*](#)
- [*OneController Release Notes*](#)
- [*SDN Getting Started Guide*](#) (coming soon)

1 OneController Overview

SDN Overview
OneController Overview
OneController Models

SDN Overview

Software-defined networking (SDN) is an approach to computer networking that seeks to manage network services through decoupling the system that makes decisions about where traffic is sent (control plane) from the underlying systems that forward traffic to the selected destination (data plane).

The desire to move to the SDN model is being driven by several factors that are currently limiting conventional networking solutions from meeting today's needs:

- **Complexity:** Currently, to add or move devices, IT must touch multiple switches, routers, firewalls, Web authentication portals, etc. and update ACLs, VLANs, Quality of Services (QoS), and other protocol-based mechanisms using device-level management tools. Due to this complexity, today's networks are relatively static as IT seeks to minimize the risk of service disruption.
- **Lack of centralized orchestration:** Current networks rely on device-level management tools and manual processes. To implement a network-wide policy, IT may have to configure thousands of devices and mechanisms.
- **Inability to scale:** Conventional networks deal with increased demand by increasing physical infrastructure. As long as the increased demand is static, this solution works. However, increasingly, traffic patterns are incredibly dynamic and therefore unpredictable due to an increased mobility of users, more types of devices (smartphones, tablets), more online content, more cloud-based computing, and a more globally connected world (increased number of users).

SDN is purporting to address these issues by being dynamic, manageable, cost-effective, and adaptable, seeking to be suitable for the high-bandwidth, dynamic nature of today's applications. SDN architectures decouple network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services.

A key element of the SDN architecture is the SDN controller. With an SDN controller, network intelligence is (logically) centralized and maintains a global view of the network, which appears to applications and policy engines as a single, logical switch. Extreme Networks OneController is based on a comprehensive, hardened OpenDaylight (ODL) controller that uniquely includes: network management, network access control, and application analytics. Extreme Networks comprehensive approach preserves the integrity of the open API provided by ODL while extending data center orchestration, automation, and provisioning to the entire network under a single pane of glass.

OneController Overview

OneController leverages the OpenDaylight Helium SR1.1 version SDN Controller to provide an open, fully pluggable and scalable platform to enable SDN and NFV for networks at any size and scale. Applications can use OneController to gather network intelligence, run algorithms to perform analytics, and then use OneController to orchestrate the new rules, if any, throughout the network. Additionally, OneController is based on the modular OpenDaylight platform that allows multiple Java modules to run concurrently within the Karaf framework, and lets the modules access Java APIs exposed by other modules using the OpenDaylight Service Layer Abstraction (SAL) framework.

The OneController framework contains a collection of dynamically pluggable modules to provide network services such as:

- Host and node service
- Flow service
- Physical and overlay (flow-based) topology service
- Path service to setup and manage a path based on specified constraints such as bandwidth between a given source and destination
- Multi-tenant network virtualization service
- Network statistics service

OneController also provides the following features:

- Web-based GUI for configuring the OneController appliance
- OpenFlow modules for Lync integration (configuring only the access switches)

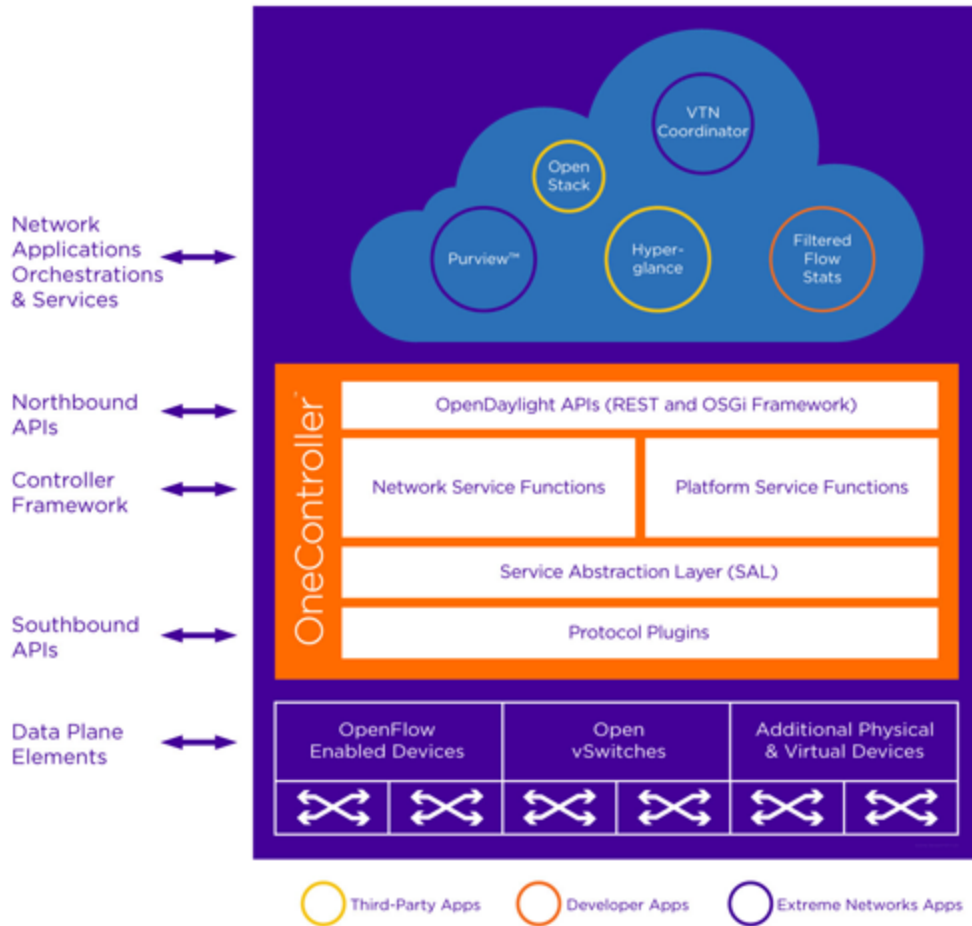


Figure 1: Extreme Networks OneController

Extreme Networks SDN platform includes management, policy, analytics, orchestration, OneController and switch level APIs.

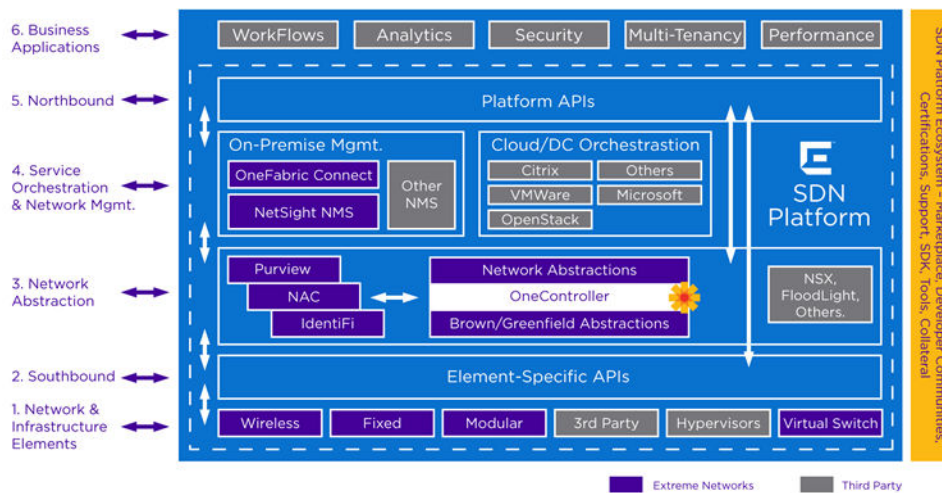


Figure 2: Extreme Networks SDN Platform

OneController Models

OneController is available in two models:

- *OneC-A-600*—physical appliance (see [OneC-A-600 Overview](#) on page 10)
- *OneC-V*—virtual appliance (see [OneC-V Overview](#) on page 10)

OneC-A-600 Overview

The *OneC-A-600* is a physical appliance with the OneController software pre-installed on it.

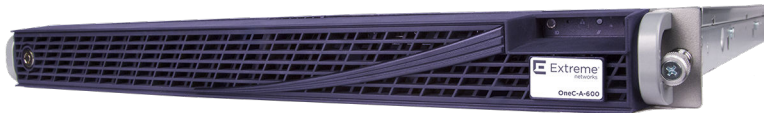


Figure 3: OneC-A-600

The OneC-A-600 features:

- MontaVista 32-bit Linux operating system
- 2 × XEON CPUs (24 cores)
- Dual 1TB hard drives with RAID controller
- 32GB RAM
- Dual power supplies
- 4 × 1G ports (ETH0 for management; ESA0, ESA1, and ESA2 are data ports)

OneC-V Overview

The *OneC-V* is a virtual appliance, deployable on your own virtualization server (see [Installing OneC-V Virtual Appliance](#) on page 13). The currently supported virtualization server software is VMware ESXi.

Minimum ESXi server specifications:

- VMware ESXi 5.5 or later
- 4 GB RAM
- Ability to offer 8 virtual cores (vCPUs) to VMs
- 100 GB virtual disk space
- One physical Ethernet NIC



Note

If the host has only one NIC, use it for the OneC-V's admin interface. OneC-V has three interfaces (Admin, ESA0, ESA1).

OneC-V supports the following main VMware tools and functionality:

- GuestInfo plugin
- Controlled startup and shutdown from ESXi
- Health monitoring (comparable to hardware watchdog functionality)

2 Installing and Setting Up OneController

Installing OneController
Installing Additional Features
Reverting to the Factory Default Settings

Installing OneController

OneController is available in two models. For information about installing OneController on:

- *OneC-A-600*—hardware appliance (see [Installing and Setting Up the OneC-A-600 Hardware Appliance](#) on page 11)
- *OneC-V*—virtual appliance (see [Installing OneC-V Virtual Appliance](#) on page 13)

Installing and Setting Up the OneC-A-600 Hardware Appliance

To install and set up the OneC-A-600:

- 1 Unpack, mount, and connect the OneC-A-600 to power (see the *OneC-A-600 Quick Reference*, shipped in the box).
- 2 Perform the initial configuration (sets network information, time/date, interfaces, log servers, and SNMP).

There are three ways to do this:

- Via serial port, and then run the command line wizard.
- Via management port using SSH, and then run the command line wizard.
- Via management port using HTTP, log on to OneController GUI, and then make change through the GUI setup wizard.

Through *serial port*:

- a Connect to the serial port with a computer (for location of serial port, see *OneC-A-600 Quick Reference*).
- b Run a terminal emulation program (for example, PuTTY).
- c Log on using: username = **admin**; password = **abc123**.

The command line configuration wizard starts automatically to guide you through the configuration.

Through *management port* using SSH:

- a Connect to the management port with a computer (for location of management port, see *OneC-A-600 Quick Reference*). Connector type = RJ45; speed/serial port parameter setting = 115200 8N1.

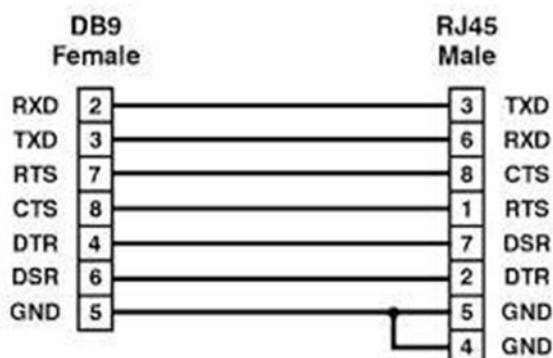


Figure 4: Serial Port Console Pinout

- b Configure the computer's Ethernet port with a statically assigned, unused IP address in the 192.168.10.0/24 subnet.
- c Connect using SSH to 192.168.10.1 (OneC-A-600's default IP address), and then log on using: username = `admin`; password = `abc123`.

The command line configuration wizard starts automatically to guide you through the configuration.

Through *management port* using HTTP:

- a Connect to the management port with a computer (for location of management port, see *OneC-A-600 Quick Reference*).
 - b Configure the computer's Ethernet port with a statically assigned, unused IP address in the 192.168.10.0/24 subnet.
 - c Log on to the OneController GUI (see [Logging On to the OneController GUI](#) on page 30) using IP address 192.168.10.1 (OneC-A-600's default IP address).
 - d Use the OneController Setup menu to configure network information, time/date, etc. (see [Changing System Settings](#) on page 54).
- 3 Upgrade the pre-installed OneController software, if needed.

To ensure that you have the latest version of the OneController software, compare the version installed on your One-Controller-A-600 hardware appliance versus the latest version available on the Extreme Networks website:

- a If you are not already connected, log on to the OneController GUI (see [Logging On to the OneController GUI](#) on page 30) using IP address 192.168.10.1 (OneC-A-600's default IP address) or the IP address that you set in step 2 on page 11.
- b Check the currently installed version of the OneController software displayed in the **Manufacturing Information** report (see [Viewing OneController Reports](#) on page 71).
- c Check the latest available version of the OneController software by going to <https://extranet.extremenetworks.com/downloads/Pages/OneController.aspx>, and then click the **Software** tab.
- d If the pre-installed software is out of date, upgrade it (see [Upgrading OneController](#) on page 49).

Installing OneC-V Virtual Appliance

The OneController software is available as a virtual appliance (OneC-V) that you can deploy on a virtualization server. The currently supported virtualization server software is VMware ESXi.

For the minimum specifications for the ESXi server, see [OneC-V Overview](#) on page 10.

To install OneC-V:

- 1 Download the OneC-V OVA file from <https://extranet.extremenetworks.com/downloads/Pages/OneController.aspx> (on the **Software** tab).
- 2 Deploy the OneC-V OVA file:
 - a From the vSphere client click **File > Deploy OVF Template**.

The **Deploy OVF Template—Source** dialog box appears (see the following figure).

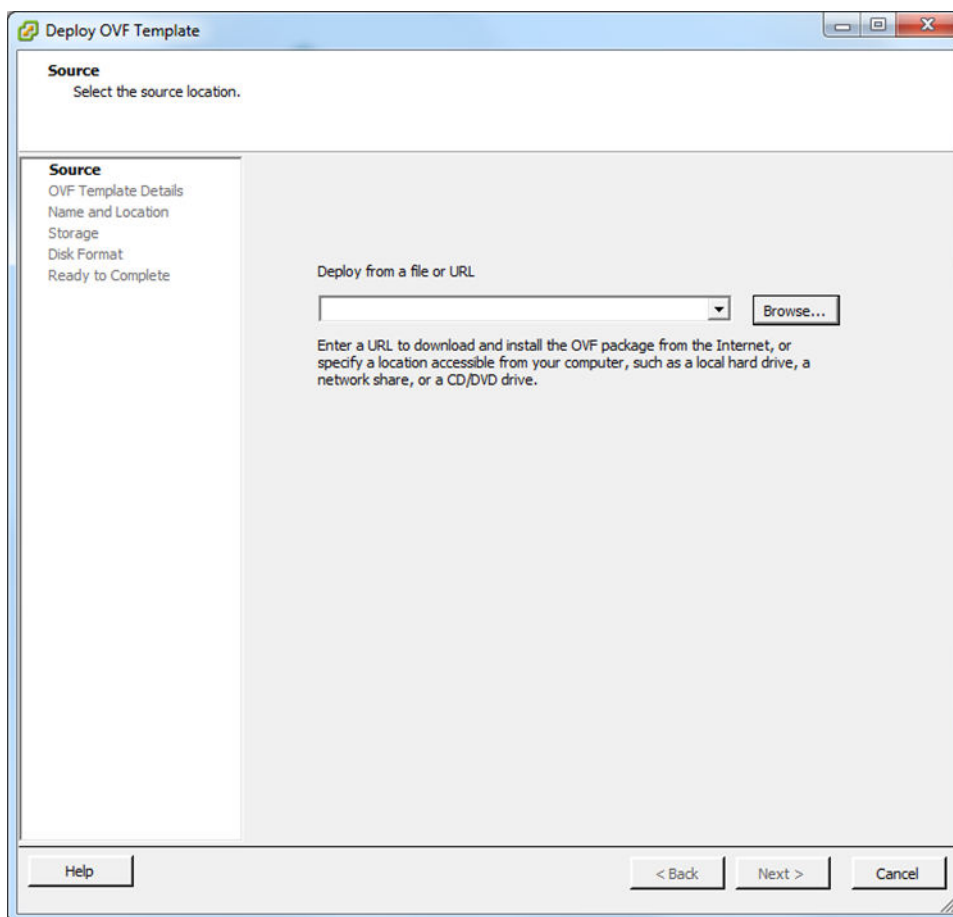


Figure 5: Deploy OVF Template: Source Dialog Box

- b Click **Browse**, go to the directory where the OneC-V OVA file resides, select the file, and then click **Open**.

- c Click **Next**.

The **Deploy OVF Template: OVF Template Details** dialog box appears (see the following figure).

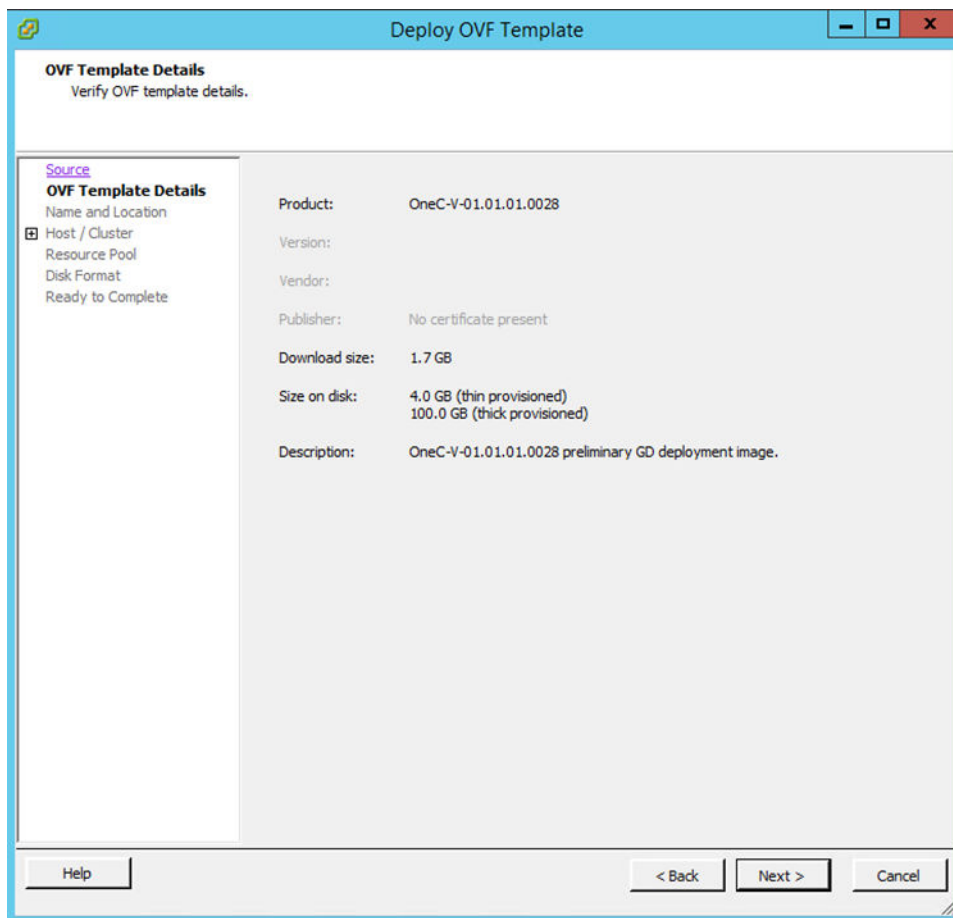


Figure 6: Deploy OVF Template: OVF Template Details Dialog Box

- d Click **Next**. The **Deploy OVF Template: Name and Location** dialog box appears (see the following figure).

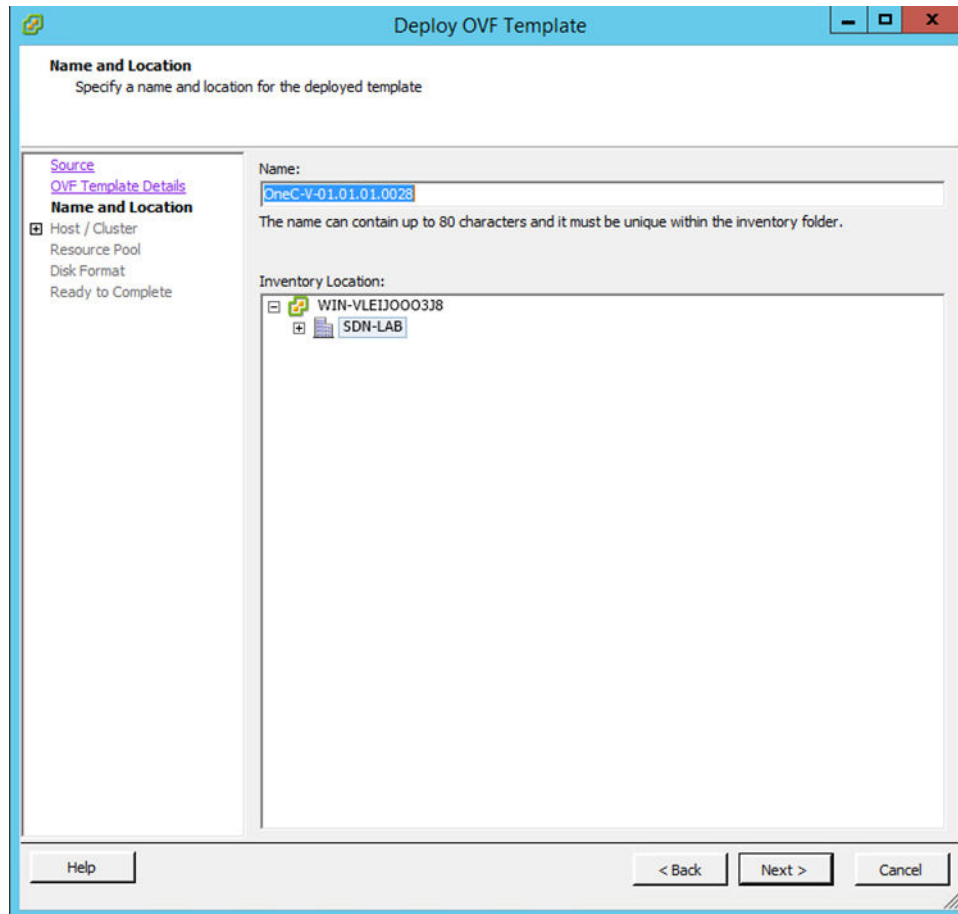


Figure 7: Deploy OVF Template: Name and Location Dialog Box

- e In the **Name** box, enter a name for the OneC-V VM, and then click **Next**.

The **Deploy OVF Template: Host / Cluster** dialog box appears (see the following figure).

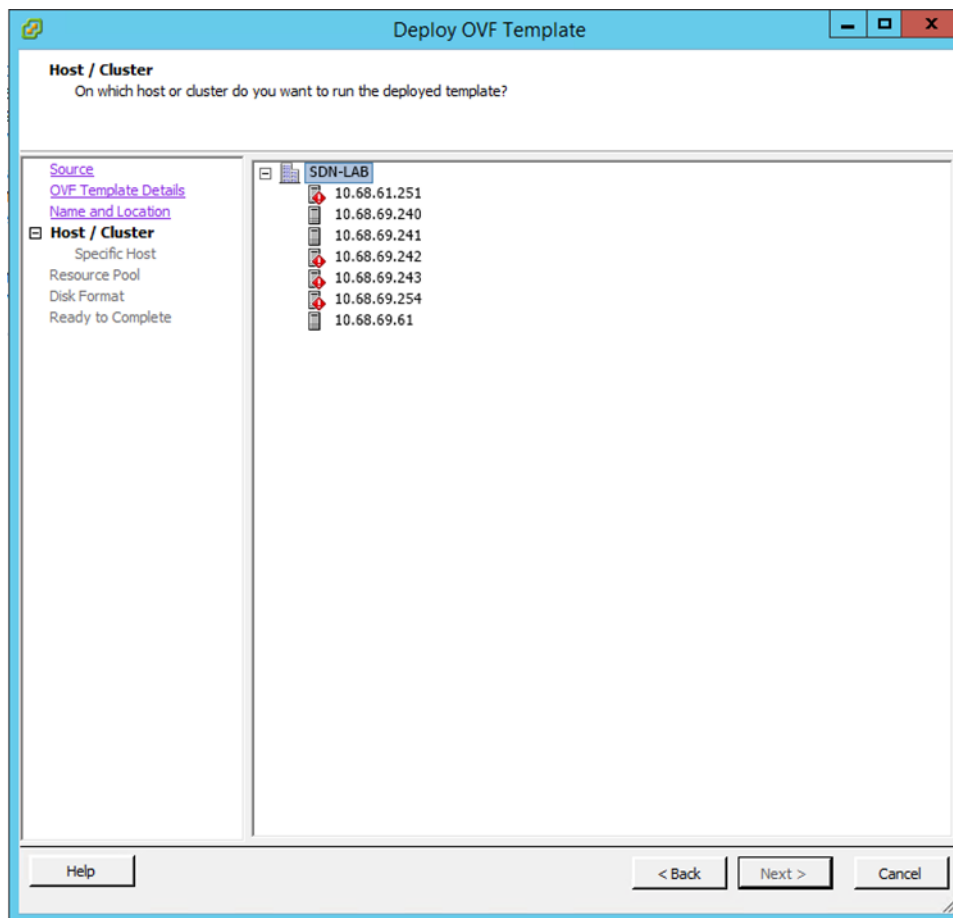


Figure 8: Deploy OVF Template: Host / Cluster Dialog Box

- f Select a host/cluster location, and then click **Next**.

The **Deploy OVF Template: Storage** dialog box appears (see the following figure).

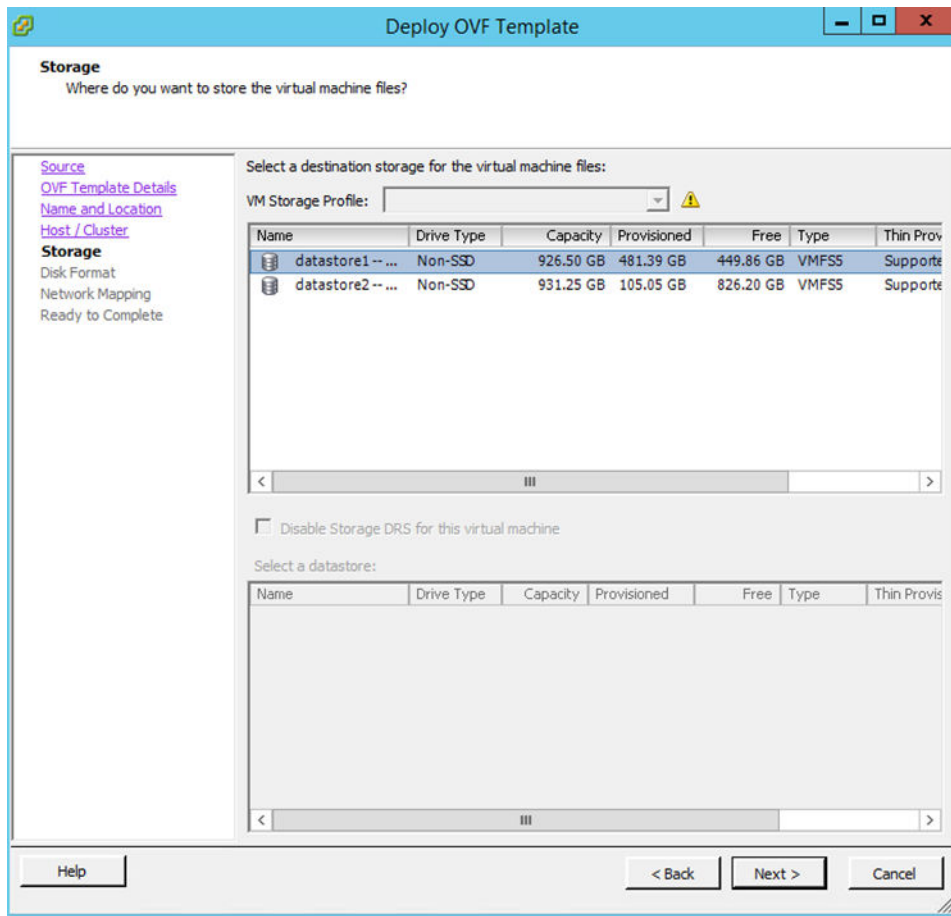


Figure 9: Deploy OVF Template: Storage Dialog Box

- g Select where to store the virtual machine files, and then click **Next**.

The **Deploy OVF Template: Disk Format** dialog box appears (see the following figure).

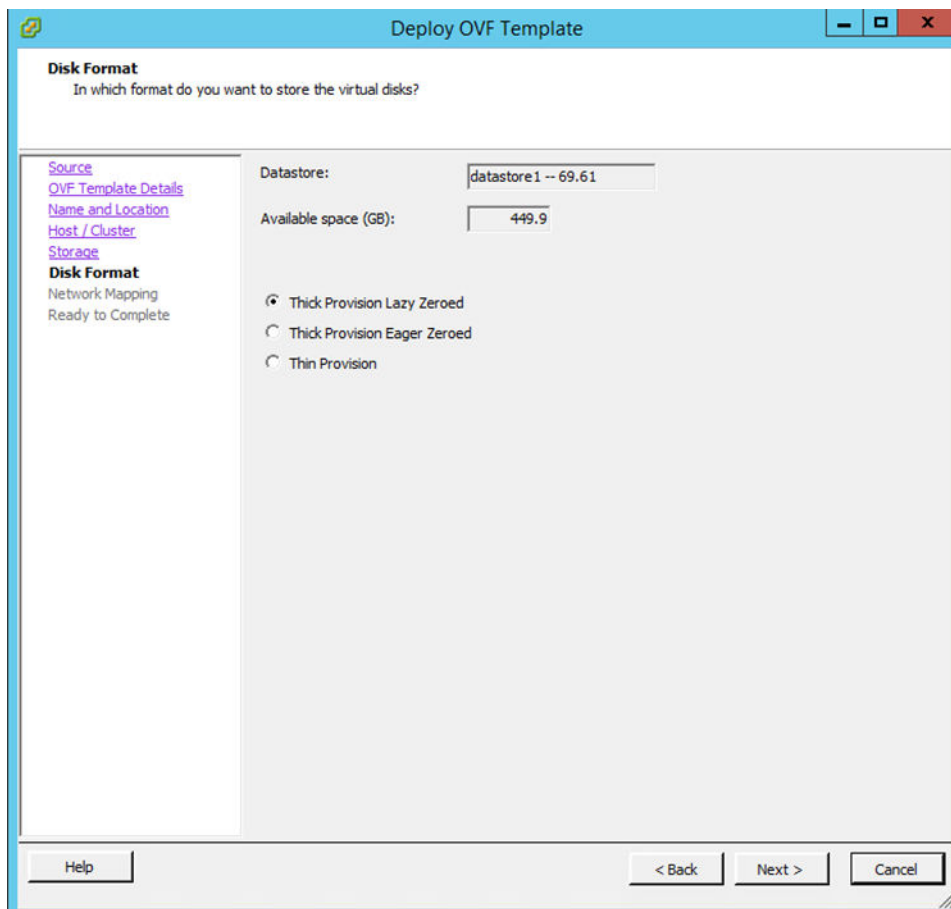


Figure 10: Deploy OVF Template: Disk Format Dialog Box

- h Accept the default settings by clicking **Next**.

The **Deploy OVF Template: Network Mapping** dialog box appears (see the following figure).

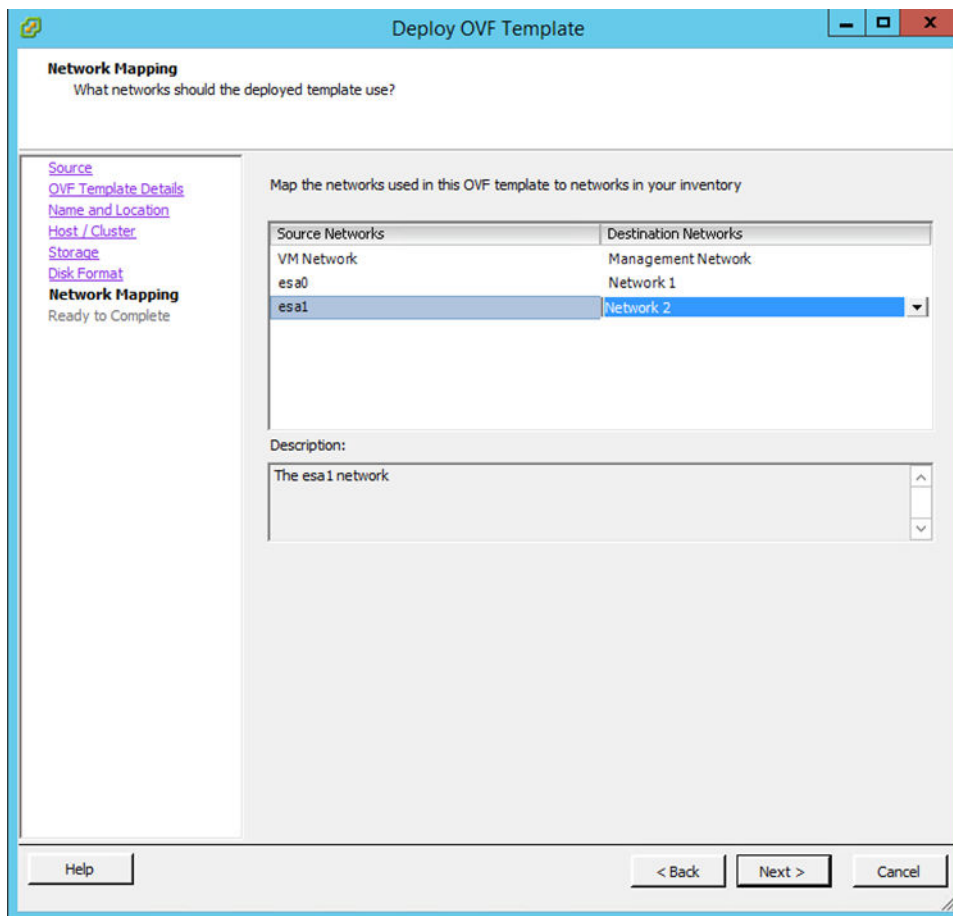


Figure 11: Deploy OVF Template: Network Mapping Dialog Box

- i Using the drop-down controls under the **Destination Networks** column, map the interfaces in the OVA file to the inventory networks:
- VM Network = Management Network
 - esa0 = Network 1
 - esa1 = Network 2

- j Click **Next**.

The **Deploy OVF Template: Ready to Complete** dialog box appears (see the following figure).

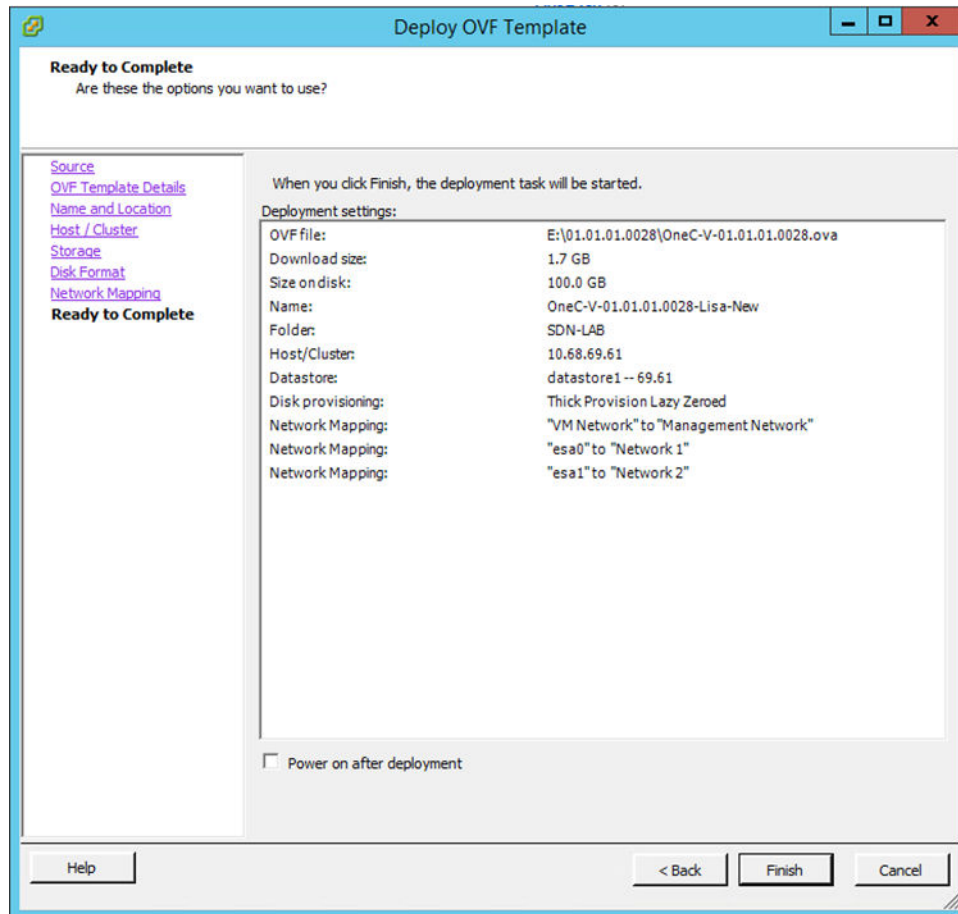


Figure 12: Deploy OVF Template: Ready to Complete Dialog Box

- k Review your selections, and then click **Finish** to complete the configuration. The import may take several minutes to complete.

- 3 Power on the OneC-V virtual machine by right-clicking it in the left pane, and then clicking **Power > Power On** (see the following figure).

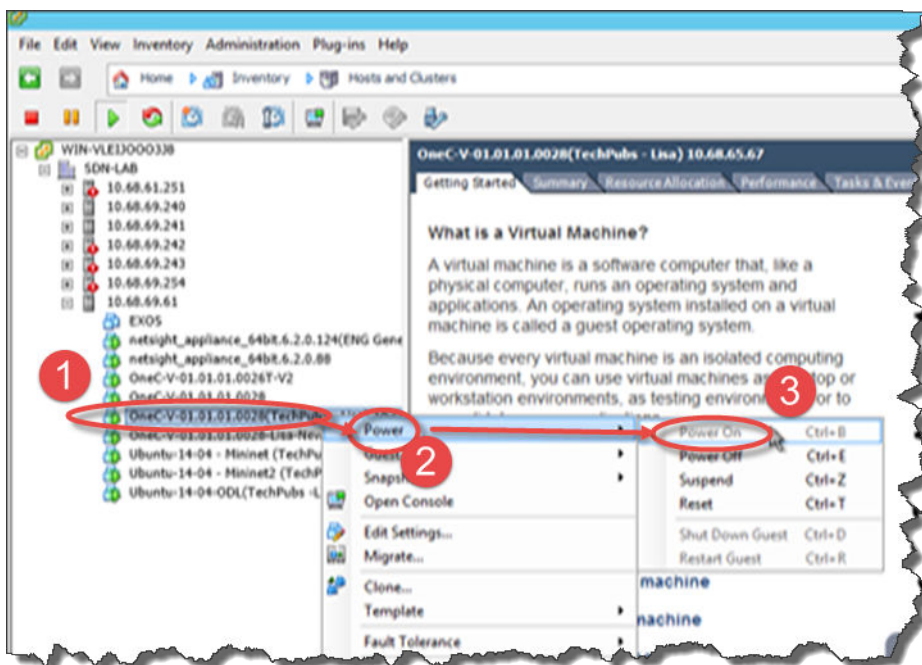


Figure 13: Powering on the OneController Virtual Machine

- 4 Configure the OneC-V system:



Note

This includes changing the Admin interface's management port IP address. Failing to change this IP address can cause IP address conflicts on the network.

- a Click the OneC-V virtual machine in the left pane, and then click the **Console** tab (see the following figure).

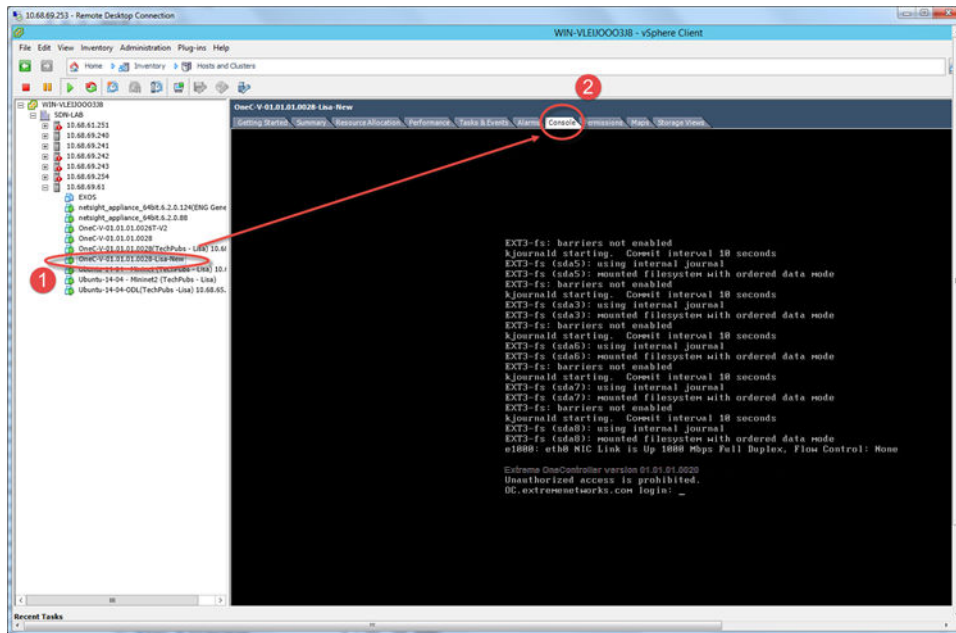


Figure 14: Console Tab

- b Wait for the logon prompt to appear, and then type the credentials username = admin and password = abc123. The configuration script starts.

5 Enter choices for the following settings (press **Enter** to accept the default setting):

Description	Values
Continent	Select the continent for time zone purposes: <ul style="list-style-type: none"> • Africa [A - J] = 0 • Africa [K - W] = 1 • America [A - A] = 2 • America [B - D] = 3 • America [E - I] = 4 • America [J - M] = 5 • America [N - R] = 6 • America [S - Y] = 7 • Antarctica = 8 • Arctic = 9 • Asia [A - G] = 10 • Asia [H - O] = 11 • Asia [P - V] = 12 • Asia [Y - Y] = 13 • Atlantic = 14 • Australia = 15 • Europe [A - L] = 16 • Europe [M - U] = 17 • Europe [V - Z] = 18 • Indian [V - Z] = 19 • Pacific [A - N] = 20 • Pacific [P - W] = 21
City	Select the city for time zone purposes.
Set Time	Set the current time in the format hh:mm (h = hours, m = minutes).
Set Date	Set the current date in the format yyyy:mm:dd (y = year, m = month, d = day).
Ntp Server	NTP server's IP address. You can designate up to three NTP servers.
Netmask	NTP server's subnet mask.
Gateway	NTP server's gateway.
Host Name	NTP server's hostname.
Domain Name	NTP server's domain name.
Static IP Address	Management port's (Admin) IP address.
Netmask	Management port's (Admin) subnet mask.
Gateway	Management port's (Admin) gateway.
Host Name	Management port's (Admin) hostname.
Domain Name	Management port's (Admin) domain name.
SNMP Mode	1 = Disable SNMP 2 = Enable SNMPv1/v2c 3 = Enable SNMPv3

Description	Values
Syslog Server	Syslog server's IP address. You can designate up to three Syslog servers.
Data Port 1	
Static IP Address	Data port's (EAS0) IP address.
Netmask	
Data Port 2	Data port's (EAS0) subnet mask.
Static IP Address	Data port's (EAS1) IP address.
Netmask	Data port's (EAS1) subnet mask.

Installing Additional Features

List of Installed and Active Features

Multiple features are installed with OneController. Several of these features are also active (functioning). You can make installed, but inactive, features active (see [Karaf Overview](#) on page 26)

The following table lists all OneController installed features, and indicates which ones are active by default (✓ in **Active** column).

Table 3: List of Installed and Active Features

Feature	Description	Active
AAA	Authentication, Authorization, and Accounting	✓
ADSAL	API Driven Service Abstraction Layer	✓
ARP Manager	Address Resolution Protocol Manager	✓
BGP	Border Gateway Protocol	
Controller	OpenDaylight Controller and its Config Plugins	✓
COPS	Common Open Policy Service	
DLUX	Web UI with Extreme Networks Platform Manager	✓
Felix	OSGi Dependency Management	✓
FRM	Forwarding Rules Manager	✓
GBP	Group-Based Policy	
Gemini Web	OSGi Web Container	✓
Host Tracker	Catalogs Hosts in the Network	✓
Jackson JAX RS	Java Data Parsing Tools	✓

Table 3: List of Installed and Active Features (continued)

Feature	Description	Active
Jersey	RESTful Web Services framework	✓
Jetty	Java Servlet Container	✓
LISP	Locator/Identifier Separation Protocol	
MDSAL	Model Driven Service Abstraction Layer	✓
MDSAL API Docs	API Explorer based on Swagger	✓
NETCONF	Network Configuration Protocol	✓
Netty Config	Netty.io Configuration API	✓
OpenFlow	OpenFlow Protocol Plugins	✓
OVSDB	Open vSwitch Database Protocol	
PCEP	Path Computation Element Communication Protocol	
Platform Manager	OneController Platform Manager API	✓
Plugin2OC	Plugin to OpenContrail	
RESTConf	REST API for accessing YANG / NETCONF	✓
SDNI	SDN Interface (Cross-Controller Federation)	
SFC	Service Function Chaining	
SLF4J Logging	Simple Logging Façade for Java	✓
SNBI	Secure Network Bootstrapping Infrastructure	
SNMP	Simple Network Management Protocol	
Spring	Spring Dependency Injection Framework	✓
Stats Manager	Send Statistics Requests to OpenFlow Nodes	✓
Switch Manager	Catalogs Capabilities of Network Elements	✓
Tomcat	Java Servlet Container	
Topology Manage	Network Topology Manager	✓
TTP	Table Type Patterns	
VTN	Virtual Tenant Network	
YANG	Tools for YANG models	✓

Feature Compatibility

The following tables lists the contents of the OpenDaylight compatible-with-all integration test.

Table 4: OpenDaylight Compatible-with-All Test Contents

odl-aaa-all	odl-openflow-nxm-extensions	odl-sfclisp
odl-aaa-authz	odl-openflowjava-protocol	odl-sfcofl2
odl-adsal-all	odl-openflowplugin-flow-services	odl-snbi-all
odl-adsal-compatibility	odl-openflowplugin-flow-service-rest	odl-ttp-all
odl-bgpcep-all	odl-openflowplugin-flow-service-ui	odl-snmp4sdn-all
odl-dlux-core	odl-ovsdb-all	odl-tcpmd5-all
odl-listflowmapping-all	odl-packetcable-all	odl-
odl-mdsal-broker	odl-sdninterfaceapp-all	odl-
odl-netconf-connector-ssh	odl-restconf	odl-
odl-nsf-all	odl-sfc-all	odl-

There are six modules that the OpenDaylight community test independently against compatible-with-all, but not against each other. The following table lists whether these modules are compatible, incompatible, or compatibility is unknown.

Table 5: Integration Test Feature Sets

	GBP	L2switch	Open Contrail	OVSDB OpenStack	OVSDB SFC	VTN Manager
Compatible-with-all	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
L2switch	Unknown	—	—	—	—	—
Open Contrail	Unknown	Unknown	—	—	—	—
OVSDB OpenStack	Unknown	Unknown	Unknown	—	—	—
OVSDB SFC	Unknown	Unknown	Unknown	Unknown	—	—
VTN Manager	Unknown	Incompatible	Unknown	Unknown	Unknown	—

Karaf Overview

OneController is a Java-based (Java 7) software package that runs within an Apache Karaf container. Karaf is a lightweight container based on OSGi that allows you to dynamically load (make active) and unload modules (called features).

A list of the main Karaf commands are listed at <http://karaf.apache.org>.

For a list of OneController features that installed and active by default, see [List of Installed and Active Features](#) on page 24.

To activate additional features:

- 1 Access the Karaf console (see [Accessing the Karaf Console](#) on page 27).
- 2 See which features are already installed and active, and which are available to activate (see [Listing Features](#) on page 27).
- 3 Activate the desired features (see [Activating Features](#) on page 28).

Accessing the Karaf Console

To access the Karaf console:

- 1 Connect to the OneController using SSH: `admin@<IP address>` (where `<IP address>` = OneController IP address) and password = `abc123`.
- 2 At the command prompt, connect to the Karaf shell using SSH by issuing the following command:
`ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no -p 8101 karaf@127.0.0.1`
- 3 When prompted, type the password `karaf`.

The following prompt appears.

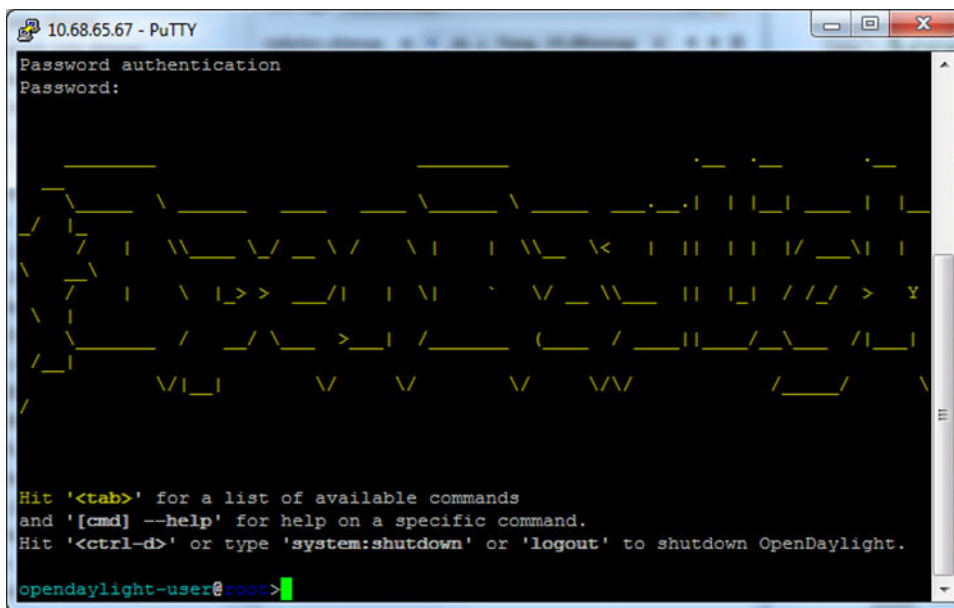


Figure 15: Karaf Prompt

Listing Features

To list features:

- To list all *installed (available) features*, issue the command: `feature:list` (see the following figure).

```

Name | Version | Installed | Repository | Description
-----|-----|-----|-----|-----
odl-netconf-all | 0.2.5-Helium | | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: All
odl-netconf-api | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: API
odl-netconf-mapping-api | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: Mapping API
odl-netconf-util | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium |
odl-netconf-impl | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: Impl
odl-config-netconf-connector | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: Connector
odl-netconf-netty-util | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: Netty Util
odl-netconf-client | 0.2.5-Helium | | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: Client
odl-netconf-monitoring | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Net
conf :: Monitoring
framework-security | 3.0.1 | | standard-3.0.1 | OSGI Security for
karaf
standard | 3.0.1 | x | standard-3.0.1 | Karaf standard feat
ure
aries-annotation | 3.0.1 | | standard-3.0.1 | Aries Annotations
    
```

Figure 16: Feature:List Command Output

- To list all *active features*, issue the command: `feature:list -i` (see the following figure).

```

Name | Version | Installed | Repository | Description
-----|-----|-----|-----|-----
odl-netconf-api | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Netconf :: API
odl-netconf-mapping-api | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Netconf :: Mapping
odl-netconf-util | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium |
odl-netconf-impl | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Netconf :: Impl
odl-config-netconf-connector | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Netconf :: Connect
or
odl-netconf-netty-util | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Netconf :: Netty U
til
odl-netconf-monitoring | 0.2.5-Helium | x | odl-netconf-0.2.5-Helium | OpenDaylight :: Netconf :: Monitor
ing
standard | 3.0.1 | x | standard-3.0.1 | Karaf standard feature
config | 3.0.1 | x | standard-3.0.1 | Provide OSGI ConfigAdmin support
    
```

Figure 17: Feature:List -i Command Output

Activating Features

To activate new features, issue the command `feature:install <feature name>` (see the following figure).

```

.opendaylight-user@root>feature:install odl-ovsdb-
odl-ovsdb-all odl-ovsdb-library odl-ovsdb-northbound odl-ovsdb-openstack
odl-ovsdb-ovsafc odl-ovsdb-plugin odl-ovsdb-schema-hardwarevtep odl-ovsdb-schema-openvswitch
.opendaylight-user@root>feature:install odl-ovsdb-
    
```

Figure 18: Feature Install Command



Note
Press **TAB** after typing the first few letters of a feature’s name to show a list of matching features.

De-activating Features

To de-activate features, issue the command `feature:uninstall <feature name>` (see the following figure).

```

.opendaylight-user@root>feature:uninstall odl-openflow
odl-openflowjava-protocol odl-openflowplugin-all odl-openflowplugin-flow-services
odl-openflowplugin-flow-services-rest odl-openflowplugin-flow-services-ui odl-openflowplugin-southbound
.opendaylight-user@root>feature:uninstall odl-openflow
    
```

Figure 19: Feature Uninstall Command

Viewing the Log

To view the log, issue the command `log:display` (see the following figure).

```

opendaylight users@>log:display
014-11-19 11:43:07,222 | INFO | Event Dispatcher | RegionsPersistenceImpl | 239 - org.apache.karaf.region.persist - 3.0.1 | Loading
region digraph persistence
014-11-19 11:43:07,293 | INFO | Event Dispatcher | RegionsPersistenceImpl | 239 - org.apache.karaf.region.persist - 3.0.1 | Initial
zing region digraph from etc/regions-config.xml
014-11-19 11:43:07,509 | INFO | Event Dispatcher | SecurityUtils | 41 - org.apache.sshd.core - 0.9.0 | BouncyCastle not re
gistered, using the default JCE provider
014-11-19 11:43:09,446 | INFO | Event Dispatcher | HttpServiceFactoryImpl | 65 - org.ops4j.pax.web.pax-web-runtime - 3.1.0 | Bindin
g Bundle: [org.opendaylight.aaa.authn-sts_0.1.0.Helium [52]] to http service
014-11-19 11:43:09,520 | INFO | Event Dispatcher | ConfigurationFactory | 85 - net.sf.ehcache - 2.8.3 | No configuration found, c
onfiguring ehcache from ehcache-failsafe.xml found in the classpath: bundleresource://85.fwk927935/ehcache-failsafe.xml
014-11-19 11:43:09,858 | INFO | Event Dispatcher | DefaultTokenStore | 93 - org.opendaylight.aaa.authn-store - 0.1.0.Helium |
initialized token store with default cache config

```

Figure 20: Log:Display Command

Reverting to the Factory Default Settings

At any time after installation, you can revert to the factory default settings established by the installation. This action does not remove any OneController software upgrades (see [Upgrading OneController](#) on page 49) and does not change the management port address, so that you do not lose connectivity.

To revert to the factory default settings:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

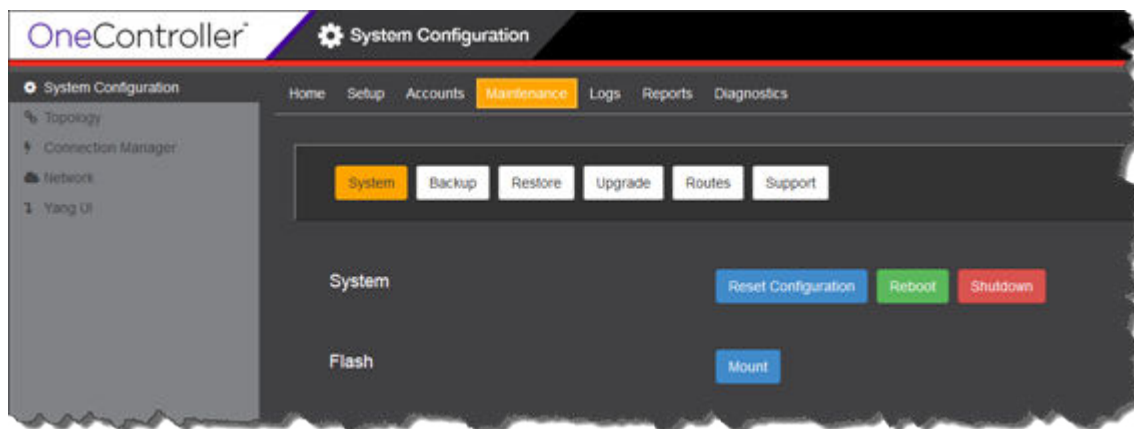


Figure 21: Maintenance System Screen

- 2 Click **Reset Configuration**. The system reboots, shutting down the OneController GUI interface.
- 3 Wait for the system to restart, and then restart the OneController GUI (see [Logging On to the OneController GUI](#) on page 30).

3 Getting Started

Logging On to the OneController GUI
Shutting Down or Rebooting OneController

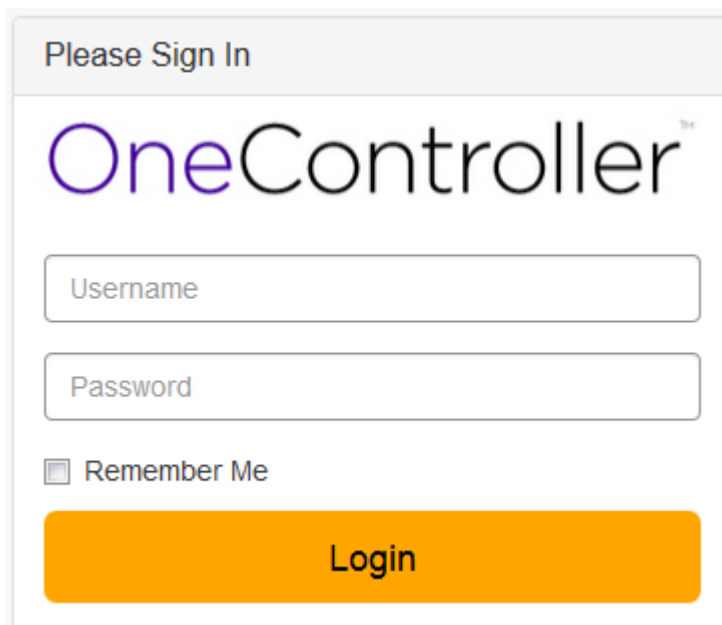
Logging On to the OneController GUI

You can access the OneController software through its web-based GUI DLUX.

To start the OneController GUI:

- 1 Open a web browser.
- 2 Enter the following in the address box: `http://<ipaddress>:8181/dlux/index.html`, where `<ipaddress>` is the IP address for OneController.

The **OneController logon** screen appears (see the following figure).



Please Sign In

OneController™

Username

Password

Remember Me

Login

Figure 22: OneController Logon Screen

- 3 Type your user credentials in the boxes, and then click **Login**.



Note

The default logon credentials are user name = `admin` and password = `abc123`.

The **OneController** main screen appears (see the following figure).

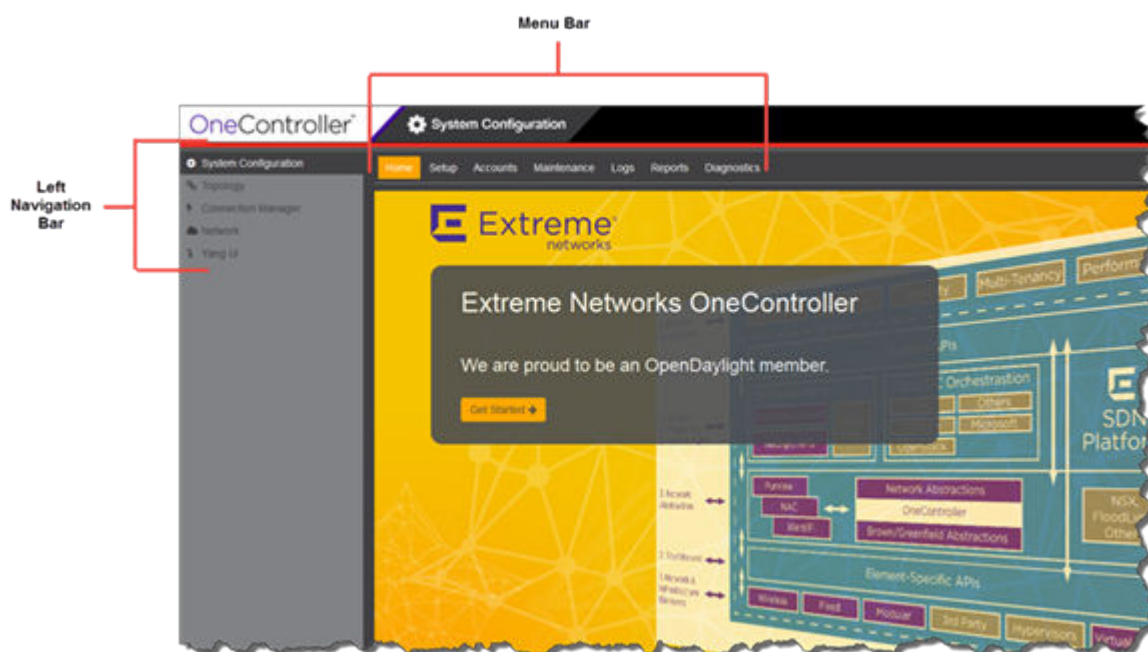


Figure 23: OneController Main Screen

Shutting Down or Rebooting OneController

To shut down or reboot OneController:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

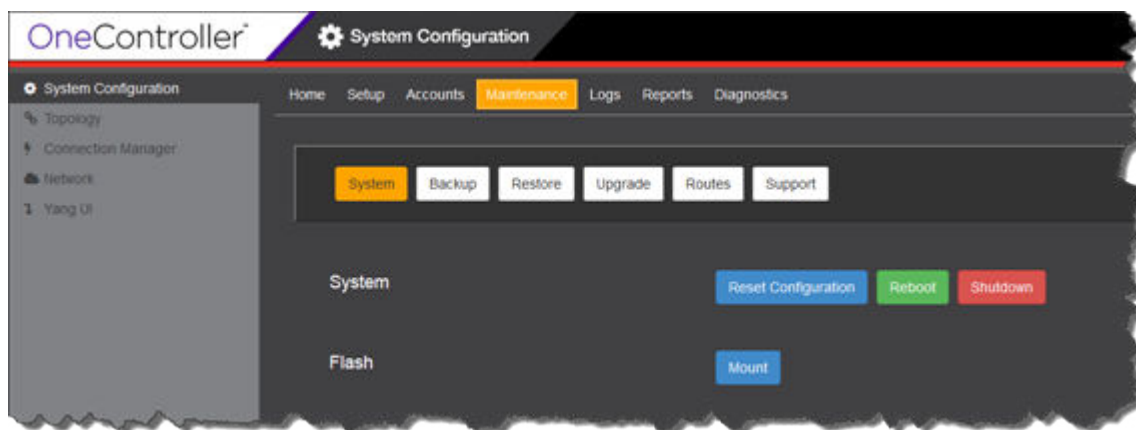


Figure 24: Maintenance—System Screen

- 2 Click **System**.
The **System** screen appears (see previous figure).
- 3 Click **Reboot** or **Shutdown** as desired.
- 4 When prompted, click **Yes** to confirm your choice.

4 OneController Administration

User Accounts
Backing Up and Restoring Configurations and Logs
Upgrading OneController
Changing System Settings

User Accounts

Creating User Accounts

To create user accounts:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Accounts**. The **Accounts** screen appears (see the following figure).

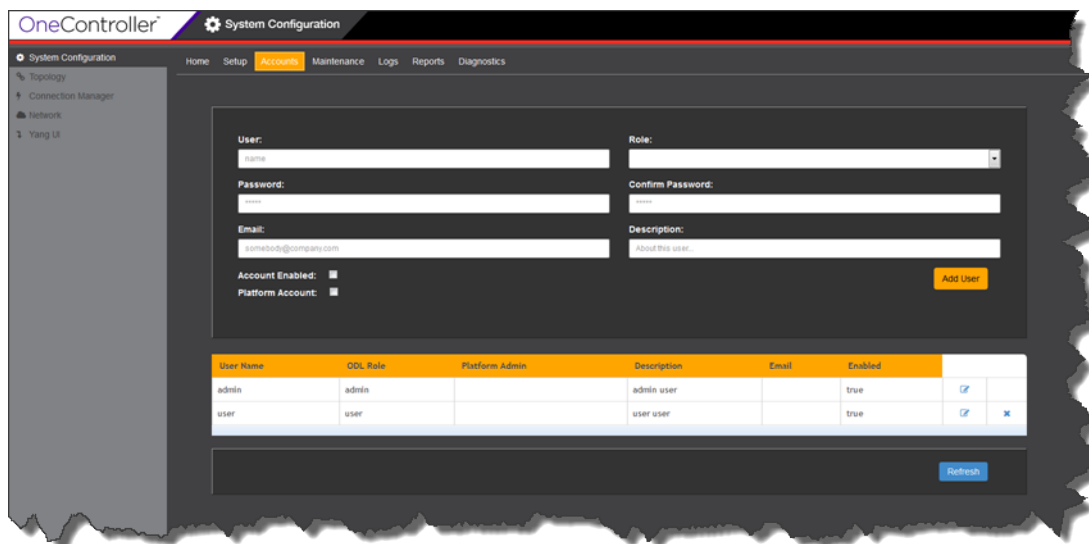


Figure 25: Accounts Screen

- 2 Enter information in the following fields:

Option	Description
User	User's name (should be a userid compatible with Linux)
Role	<ul style="list-style-type: none"> • Admin—assigns administrator role to user. • User—assigns user role to user.
Password	Type the new user's password, and then type it again in Confirm Password box.
Email	User's email address
Description	User description
Account Enabled	<p>Select to enable the account.</p> <p>You can temporarily disable an account by clearing this check box.</p>
Platform Account	<p>Select to provide the user with a Linux account, which allows connecting to the OneC-A-600 hardware appliance using SSH.</p> <p>The password for the Linux account is the same as the one set to access the OneController GUI (set in the Password box). This account is created in the <code>/home</code> directory and is added to the group "admin".</p>

- 3 Click **Add User**.

The new user appears in the table. You can also edit and delete existing user accounts (see [Modifying User Accounts](#) on page 34 and [Deleting User Accounts](#) on page 36).

Modifying User Accounts

To modify user accounts:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Accounts**. The **Accounts** screen appears (see the following figure).

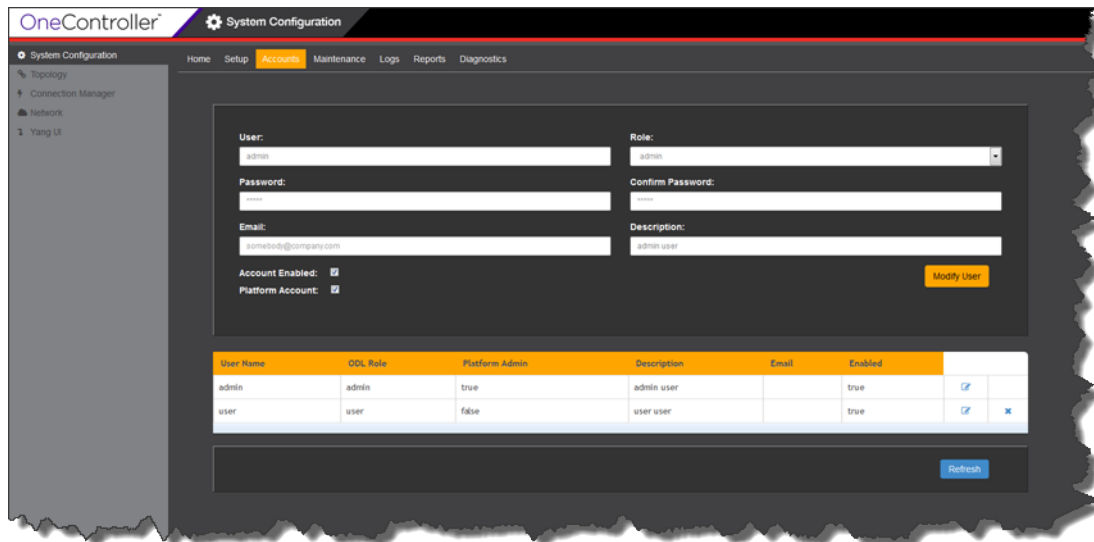



Figure 26: Accounts Screen

- 2 In the user table, for the desired user account, click  .
The information for the user appears in the fields.
- 3 Change information in the following fields as needed:

Option	Description
User	User's name (should be a userid compatible with Linux)
Role	<ul style="list-style-type: none"> • Admin—assigns administrator role to user. • User—assigns user role to user.
Password	Type the new user's password, and then type it again in Confirm Password box.
Email	User's email address
Description	User description
Account Enabled	<p>Select to enable the account.</p> <p>You can temporarily disable an account by clearing this check box.</p>
Platform Account	<p>Select to provide the user with a Linux account, which allows connecting to the OneC-A-600 hardware appliance using SSH.</p> <p>The password for the Linux account is the same as the one set to access the OneController GUI (set in the Password box). This account is created in the <code>/home</code> directory and is added to the group "admin".</p>

- 4 Click **Modify User**.

The revised user information appears in the lower table.

Deleting User Accounts

Deleting an account permanently removes access for that user. To *temporarily* remove access, disable the account instead, by clearing the **Account Enabled** check box (see [Modifying User Accounts](#) on page 34).



Note

Deleting a currently logged on user does not force the user out of OneController.

To delete user accounts:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Accounts**. The **Accounts** screen appears (see the following figure).

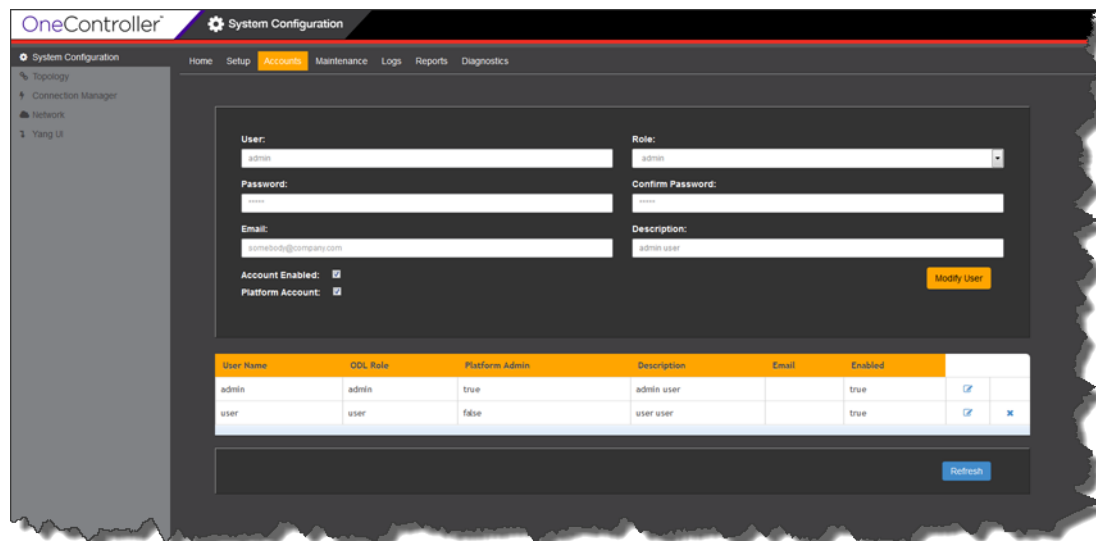


Figure 27: Accounts Screen

- 2 In the table, for user that you want to delete, click .
- 3 The user account disappears from the table.

Backing Up and Restoring Configurations and Logs

You can *back up* the following information (see [Backing Up Configurations and Logs](#) on page 37):

- Platform configuration and logs
- OneController configuration and logs

The following OneController directories and files are backed up:

- /usr/opensight/data/log/
- /usr/opensight/configuration/
- /usr/opensight/etc/
- /usr/opensight/idmlight.db
- /usr/opensight/log (backed up if it exists)
- /usr/opensight/ObjectStore (if it exists)
- /usr/opensight/PutObjectStoreHere (if it exists)

Restoring only restores configurations, not log files (see [Restoring Configurations](#) on page 40).

You can also *copy* backup files to an external server (see [Copying Backup Files to Remote Location](#) on page 42).

Backing Up Configurations and Logs

You can perform an immediate backup or schedule backups at recurring times. The backup file is saved as a zip file that can be stored on the local machine, external USB drive (see [Connecting USB Portable Drives to OneController](#) on page 45), or a remote machine.

If a backup is scheduled, its next occurrence appears next to **Next Backup** (see [Figure 29: Maintenance—Backup Screen](#) on page 38). You can delete backup schedules (see [Deleting Backup Schedules](#) on page 39). Backup files appear on the **Restore** page (see [Restoring Configurations](#) on page 40).

To create backup files:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

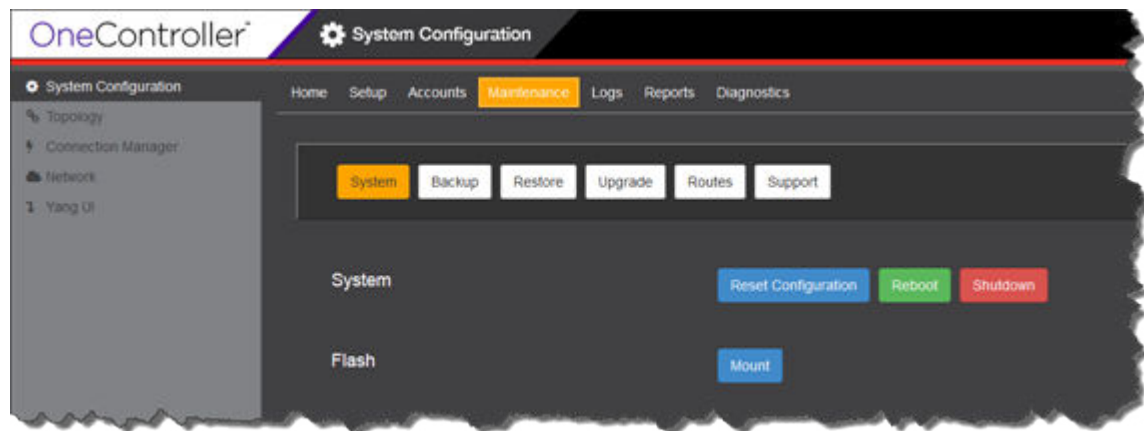


Figure 28: Maintenance—System Screen

2 Click Backup.

The Maintenance Backup screen appears (see the following figure).

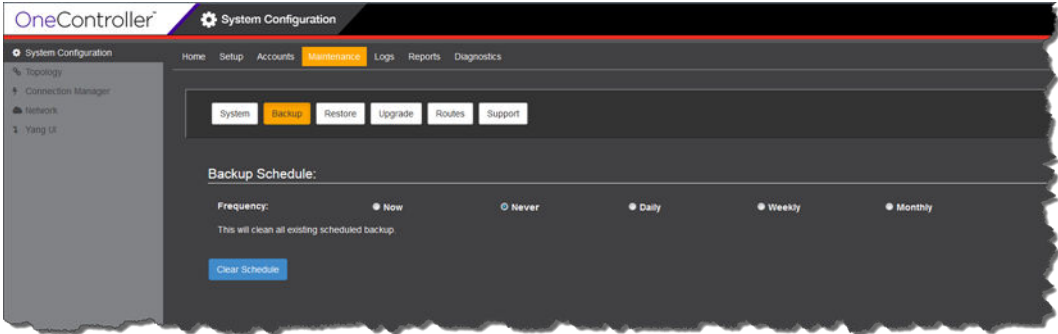



Figure 29: Maintenance—Backup Screen

3 Select a scheduled frequency:

Frequency	Description
Now	Starts the backup immediately.
Daily	<p>Schedules a recurring daily backup.</p> <p>Select:</p> <ul style="list-style-type: none"> • Every day—seven days a week • Every weekday—five days a week (Monday–Friday) <p>, and then Start Time</p>
Weekly	<p>Schedules recurring weekly backups.</p> <p>Select day(s) of the week for the backup to occur:</p> <p>, and then Start Time</p>
Monthly	<p>Schedules recurring monthly backups.</p> <p>Select the day of the month for the backup in the Day of Month list, and then Start Time</p>



Frequency	Description
	

- 4 For daily, weekly, and monthly scheduled backups, under **Backup Options**, select the location to backup the files to in the **Select Where to Back up** list:
 - **Flash**—To a USB portable drive. You must mount the USB drive first (see [Connecting USB Portable Drives to OneController](#) on page 45).
 - **Local**—On the same hardware that hosts OneController in `/var/controller/images/bu_restore`.
 - **Remote**—To a remote device:
 - a To move the backup file to a remote file server or desktop, select a supported protocol in the **Protocol** list:
 - ftp
 - scp
 - http
 - b Enter the IP address or host name for the remote device in the **Server** box.
 - c Enter your logon credentials for the remote device in the **User ID** and **Password** boxes. Re-enter your password in the **Confirm** box.
 - d Enter the location to copy the backup files to in the **Directory** box (in the form "\\top level folder name\folder name" for example). If the file is in the root directory, you can leave this blank.
- 5 Click:
 - **Start** (if you selected **Now** for an immediate backup)
 - **Schedule** (if you selected **Daily**, **Weekly**, or **Monthly**).

Backup files appear (in the form `<hostname>.<MMDDYYYY>.<Time-as-an-integer>.zip`) on the **Restore** screen (see [Restoring Configurations](#) on page 40).

Deleting Backup Schedules

To delete existing scheduled backups:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

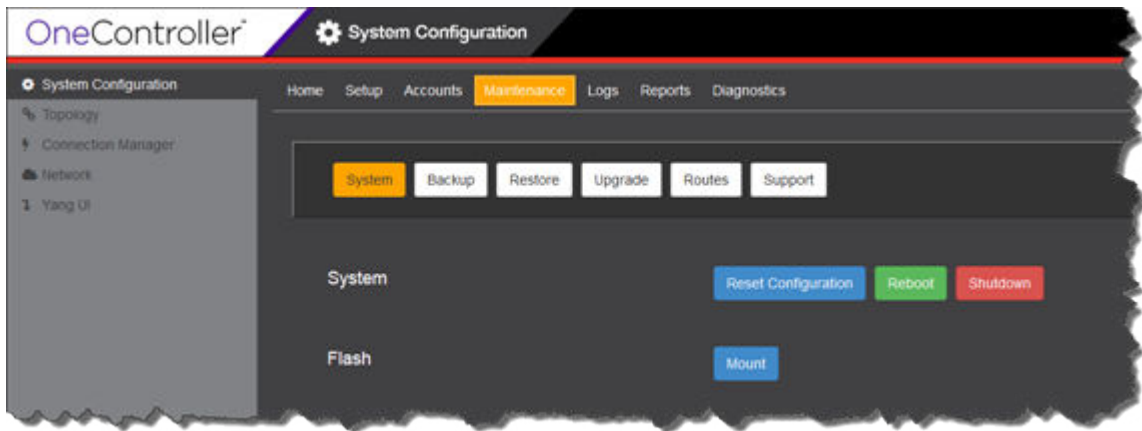


Figure 30: Maintenance—System Screen

- 2 Click **Backup**. The **Maintenance Backup** screen appears (see the following figure).

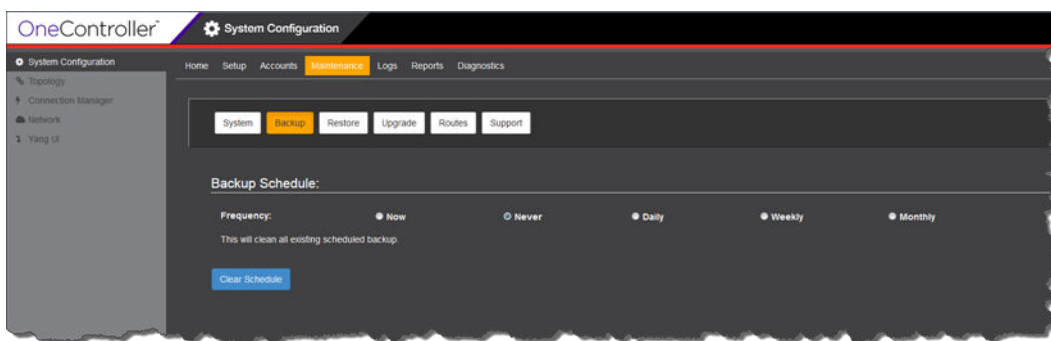


Figure 31: Maintenance—Backup Screen

- 3 For **Frequency**, select **Never**.
- 4 Click **Clear Schedule**.

Restoring Configurations

To restore backed up configurations (see [Backing Up Configurations and Logs](#) on page 37):

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

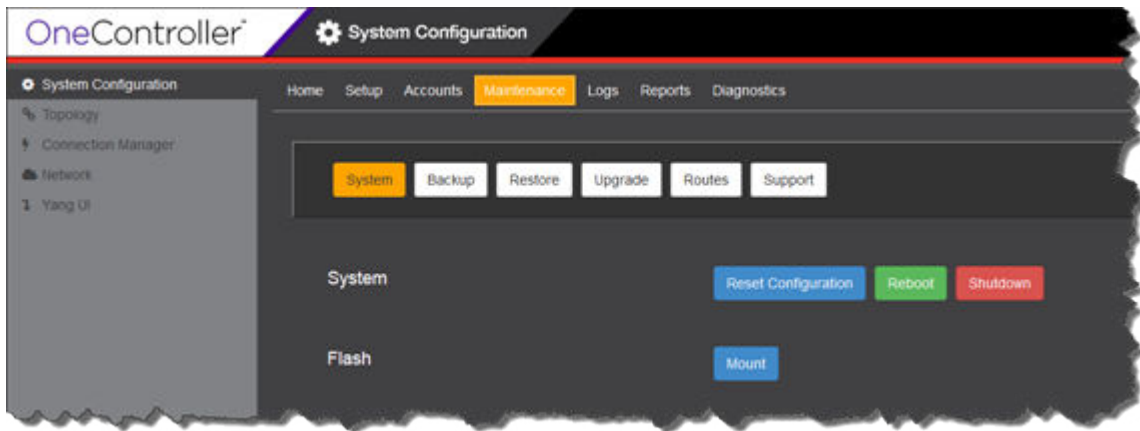


Figure 32: Maintenance—System Screen

- 2 Click **Restore**. The **Restore** screen appears (see the following figure).

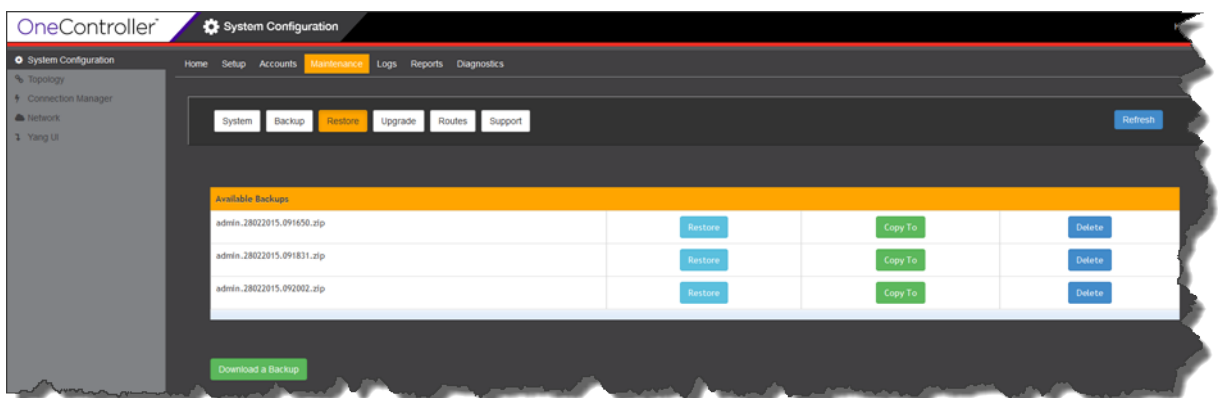
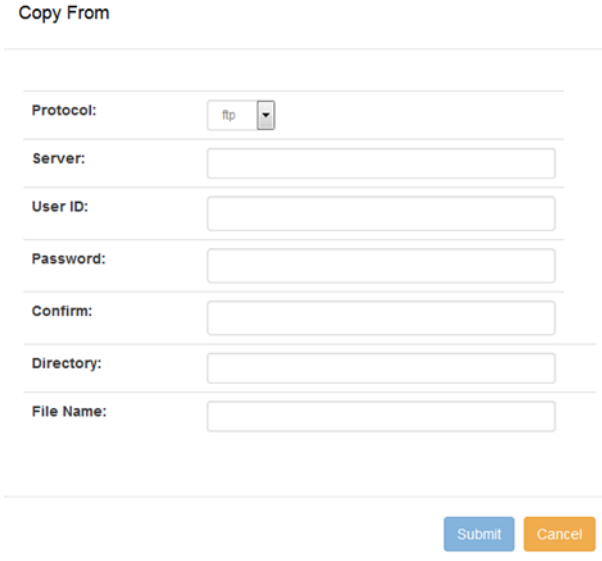


Figure 33: Maintenance—Restore Screen

- 3 If the backup configuration file is *located on a remote server*, you must first download it locally:

- a Click **Download a Backup**.

The **Copy To** dialog box appears (see the following figure).



The screenshot shows a 'Copy From' dialog box with the following fields and controls:

- Protocol:** A dropdown menu with 'ftp' selected.
- Server:** A text input field.
- User ID:** A text input field.
- Password:** A text input field.
- Confirm:** A text input field.
- Directory:** A text input field.
- File Name:** A text input field.
- Buttons:** 'Submit' (blue) and 'Cancel' (orange) buttons at the bottom right.

Figure 34: Copy From Dialog Box

- b For the type of remote server, select the appropriate protocol in the **Protocol** list:
- ftp
 - scp
 - http
- c Enter the IP address or host name for the server that you are copying from in the **Server** box.
- d Enter your logon credentials for the server that you are copying from in the **User ID** and **Password** boxes. Re-enter your password in the **Confirm** box.
- e Enter the location to copy the backup files from in the **Directory** box (in the form "`\\top level folder name\folder name`").
- f Enter the name of the backup file in the **File Name** box.
- g Click **Submit**.
- The backup file now appears in the **Available Backups** table.
- 4 Under **Available Backups** for the desired backup file, click **Restore**. When prompted to confirm your selection, click **Yes**.

Copying Backup Files to Remote Location

To copy backup files to a remote location:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

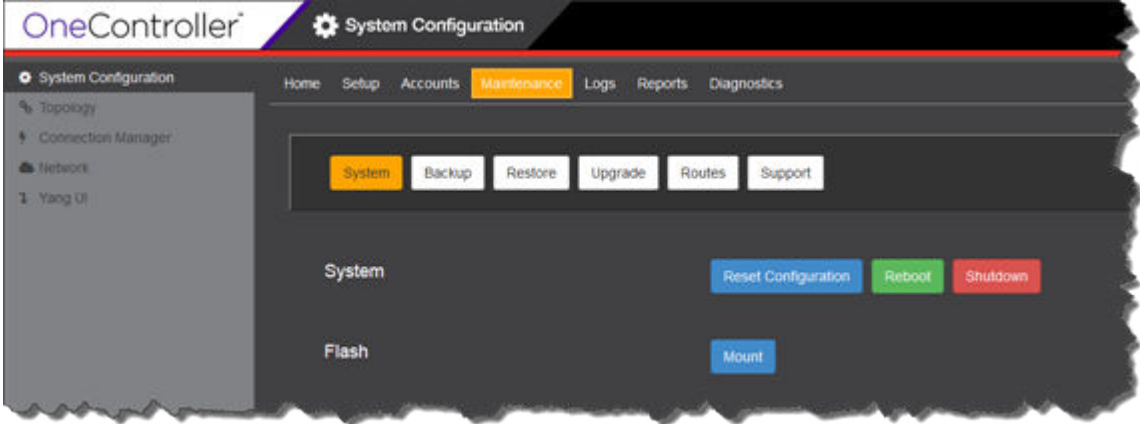


Figure 35: Maintenance—System Screen

- 2 Click **Restore**. The **Restore** screen appears (see the following figure).

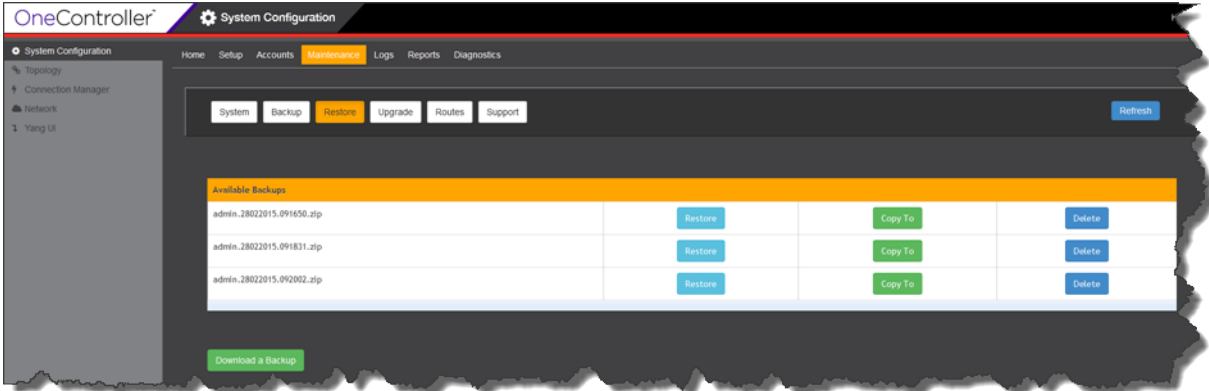


Figure 36: Maintenance—Restore Screen



- 3 Under **Available Backups** for the desired backup files, click **Copy To**.
The **Copy To** dialog box appears (see the following figure).

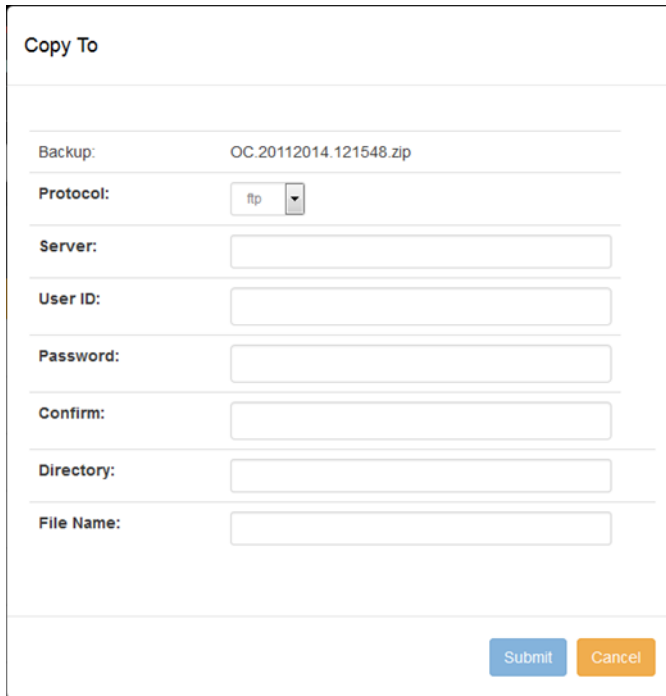


Figure 37: Copy To Dialog Box

- 4 For transmitting the files, select the protocol in the **Protocol** list:
 - ftp
 - scp
 - http
- 5 Enter the IP address or host name for the server that you are copying to in the **Server** box.
- 6 Enter your logon credentials for the server that you are copying to in the **User ID** and **Password** boxes. Re-enter your password in the **Confirm** box.
- 7 Enter the location to copy the backup files to in the **Directory** box (in the form "`\\top_level_folder_name\folder_name`").
- 8 Enter the name of the backup file in the **File Name** box.
- 9 Click **Submit**.

Deleting Backup Files

To delete existing backup files:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

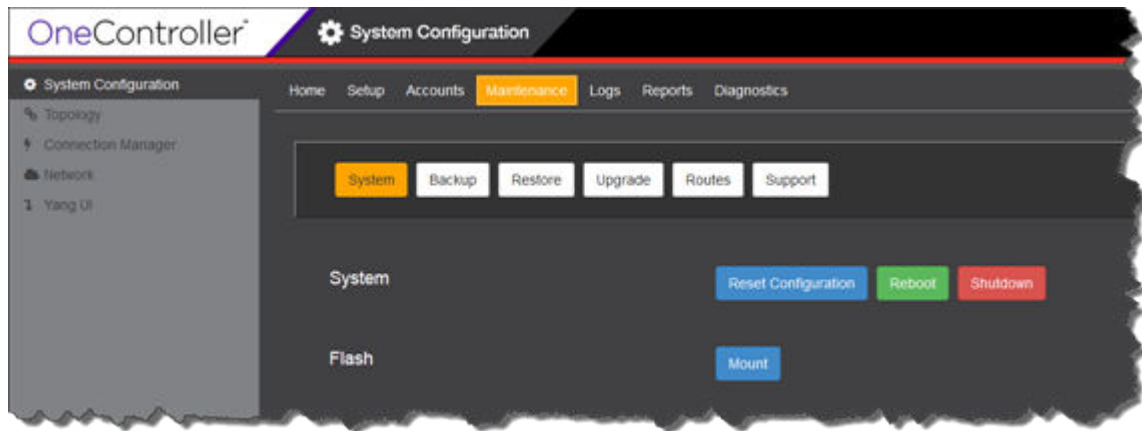


Figure 38: Maintenance—System Screen

- 2 Click **Restore**. The **Restore** screen appears (see the following figure).

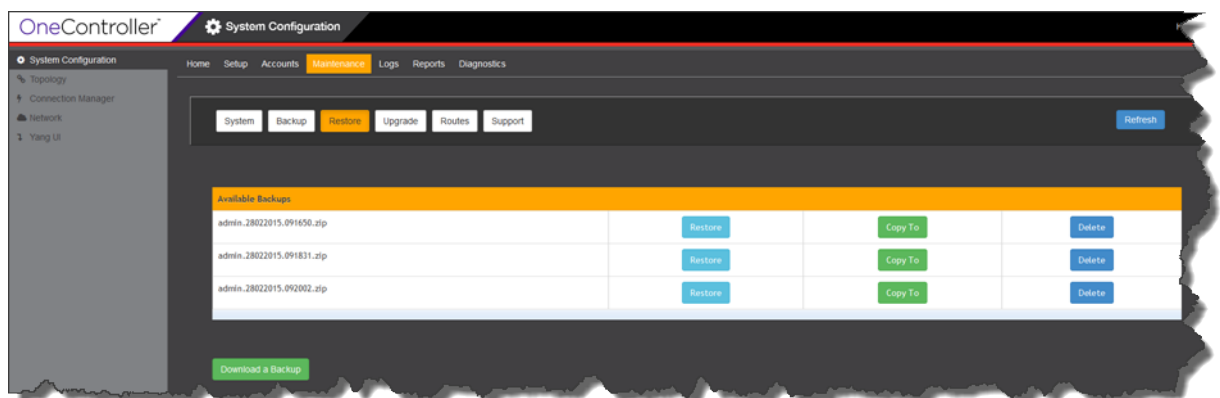


Figure 39: Maintenance—Restore Screen

- 3 Under **Available Backups**, for the desired backup file click **Delete**. When prompted to confirm your selection, click **Yes**.

The backup file is removed from the list.

Connecting USB Portable Drives to OneController

For backing up and restoring configurations/logs (see [Backing Up Configurations and Logs](#) on page 37 and [Restoring Configurations](#) on page 40), you may want to use an external, portable USB drive. To use a USB portable drive, you must mount it first so that OneController recognizes it.

USB requirements:

- USB drive must be formatted as File Allocation Table (FAT).

- All desired files must be in the top level directory.
- USB v2.0 (if USB v3.0, it must be backward compatible).

To enable use of a USB drive:

- 1 Insert a USB drive into:
 - OneC-A-600: USB ports on front or back panel. Only one USB drive can be inserted at a time.
 - OneC-V: USB port on ESXi host hardware.
- a For the OneC-V, in the VMware vSphere client in the left pane, right-click the OneController virtual machine, and click **Edit Settings**(see the following figure).

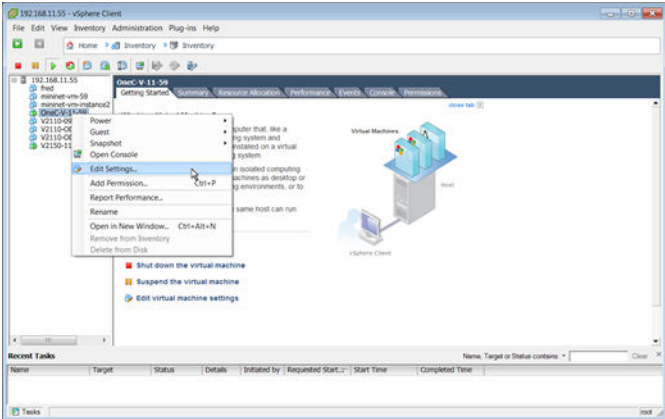


Figure 40: vSphere Client—Edit Settings

The Virtual Machine Properties dialog box appears (see the following figure).

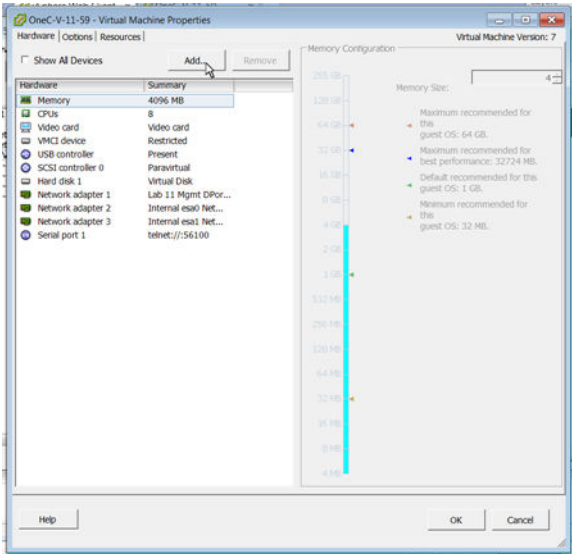


Figure 41: vSphere Client—Virtual Machine Properties Dialog Box

- b Click the **Hardware** tab.



- c Click **Add**.

The **Add Hardware** dialog box appears (see the following figure).

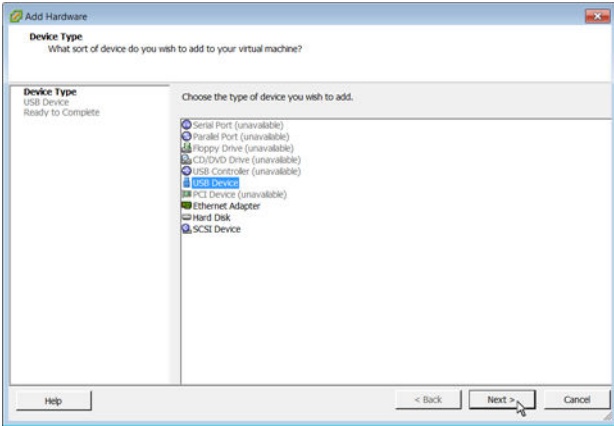


Figure 42: Add Hardware Dialog Box

- d Click **USB controller**, and then click **Next**.

The **Add Hardware—Select USB Device** dialog box appears (see the following figure).

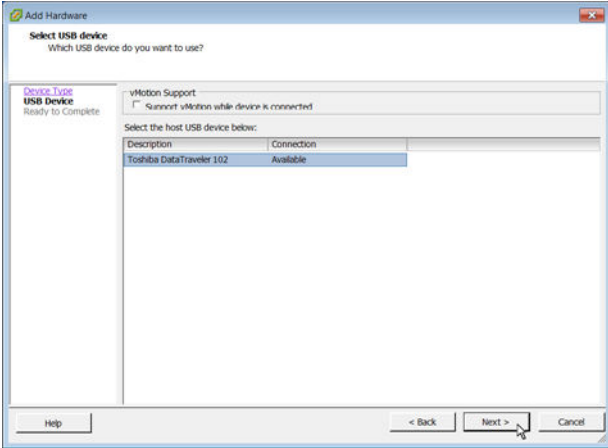


Figure 43: Add Hardware—Select USB Device Dialog Box



- e Select the USB device in the list, and then click **Next**.

The **Add Hardware—Ready to Complete** dialog box appears (see the following figure).

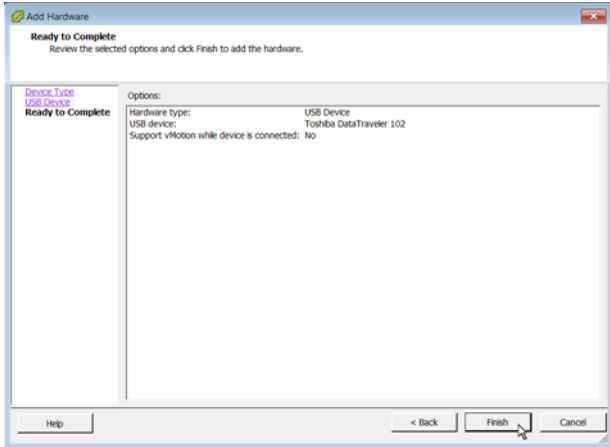


Figure 44: Add Hardware—Ready to Complete Dialog Box

- f Click **Finish**.

The USB device appears in the **Virtual Machine Properties** dialog box (see the following figure).

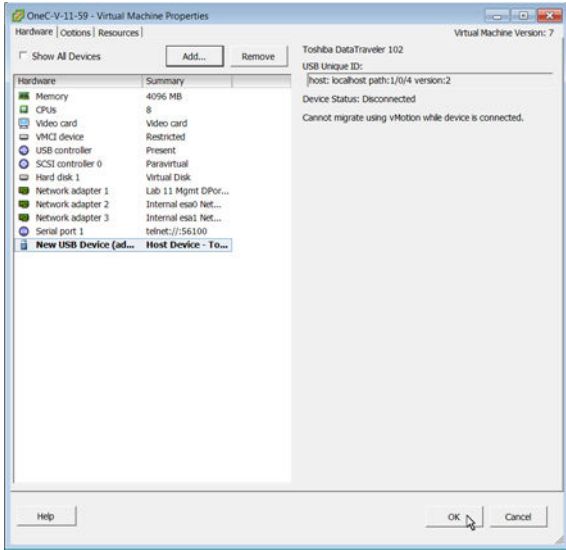


Figure 45: Virtual Machine Properties Dialog Box

- g Click **OK**.



- On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

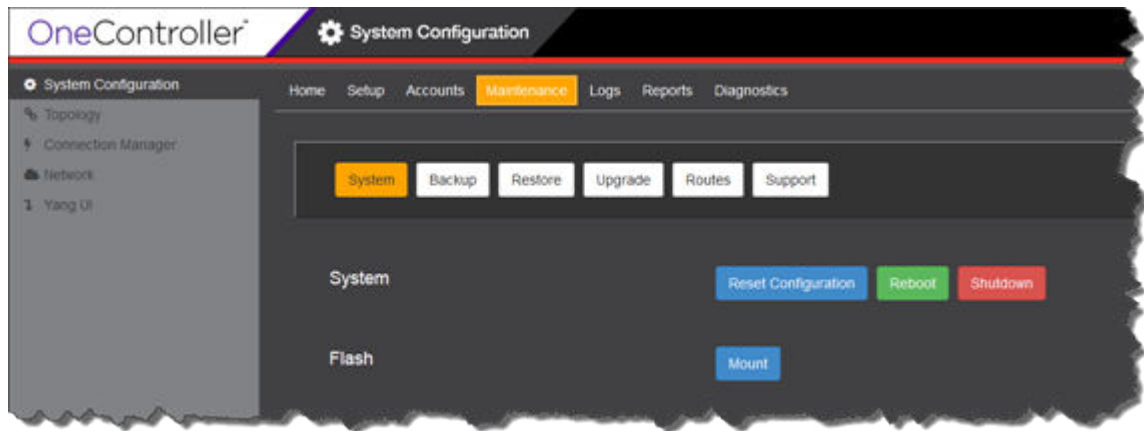


Figure 46: Maintenance—System Screen

- Click **Mount**. The USB device's status information and list of files appears (see the following figure).

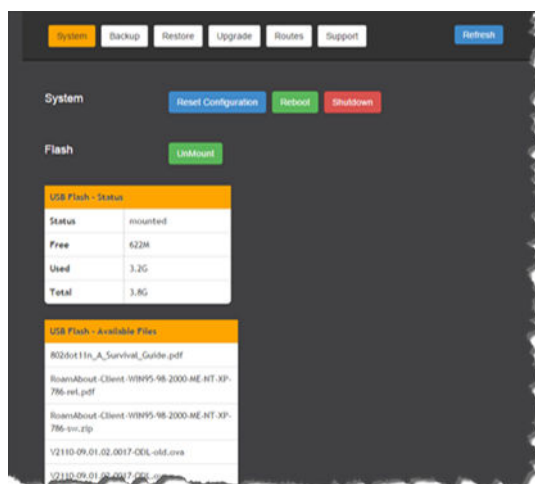


Figure 47: Maintenance—System, Mount USB Results Screen

Upgrading OneController

After the initial installation (see [Installing and Setting Up OneController](#) on page 11), you can upgrade OneController with updated images available at <https://extranet.extremenetworks.com/downloads/Pages/OneController.aspx> on the **Software** tab.

The upgrade images have the following extensions:

- OneC-V Controller image extension: *jsf*
- OneC-A-600 Controller image extension: *ice*

The configuration directories that are copied during a backup (see [Backing Up and Restoring Configurations and Logs](#) on page 36) are copied before an upgrade starts. The platform configuration is restored upon completion of the upgrade.

Caution



The OneController configuration directories are restored to `/usr/.opendaylight/preserved` when an upgrade finishes. Because OneController is based on the OpenDaylight controller, whose development is not controlled by Extreme Networks, the compatibility of your current configuration files with new OneController image cannot be assured. After the upgrade is complete, use a file compare utility to examine differences between your old backup configuration files in the `preserved` directory with the new configuration files in `/usr/.opendaylight/configuration/` that were installed by the upgrade. Make changes to the new configuration files as needed.

To upgrade the OneController software:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

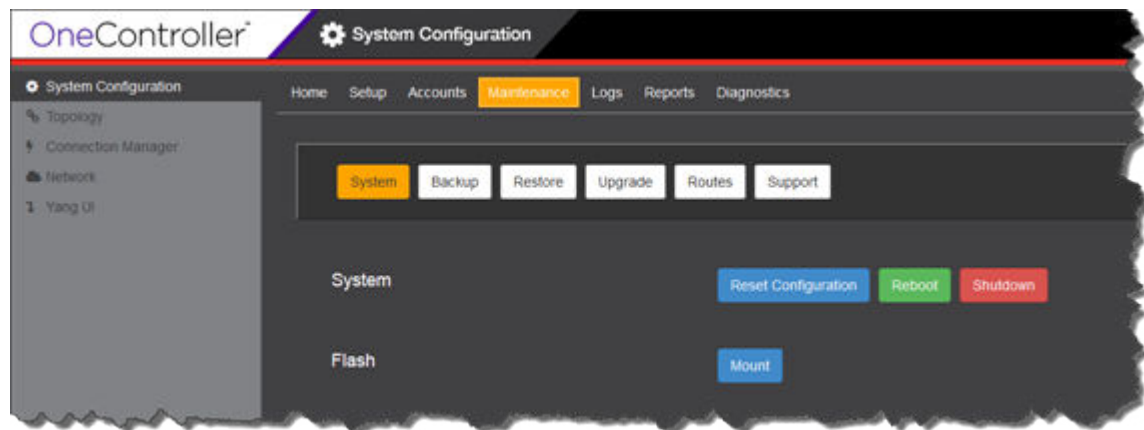


Figure 48: Maintenance—System Screen

2 Click **Upgrade**.

The **Upgrade** screen appears (see the following figure).

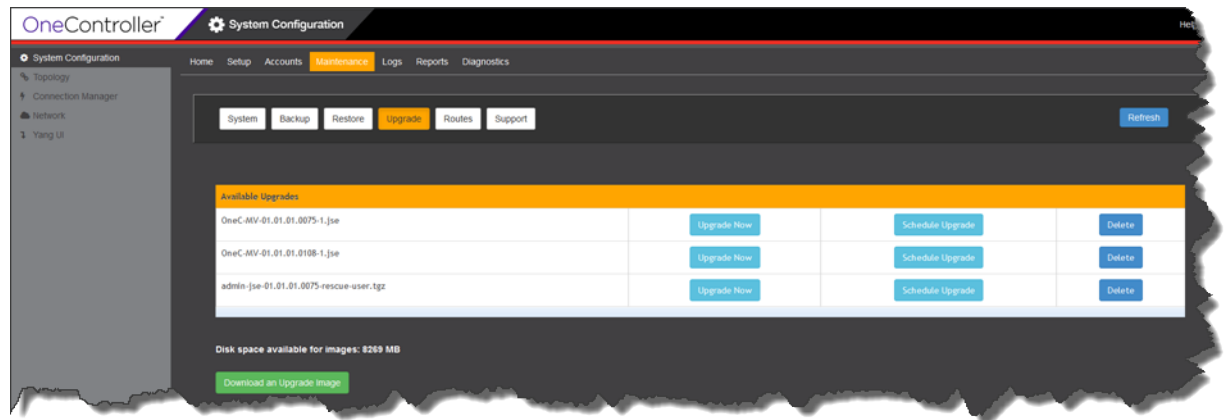
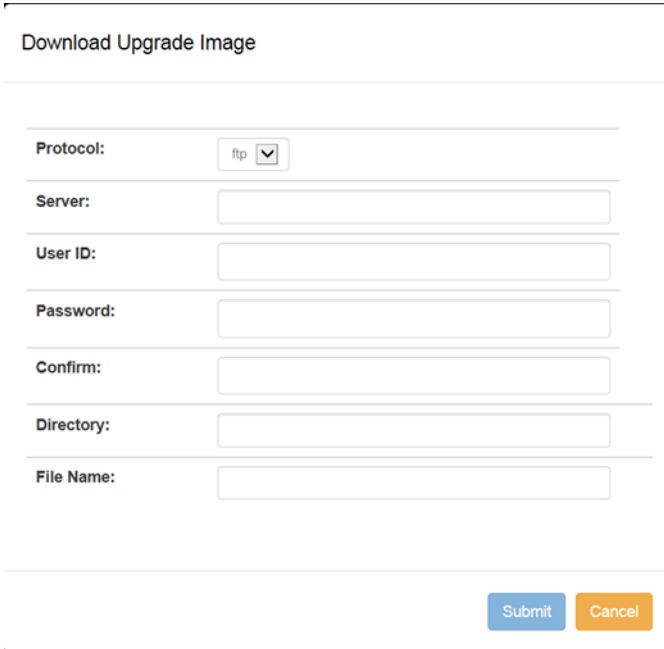


Figure 49: Maintenance—Upgrade Screen

Any software upgrade images that are available locally (on the hardware that is running OneController) appear in the **Available Upgrades** table.

- 3 If the image that you want to upgrade to is not local, copy it locally:
 - a Click **Download an Upgrade Image**.
The **Download Upgrade Image** dialog box appears (see the following figure).



The screenshot shows a dialog box titled "Download Upgrade Image". It contains the following fields and controls:


- Protocol:** A dropdown menu with "ftp" selected.
- Server:** A text input field.
- User ID:** A text input field.
- Password:** A text input field.
- Confirm:** A text input field.
- Directory:** A text input field.
- File Name:** A text input field.
- Buttons:** "Submit" (blue) and "Cancel" (orange) buttons at the bottom right.

Figure 50: Download Upgrade Image Dialog Box

- b For transmitting the file, select the protocol in the **Protocol** list:
 - ftp
 - scp
 - http
- c Enter the IP address or host name for the server that you are copying the image file from in the **Server** box.
- d Enter your logon credentials for the server you are copying from in the **User ID** and **Password** boxes. Re-enter your password in the **Confirm** box.
- e Enter the upgrade image location where you are downloading from in the **Directory** box (in the form "\\top level folder name\folder name" for example). If the file is in the root directory, you can leave this blank.
- f Enter the name of the upgrade file in the **File Name** box.
- g Click **Submit**.
- h Click **Refresh**.
The upgrade image appears in the **Available Upgrades** table.

- 4 To upgrade at a *later date*:
 - a For the desired upgrade image, click **Schedule Upgrade**.
The **Schedule Upgrade** dialog box appears (see the following figure).

Figure 51: Schedule Upgrade Dialog Box

- b In the **Backup Method** list, select where the current OneController image should be backed up to:
 - **none**—no backup is performed
 - **local**—on the same hardware that hosts OneController
 - **usb**—on a removable USB flash drive connected the hardware that hosts OneController
- c Select the upgrade date in **Start Date** by typing a date or by clicking .
- d In **Start Time**, select the upgrade time:

- e Click **Submit**.

- 5 To upgrade *immediately*:
 - a For the desired upgrade image, click **Upgrade Now**.
The **Upgrade Now** dialog box appears (see the following figure).

Figure 52: Upgrade Now Dialog Box

- b In the **Backup Method** list, select where the current OneController image should be backed up to:
 - **none**—no backup is performed
 - **local**—on the same hardware that hosts OneController
 - **usb**—on a removable USB flash drive connected the hardware that hosts OneController
- c Click **Submit**.

OneController upgrades the software and reboots.

You can verify that the upgrade was successfully performed by checking the software version shown in the **Manufacturing Information** report (see [Viewing OneController Reports](#) on page 71).

Changing System Settings

Using the OneController GUI, you can change the following OneController system settings that you set up originally during installation (see [Installing and Setting Up OneController](#) on page 11).

The **Reset Configuration** button resets the system settings back to the factory default (see [Reverting to the Factory Default Settings](#) on page 29) without removing any customer-installed features (see [Installing Additional Features](#) on page 24).

To change hardware settings:

- 1 Click **Setup**, and then the desired hardware settings tab:
 - **Host Info**: set host name, domain name, DNS servers (see [Host Information](#) on page 55)
 - **Time**: set the time zone and current time, and whether to enable NTP support (see [Time](#) on page 55)
 - **Interfaces**: set IP address/netmask/VLAN ID for all the interfaces (see [Interfaces](#) on page 56)
 - **Logging Server**: set remote log servers' IP addresses (see [Remote Logging \(Syslog\) Server](#) on page 57)
 - **SNMP**: configure or disable the OneController SNMP agent (see [SNMP](#) on page 58)
- 2 Click **Setup**, and then click the **Summary** tab. A summary of all of your system settings appears.

3 Click **Submit**.



Note

Changes made on any of the system setting screens are not applied until you click the **Submit** button on the Summary screen.

Host Information

To access the **Host Information Setup** screen, click **Setup**, and then click the **Host Info** tab. The **Host Information Setup** screen appears (see the following figure).

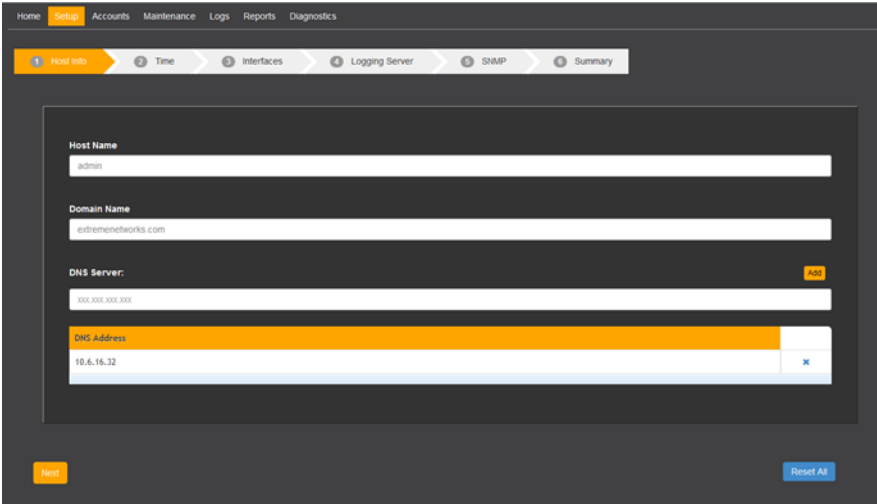


Figure 53: Host Information Setup Screen

Host Name	OneController's host name.
Domain Name	Domain name.
DNS Server	<p>DNS server IP address. Up to three DNS servers are supported. To <i>add</i> a DNS server:</p> <ol style="list-style-type: none"> 1 Type a new DNS server IP address in the DNS Server box. 2 Click Add. The new DNS server appears in the DNS Address table. <p>To <i>delete</i> a DNS server: In the DNS Address table, next to the DNS sever that you wish to remove, click the X. The DNS server disappears from the DNS Address table.</p>

Time

To access the **Time Setup** screen, click **Setup**, and then click the **Time** tab. The **Time Setup** screen appears (see the following figure).



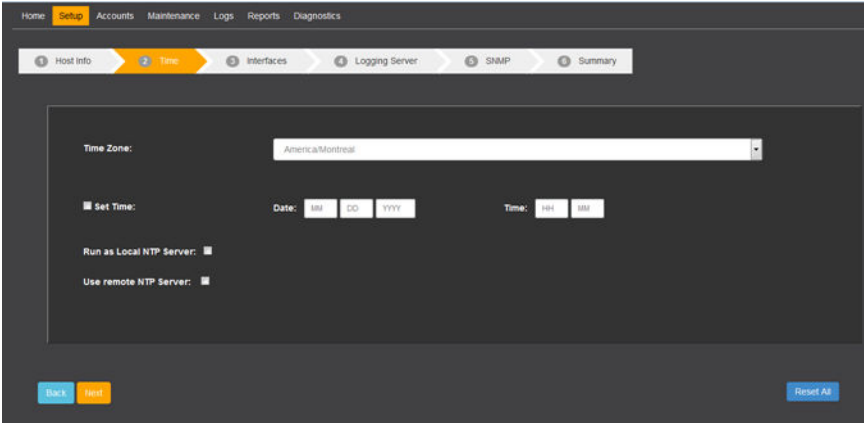


Figure 54: Time Setup Screen

Time Zone	Sets the time zone.
Date and Time	To set the time and date, select Set Time , enter values in the Date and Time boxes, and then click Set Time Now .
Run as Local NTP Server	Sets the OneC-A-600 hardware appliance to act as an NTP server. This can be useful for synchronizing time for a cluster of OneControllers.
Use remote NTP Server	<p>Selecting Use remote NTP Server enables the OneController hardware to use a remote NTP server at the indicated IP address. You can designate up to three NTP servers for OneController.</p> <ol style="list-style-type: none"> 1 Type an IP address for the desired NTP server in the Remote NTP Server box. 2 Click Add. <p>The NTP server appears in the NTP Server table.</p>

Interfaces

To access the **Interfaces Setup** screen, click **Setup**, and then click the **Interfaces** tab. The **Interfaces Setup** screen appears (see the following figure).



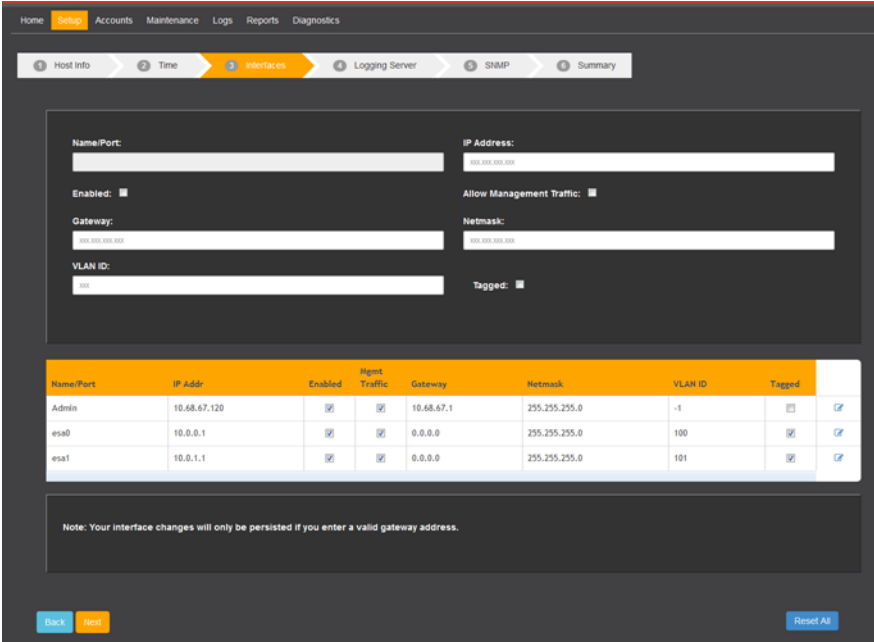



Figure 55: Interfaces Setup Screen

To change an interface's information, click  next to the interface in the table. The information for the interface appears in the relevant boxes. Click **Apply** to apply the changes.

Name/Port	The OneController interface (Admin, EAS0, EAS1).
IP Address	Interface's IP address.
Enabled	Whether or not the interface is enabled.
Allow Management Traffic	Select to allow management traffic over the selected port.
Gateway	Interface's gateway.
Netmask	Interface's subnet mask.
VLAN ID	VLAN ID.
Tagged	Whether or not tagging is enabled.

Remote Logging (Syslog) Server

You can specify up to three Syslog servers.

To access the **Logging Server Setup** screen, click **Setup**, and then click the **Logging Server** tab. **Logging Server Setup** screen appears (see the following figure).



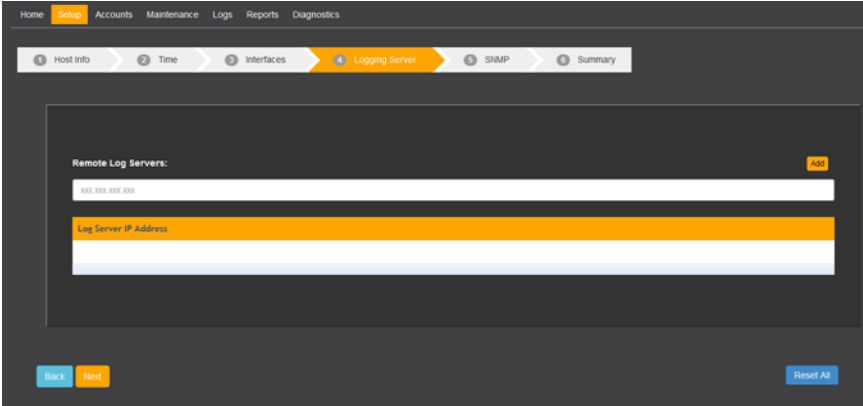


Figure 56: Logging Server Setup Screen

To *add* a remote logging (Syslog) server, type the IP address in the **Remote Log Servers** box, and then click **Add**. The server appears in the **Log Server IP Address** table.

To delete a remote logging server, click **X** next to the desired server in the table. The server disappears from the table.

Selecting the check box next to a remote logging server enables it.

SNMP

To access the **SNMP Setup** screen, click **Setup**, and then click the **SNMP** tab. The **SNMP Setup** screen appears (see the following figures).

On this screen you can enable/disable SNMP and set up SNMPv2/v3 with correct parameters (for connecting to NMS/EMS hardware—for example, NetSight—to which OneController sends its status information and events).



Note This is independent of the SNMP module that runs as part of the OneController software that can be used to send configuration information to switches.

To *disable* SNMP, click **No SNMP**.

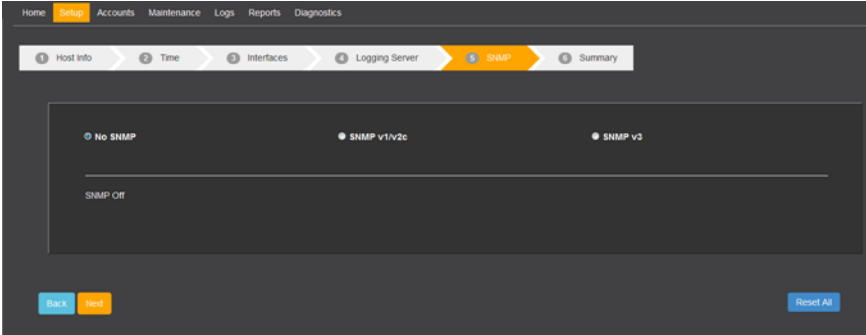


Figure 57: SNMP Setup Screen—SNMP Disabled

To *enable* *SNMPv1* or *v2c*, click **SNMPv1/v2c**, and enter values in the following boxes:



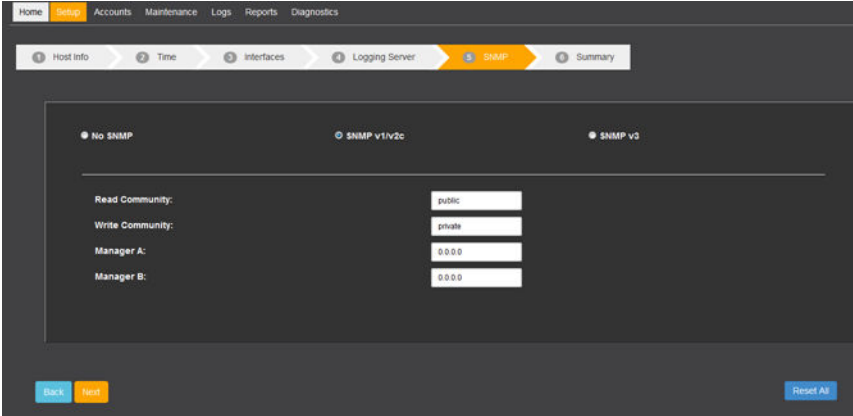


Figure 58: SNMP Setup Screen—SNMPv1/v2c

Read Community	The read community string.
Write Community	The write community string.
Manager A	IP address of Manager A.
Manager B	IP address of Manager B.

To enable SNMPv3, click **SNMPv3**, and enter values in the following boxes:

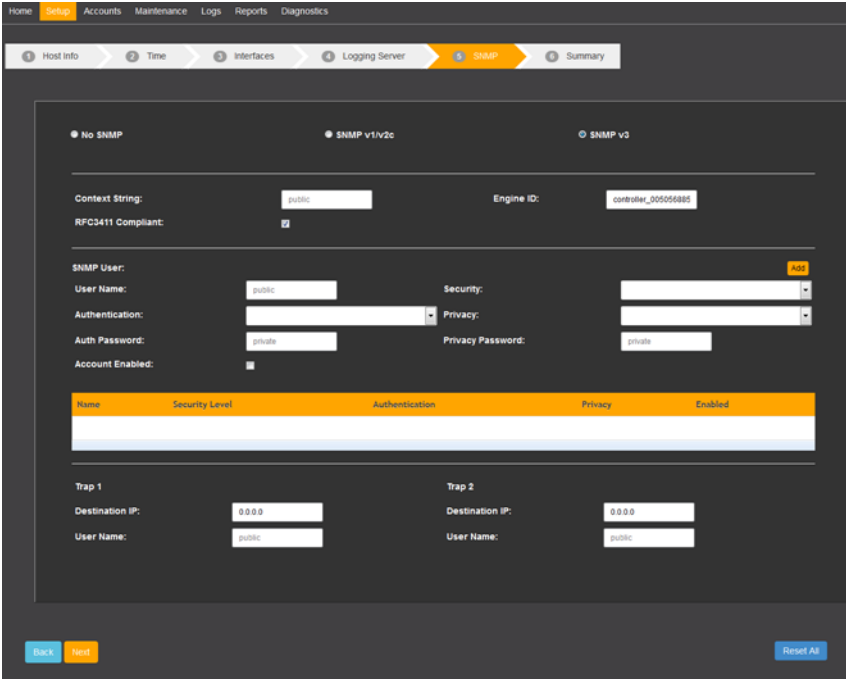


Figure 59: SNMP Setup Screen—SNMPv3



Context String	An SNMP context is a collection of management-related information. The SNMP context is identified by the combination of Engine ID and a context string. The context string can be a maximum of 32 octets (ASCII characters) long.
Engine ID	The Engine ID uniquely identifies the SNMP engine instance (SNMP agent on the OneController). The Engine ID is used in conjunction with SNMP user passphrases to generate the keys that are used to secure SNMP transmissions for the user.
RFC3411 Compliant	When enabled, the OneController prefixes the administrator-entered Engine ID string with 4 octets representing the "binary equivalent of the agent's SNMP management private enterprise number as assigned by the Internet Assigned Numbers Authority (IANA)" according to RFC3411. Otherwise, the Engine ID entered by the administrator is used as is.
SNMP User	
User Name	The unique identifier for an account that can send SNMPv3 messages to and from the controller.
Security	The SNMPv3 security level of the user account. An account must have one of three security levels: <ul style="list-style-type: none"> • authPriv—messages are both cryptographically signed and encrypted for privacy. • authNoPriv—messages are cryptographically signed, which can be used to check that the message has not been tampered with and is from, or for, the intended user. • noauthNoPriv—messages are not signed and authenticated and are not encrypted for privacy. Some MIBs and OIDs may be inaccessible to accounts with this security level.
Authentication	Sets the algorithm used to generate signatures for authentication: <ul style="list-style-type: none"> • none—messages sent are not signed. Valid only if the account's security level is "noAuthNoPriv". • md5—standard MD5 hash algorithm. • sha—standard SHA1 hash algorithm.
Privacy	Sets the algorithm used to encrypt messages: <ul style="list-style-type: none"> • none—messages are not encrypted. • des—standard DES algorithm is used to encrypt messages. Only valid if the account's security level is "authPriv". • aes—AES 128-bit encryption is used to protect messages. Only valid if the account's security level is "authPriv".
Auth Password	Passphrase that SNMP uses to generate the key used to generate signatures for messages.
Privacy Password	Passphrase that SNMP uses to generate the key used to encrypt/decrypt messages.
Account Enabled	Enables/disables the ability to send and receive messages for this account.
Trap 1 OneController allows you to define up to two different network managers that can receive SNMP notifications (traps). Each trap destination is defined by an IP address and user name:	
Destination IP	For trap 1, the IP address where traps are forwarded to.

User Name	Account name used when sending traps to the destination IP address. The user name must correspond to one of the SNMP v3 users listed in the account table. Traps are sent using security level settings defined for the selected account. Each trap destination can use a different SNMPv3 user account for transmission.
Trap 2 OneController allows you to define up to two different network managers that can receive SNMP notifications (traps). Each trap destination is defined by an IP address and user name:	
Destination IP	For trap 2, the IP address where traps are forwarded to.
User Name	Account name used when sending traps to the destination IP address. The user name must correspond to one of the SNMP v3 users listed in the account table. Traps are sent using security level settings defined for the selected account. Each trap destination can use a different SNMPv3 user account for transmission.



5 Networking

Viewing Network Topology
Setting Static Routes
Using OneController Interfaces
Using OpenFlow

Viewing Network Topology

To view network topology, on the left navigation bar, click **Topology**. The **Topology** screen appears (see the following figure).

Note



You cannot add topology information on the **Topology** screen. Create the topology using the YANG UI. Topology information is stored in the database and appears on the **Topology** screen when switches connect to OneController using OpenFlow (see [Using OpenFlow](#) on page 64).

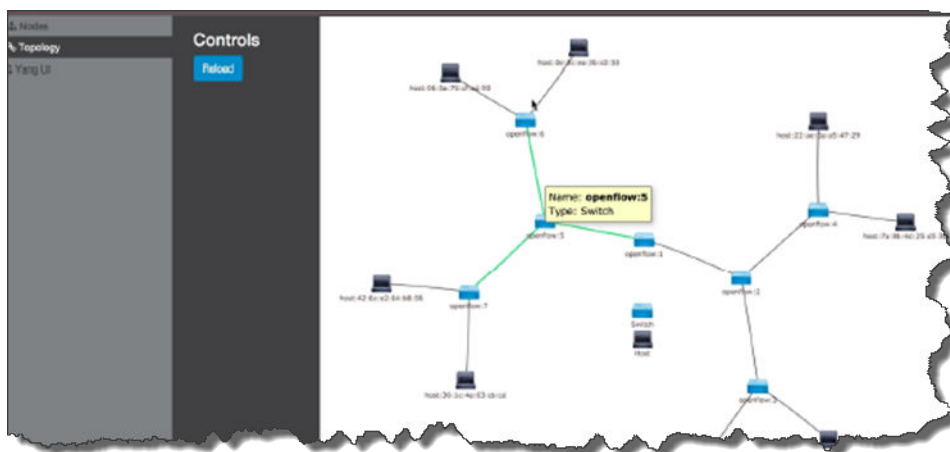


Figure 60: Topology Screen

- Blue boxes = switches
- Black boxes = hosts
- lines = connections
- To view source and destination ports, pause the pointer over hosts, links, and switches.
- To zoom in or out, use the mouse wheel.

Setting Static Routes

OneController has at least three interfaces (Admin, esa0, esa1). All of them can be in use. If you want to force all routable traffic out one specific port, you can define static routes for this. Static routes are defined by a triple of the target/destination address, netmask, and gateway address.

To set up a static route:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

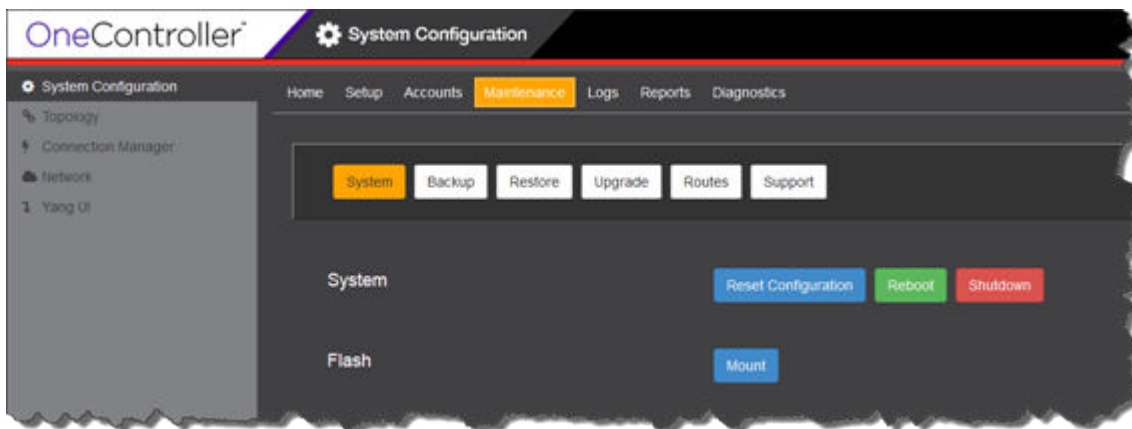


Figure 61: Maintenance—System Screen

- 2 Click **Routes**. The **Routes** screen appears (see the following figure).

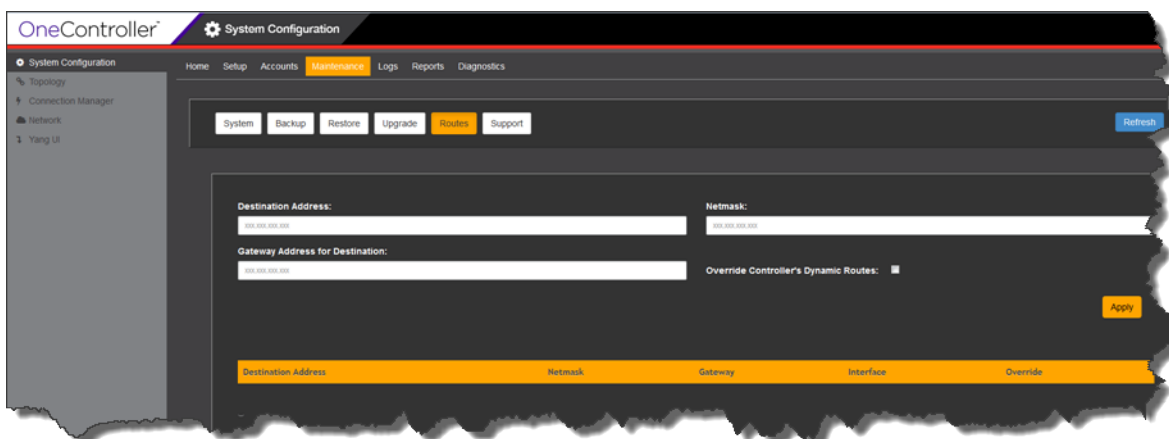


Figure 62: Maintenance—Routes Screen

- 3 Type information for the static route in the following boxes:

Option	Description
Destination Address	Target/destination address
Netmask	Netmask
Gateway Address for Destination	Gateway address of router to use (where each controller interface has its own router to use)

- 4 Leave **Override Controller's Dynamic Routes** unselected.
 5 Click **Apply**.

The static address appears in the lower table.

Using OneController Interfaces

OneController has the following interfaces.

Table 6: OneController Interfaces

Name		Speed		
OneC-V	OneC-A-600	OneC-V	OneC-V	Purpose
Admin	Eth0	1 GbE	10Gbps	Management
Esa0	Esa0	1 GbE	10Gbps	Data
Esa1	Esa1	1 GbE	10Gbps	Data
—	Esa2	1 GbE	10Gbps	Data

Ideally, you should have a dedicated management physical network or VLAN, which you connect to Admin/Eth0.

Generally, Esa0–2 interfaces should be used to connect OneController to your OpenFlow-capable switches for control communications and data traffic (see [Using OpenFlow](#) on page 64).

Using OpenFlow

About OpenFlow

ExtremeXOS OpenFlow

To implement OpenFlow, Extreme Networks has ported the Open Virtual Switch open source OpenFlow implementation to ExtremeXOS to create an OpenFlow 3.1-compliant solution.

Feature highlights include:

- **Ability to Dynamically Add OpenFlow**—ExtremeXOS is designed as an extensible operating system with an important resiliency capability that enables dynamic loading of new features without having to reboot or disrupt network operation, helping maintain system uptime.
- **Hybrid Mode Support for Both OpenFlow and Classic Ethernet Networks**—ExtremeXOS supports OpenFlow hybrid switch functionality. The default behavior for packets arriving on a switch port is to process the packet using standard Ethernet switching techniques (FDB learning and forwarding, ACL and QoS processing, VLAN isolation, and L3 routing). ExtremeXOS CLI commands are used to enable OpenFlow and to assign physical ports and LAGs belonging to specific VLANs to the OpenFlow domain for external control by an SDN controller. Extreme Networks switches support hybrid mode on a per VLAN basis. A single port can support both OpenFlow-controlled VLANs and VLANs with traditional networking services.
- **LAG for Resiliency and Redundancy ExtremeXOS**—OpenFlow supports LAGs for system redundancy and bandwidth scaling. ExtremeXOS represents an entire LAG as a single high capacity link to an SDN controller, enabling existing SDN applications to use the bandwidth scaling, load balancing, and resiliency characteristics of a LAG without being required to manage the individual member of the LAG directly. A LAG is used to incrementally increase bandwidth between switches as needed. For example, as a 1 GE port becomes oversubscribed, a second 1 GE port can be added into the LAG to increase the bandwidth between switches, without having to make the jump directly from 1 GE to 10 GE.
- **Hardware Queuing**—Extreme Networks' OpenFlow feature includes a rich set of OpenFlow-controlled QoS/slicing capabilities based on an extensive set of existing QoS capabilities. ExtremeXOS enables the definition of QoS profiles for OpenFlow packet egress queuing control. ExtremeXOS QoS profiles support rate limiting and rate shaping with single and dual rate QoS policies in addition to configurable drop policies. Using the ExtremeXOS CLI, interface queues are configured based on operator-defined service policies, and then assigned to physical ports. When those same physical ports are also configured as OpenFlow ports, the Extreme Networks switches report configured profile queues to the SDN controller with the Queue_Get_Config_Reply message. This enables the SDN controller to dynamically program the flows that are mapped to those configured queues, providing a rich set of traffic-differentiated services.
- **Automated Flow Management for Increased Flow Table Size**—ExtremeXOS OpenFlow fully supports platform-based hardware capabilities. ExtremeXOS intelligently classifies and maps controller flow-mods to the appropriate platform hardware resources to ensure maximum flow scaling. Complex flows requiring combinations of L2 and L3 match conditions are instantiated in platform TCAM ACL hardware. Simple L2-only flows are mapped to the more scalable platform L2 forwarding table. ExtremeXOS OpenFlow also fully supports OpenFlow idle_timeout and hard_timeout flow mods to evict flows from the hardware resources efficiently and effectively, allowing new flow entries as required.

Configuring Multiple SDN Controllers

ExtremeXOS allows you to configure up to two SDN controllers (designated the primary and secondary controllers). Both SDN controllers are active and control flows via a process negotiated between the controllers. *Out-of-band* control enables the SDN controllers to connect to switches using a non-OpenFlow VLAN.

Configuring two SDN controllers provides controller redundancy. If one SDN controller goes down or connectivity is lost, OpenFlow repeatedly attempts reconnection. If connectivity cannot be re-established, then the remaining SDN controller takes over all flow control.

OpenFlow Supported Platforms

OpenFlow is supported on the following platforms:

- Summit X440, X430, X460, X460-G2, X480, X670, X670-G2, and X770 series switches
- E4G-200 and 400 cell site routers
- BlackDiamond X8 with a single Management module
- BlackDiamond 8900 (XL-series) and C-series with single Management module only

OpenFlow Constraints and Limitations

The following list identifies limitations in this release that are the result of hardware restrictions:

- Supported platforms do not implement both packet and byte counters simultaneously on dynamic ACL entries. Only packet counters are supported in current implementation. Counters are not supported with FDB flows.
- IN_PORT, FLOOD, NORMAL, and TOS/DSCP editing actions are not supported.
- Flows implemented using ACL hardware have platform limitations on the simultaneous combinations of flow match conditions that can be supported. These limitations are described in each version of *ExtremeXOS Release Notes* under the ACL description section, and in the Flow Match combinations table later in this section. When receiving a flow match combination that cannot be supported with the platform's ACL hardware, the switch generates an OpenFlow error message to the controller.
- Flows implemented using FDB entries are subject to normal FDB constraints, including platform-dependent table sizes.
- FDB-based OpenFlow idle-timeout follows the configured FDB Aging Time.
- ExtremeXOS OpenFlow supports one physical table, and ingress table. The concept of an emergency flow table is not supported.
- OpenFlow 1.0 describes a "secure fail" model where a switch immediately removes all of its flows when it loses connectivity to its controller. ExtremeXOS implements an "open fail" mode. In this mode the switch maintains its existing flows after losing connectivity to a controller. The "open fail" model is required to support controller high availability solutions.
- High availability for controllers is available through the following two mechanisms:
 - Some controller clusters present a single IP address. The switch treats the cluster as a single controller.
 - Some controller clusters present multiple IP addresses. The switch connects simultaneously to primary and secondary controller targets and enables the controllers to manage failover.
- OpenFlow, XNV, and IDM are all features that enable an external agent to control resources on a switch. Due to their interaction models and resource requirements, these features are mutually exclusive. The ExtremeXOS OpenFlow implementation prevents these services from being simultaneously configured on the same port.



Note

There are other ExtremeXOS features that may not perform optimally when configured on OpenFlow enabled VLANs, or switch ports with OpenFlow supported VLANs. We make no attempt to prevent you from configuring additional services on these interfaces.

- MPLS and pseudowire instances are limited by platform capabilities.
- Failover not supported on stacks or chassis.

Setting Up OpenFlow

To set up OpenFlow on your switches:

- 1 Configure VLANs (see [Configuring VLANs](#) on page 67).
- 2 Set up Link Aggregation Groups (see [Configuring Link Aggregation Groups](#) on page 67).
- 3 Configure Quality of Service, if desired (see [Configuring Quality-of-Service \(QoS\)](#) on page 68).
- 4 Configure OpenFlow on switches (see [Configuring OpenFlow on Switches](#) on page 68).
- 5 Verify OpenFlow on switches (see [Verifying OpenFlow Configuration and Operation](#) on page 69).

Configuring VLANs

For the simplest OpenFlow setup, you need at least two VLANs: one to allow for control communications between OneController and the switches, and one for regular data traffic.

To create VLANs:

- 1 Log on to the desired switch. When the command prompt appears, type the following commands.
- 2 Type `configure vlan default delete portsport_list`, where `port_list` is the range of the ports that you want to configure the VLAN on.

This command removes ports from the default VLAN, so that you can then add them to the new VLAN.

- 3 Type `create vlan vlan_name`, where `vlan_name` is the name for the new VLAN.

This command creates the new VLAN.

- 4 Type `configure vlan vlan_name add ports port_list tagged | untagged`, where `vlan_name` is the name of the newly created VLAN, `port_list` is the range of ports to add to this VLAN, and you type either `tagged` or `untagged` as needed.

This command adds the ports deleted from the default VLAN to the newly created VLAN.

Configuring Link Aggregation Groups

LAGs allow you to combine (aggregate) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and allows you to provide redundancy if a link fails. It is highly recommended that you implement LAGs in your OpenFlow network to take advantage of the resiliency that LAGs provide.

- 1 Log on to the desired switch. When the command prompt appears, type the following commands.
- 2 Type `enable sharing port grouping port_list`, where `port` is the master logical port (LAG group ID) for the port group `port_list`.

This command defines a load-sharing group, or LAG, by assigning a group of ports to a single, logical port number.

Configuring Quality-of-Service (QoS)

If you want to set up Quality-of-Service (QoS) profiles, do this before setting up OpenFlow on your switches (see [Configuring OpenFlow on Switches](#) on page 68).



Note

QoS profiles should be configured prior to the switch registering with OneController. By default, most switches have already created QP1 and QP8.



Note

If OpenFlow queuing services are used, you must configure port QoS profiles.

The ExtremeXOS OpenFlow implementation provides basic QoS support by a simple queuing mechanism. Each queue is represented by an ExtremeXOS QoS profile. Queuing configuration and statistics can be queried by the OneController. Additionally, the enqueue action can be used to forward a packet through a queue attached to a port. When a switch registers with OneController, it notifies the OneController of the queues configured through QoS profiles.

To add a queue with a minimum bandwidth:

- 1 Log on to the desired switch. When the command prompt appears, type the following commands.
- 2 Type `create qosprofile qosprofile`. Where *qosprofile* is the name of the QoS profile that you want to configure (QP2-QP7).

This command creates a QoS profile QP2-QP7.

- 3 Type `configure qosprofile minbw minbw_number ports port_list`. Where *qosprofile* is the name of the QoS profile that you set up in the previous step, *minbw_number* is the desired minimum bandwidth expressed as a percentage (0-100%), and *port_list* is the list of ports for the QoS profile in the format 3-5, 2:5, 2:6-2:8 or All.

This command designates the minimum bandwidth for the QoS profile on the selected ports.

Configuring OpenFlow on Switches

To configure OpenFlow on your switches:

- 1 Log on to the desired switch. When the command prompt appears, type the following commands.
- 2 Type `configure access-list width double`.

This command configures the ACL (access control list) TCAM (telecommunications access method) as double wide. A double-wide ACL TCAM is preferred for OpenFlow to allow the use of longer match conditions.



Note

This command requires rebooting the switch to take effect, but you can wait until the end of this procedure to do this.

- 3 Type `enable openflow`.

This command enables OpenFlow on the switch.

- 4 Type `configure openflow controller primary out-of-band active ipaddress ipaddress vr vr_name`, where `ipaddress` is the IP address of the OneController and `vr_name` is the name of the virtual router the switch should use to communicate with OneController.

This command points the switch to OneController. You can configure up to two SDN controllers. See [Configuring Multiple SDN Controllers](#) on page 65.

- 5 Type `enable openflow vlan vlan_name`, where `vlan_name` is the name of the VLAN that you created previously (see [Configuring VLANs](#) on page 67).

This command enables OpenFlow control on the specified VLAN.

- 6 Type `enable openflow tables fdb on`.

This command enables FDB entries, allowing flows to use FDB entries, which permits scaling to 128,000 flows. FDB entries are disabled by default, limiting flows to ACLs exclusively. However, FDB flows are much simpler—they match only VLAN and destination MAC addresses with only redirect as an action.

- 7 Restart the switch.

Verifying OpenFlow Configuration and Operation

You can verify the OpenFlow setup using the following commands.

To verify that OpenFlow is enabled correctly on the switch, type:

```
show openflow
```

The following sample output of the command shows that the switch has OpenFlow enabled, that FDB is on, and that the ACL width is double.

```
* (Private) SDN-1.1 # show openflow
OpenFlow:           Enabled
Versions:           OpenFlow10, OpenFlow13
Mode:               Standard
FDB:                On
Access-list width: Double
```

```
Controller          : Primary
  Status             : ACTIVE
  Datapath ID        : 00000004968374d4
  VR                  : VR-Default
  Mode                : out-of-band Active
  Target              : tcp:10.66.65.242:6633
  Uptime(secs)       : 1134555
```

```
Controller          : Secondary
  Not configured.
```

VLAN	VID	Flows	
		Ports	Active Error
major	4089	3	2 0

```
Total number of VLAN(s): 1
```

To verify the setup of OneController on the switch, type:

```
show openflow controller {primary | secondary}
```

The following sample output of the command shows that the switch has a primary OneController (but no secondary controller), located at 10.66.65.242, and that it is communicating with OneController through the virtual router "VR-Default."

```
* (Private) SDN-1.2 # show openflow controller
Controller      : Primary
  Configured    : Yes
  Datapath ID   : 00000004968374d4
  VR            : VR-Default
  Mode          : out-of-band Active
  Target        : tcp:10.66.65.242:6633
  Status        : ACTIVE          TLS           : Disabled
  Probe(secs)  : 30              Uptime(secs) : 1135034
  Rate Limit   : 1000           Burst Size    : 250
  Packets Sent : 348705         Packets Received : 274586

Controller      : Secondary
  Configured    : No
```

To view the number of flows on the switch so that you can ensure that it is not exceeding the capacity of the switch, type:

```
show openflow flows
```

The following sample output of the command shows that the switch has two flows.

```
* (Private) SDN-1.3 # show openflow flows
Total number of flows: 2

Flow name      Type Duration (secs)      Prio Packets
-----
of_48          ACL      172915      10      172913
  Match:      Input Port:      14
             Src MAC:      00:0c:29:02:10:d3
             Dst MAC:      00:0c:29:80:ac:0a
             Ethernet Type: 0x0800
  Actions:    output:10, cookie:0x2000000000000000, idle:5:4
of_49          ACL      172915      10      172913
  Match:      Input Port:      12
             Src MAC:      00:0c:29:80:ac:0a
             Dst MAC:      00:0c:29:02:10:d3
             Ethernet Type: 0x0800
  Actions:    output:14, cookie:0x2000000000000000, idle:5:4
```

6 Diagnostics

OneController Reports and Logs
Network Diagnostics Overview
Creating TAC Diagnostic Files

OneController Reports and Logs

OneController provides information about itself in the form of logs (see [Viewing OneController Logs](#) on page 73) and reports (see [Viewing OneController Reports](#) on page 71).

Viewing OneController Reports

OneController provides system and manufacturing information reports about itself.

To view OneController reports:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Reports**. The **Report** screen appears (see the following figure).

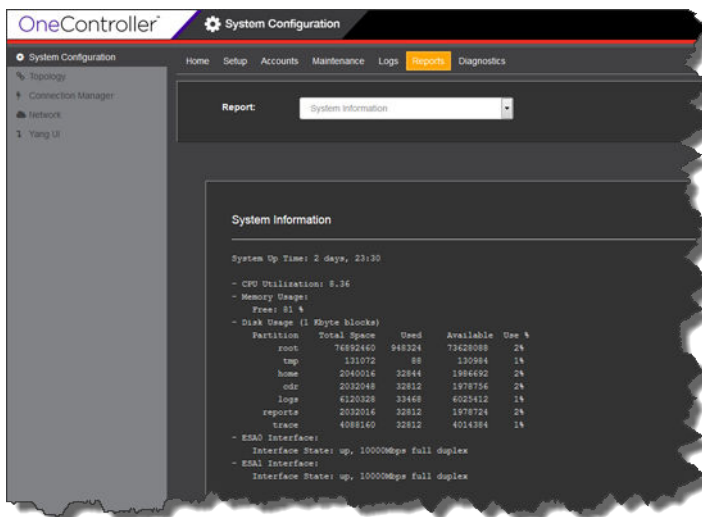


Figure 63: Report Screen—System Information Report

The **System Information** report appears by default showing:

- System up time
- Memory usage
- Disk usage
- Interface information

- To view the **Manufacturing Information** report, select **Manufacturing Information** from the **Report** list. The **Manufacturing Information** report appears (see the following figure).

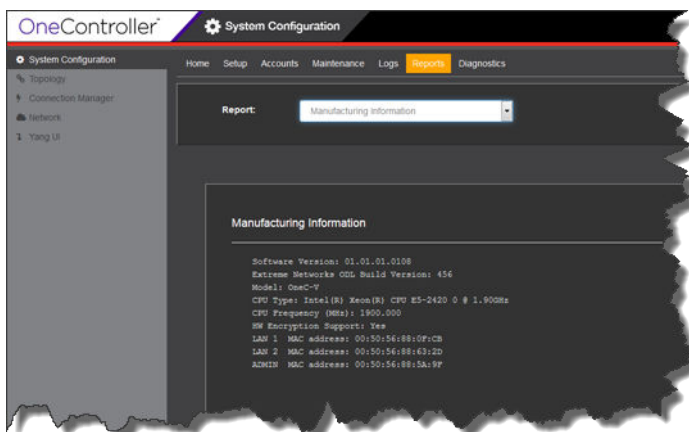


Figure 64: Report Screen—Manufacturing Information Report

The **Manufacturing Information** report displays the following information:

- Software version
- Extreme Networks ODL build version (build number for the Java/ODL part of OneController)
- Model type: OneC-V (virtual machine) or OneC-A-600 (hardware appliance)
- CPU type and speed
- If hardware encryption is supported
- ESA0, ESA1, and management port MAC addresses

Viewing OneController Logs

OneController displays Syslog messages from the `/var/log/messages` directory.

To view OneController Syslog messages:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Logs**. The **Logs** screen appears (see the following figure).

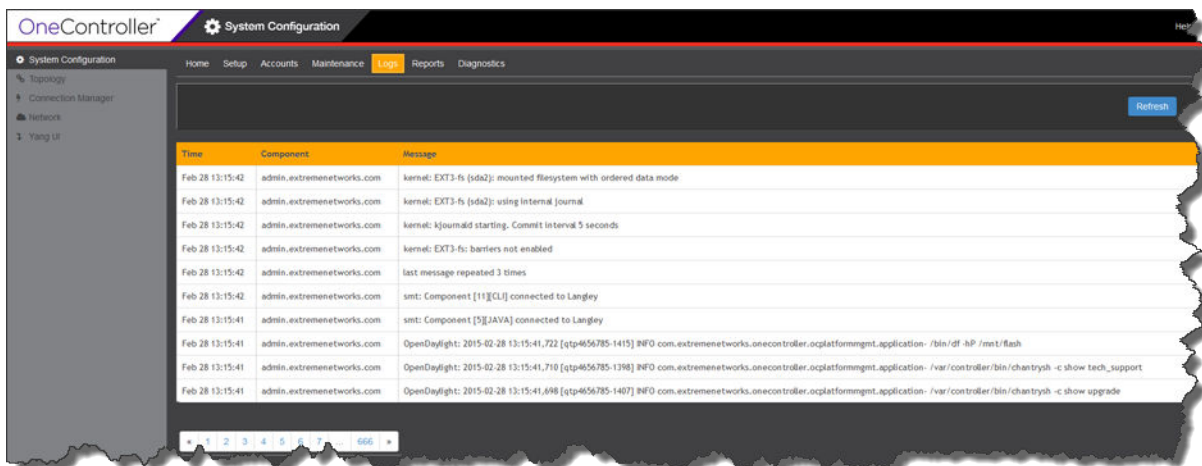
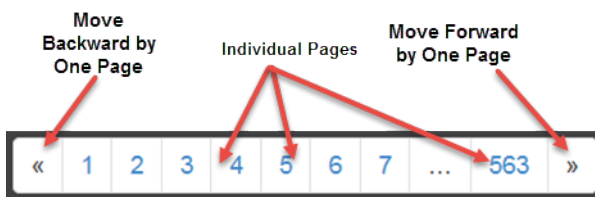


Figure 65: Logs Screen

Syslog messages appear, ten on a page, starting with the most recent one.

- 2 Use the page controls to view the list of logs.



Network Diagnostics Overview

OneController provides ping (see [Ping](#) on page 75) and traceoute (see [Traceroute](#) on page 76) capabilities, so that you can check reachability and obtain route information to help you test and troubleshoot your network setup.

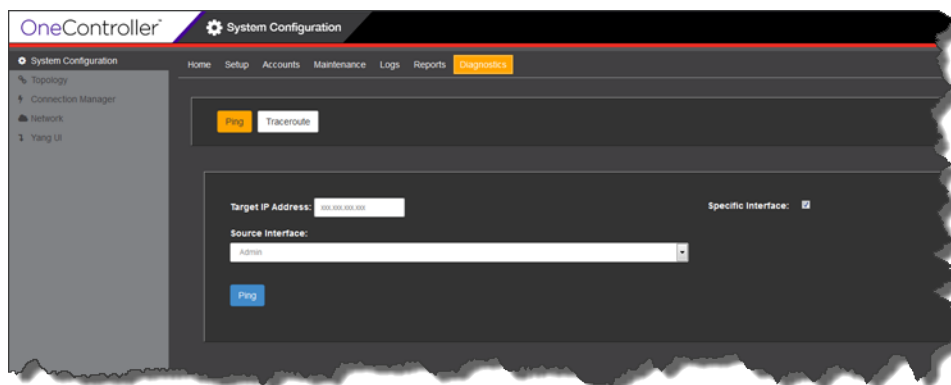


Figure 66: Diagnostics Screen—Ping

Ping

Ping allows you to test the reachability of devices on an Internet Protocol (IP) network and to measure the round-trip time for messages sent and records any packet loss for the ping packets from OneController.

To ping from OneController:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Diagnostics**. The **Diagnostics** screen appears (see the following figure).

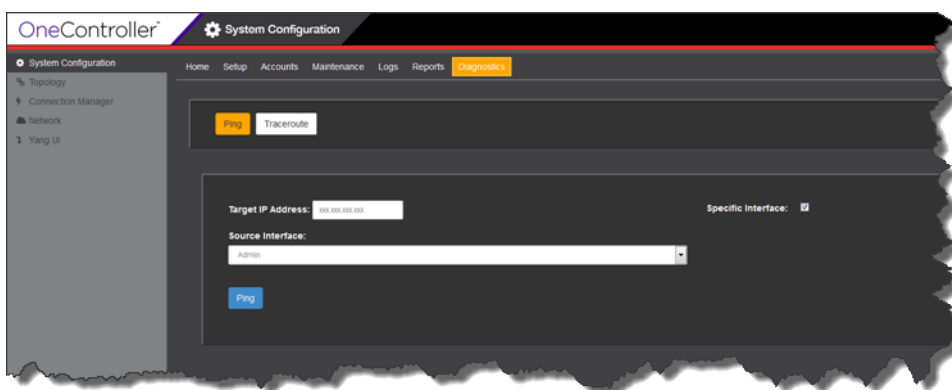


Figure 67: Diagnostics Screen

- 2 Click **Ping**.
The **Diagnostics Ping** screen appears (see previous figure).
- 3 In the **Target IP Address** box, type the IP address of the device that you want ping.
- 4 To send the ping from a specific OneController interface, select the **Specific Interface** check box, and then select the interface from the **Source Interface** drop-down list: **Admin**, **esa0**, **esa1**, **eas2** (OneC-A-600 only).

5 Click **Ping**.

The ping results appear below (see the following figure).

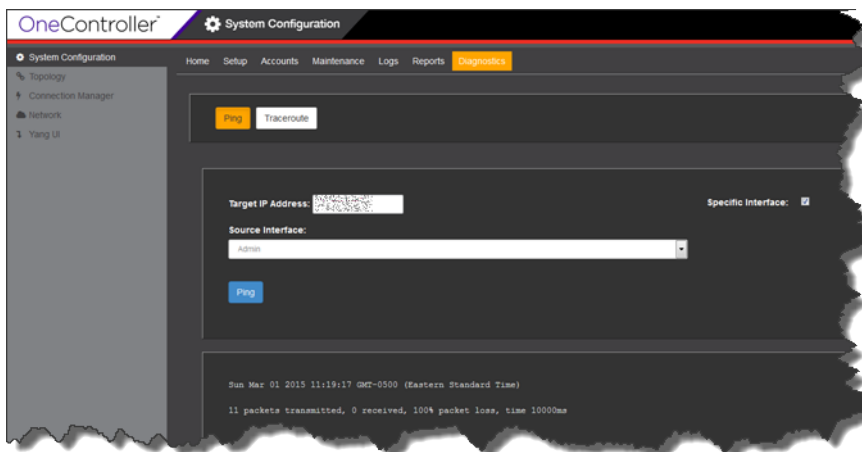


Figure 68: Diagnostics Screen—Ping (Ping Results)

Traceroute

Traceroute allows you to display the route (path) and measure transit delays of packets across an Internet Protocol (IP) network. The trace of the route appears as the round-trip times of the packets received from each successive device (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated.

To run traceroute from OneController:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Diagnostics**. The **Diagnostics** screen appears (see the following figure).

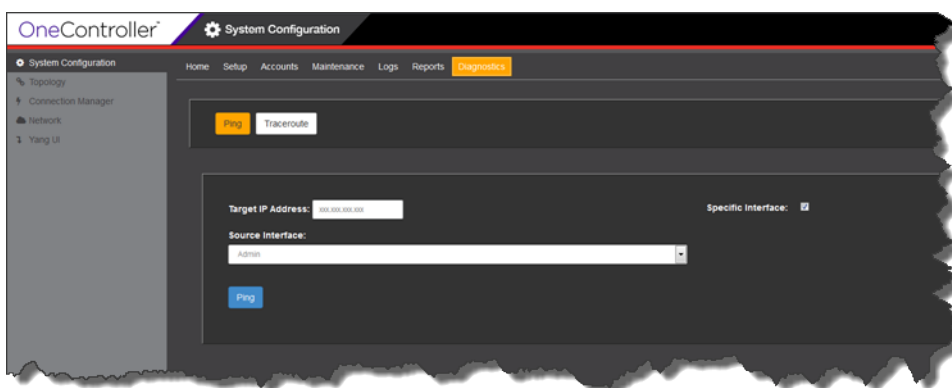


Figure 69: Diagnostics Screen

- 2 Click Traceroute.

The **Diagnostics Traceroute** screen appears (see the following figure).

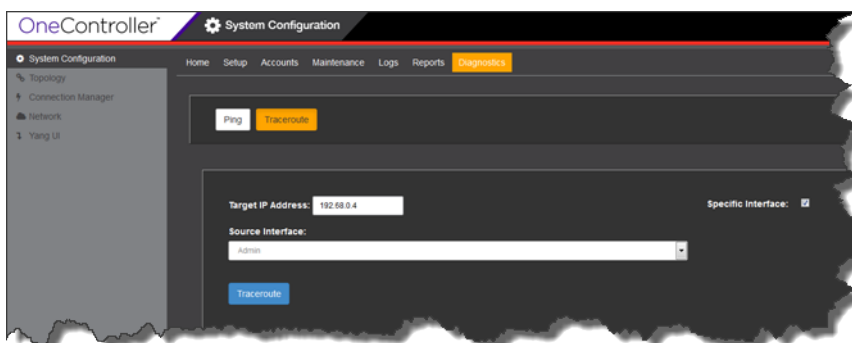


Figure 70: Diagnostics Traceroute Screen

- 3 In the **Target IP Address** box, type the IP address of the device that you want to run the traceroute to.
- 4 To run traceroute from a specific OneController interface, select the **Specific Interface** check box, and then select the interface from the **Source Interface** drop-down list: **Admin**, **esa0**, **esa1**, **esa2** (OneC-A-600 only).
- 5 Click **Traceroute**.

The traceroute results appear below (see the following figure).

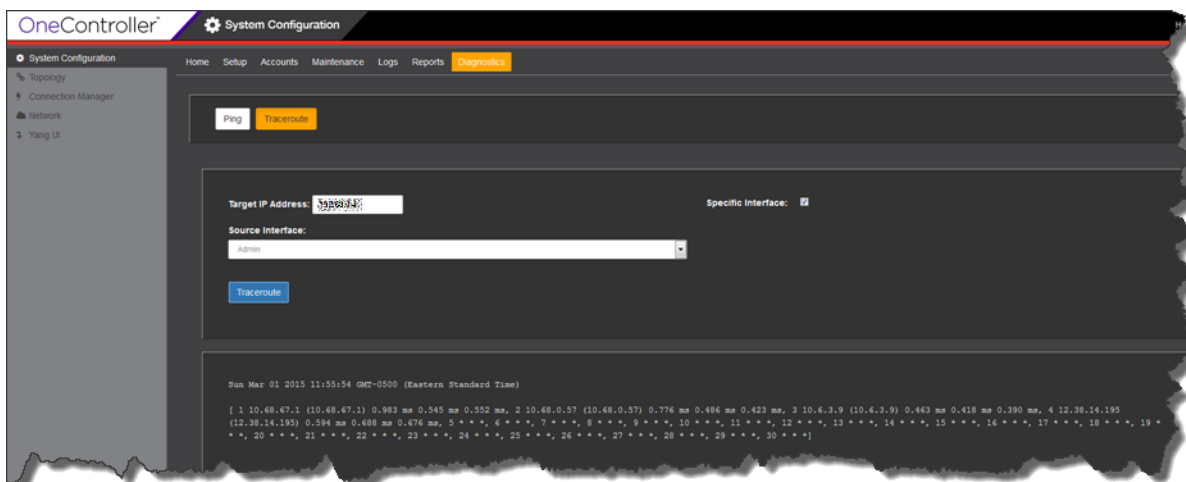


Figure 71: Diagnostics Traceroute Screen (Results)

Creating TAC Diagnostic Files

To aid in troubleshooting OneController, you can create a diagnostic file for the Extreme Networks TAC. This captures application, platform logs, configuration, and packages information in a tar.gz compressed file.

To create a diagnostic file:

- 1 On the left navigation bar, click **System Configuration**, and then, on the menu bar, click **Maintenance**. The **Maintenance System** screen appears (see the following figure).

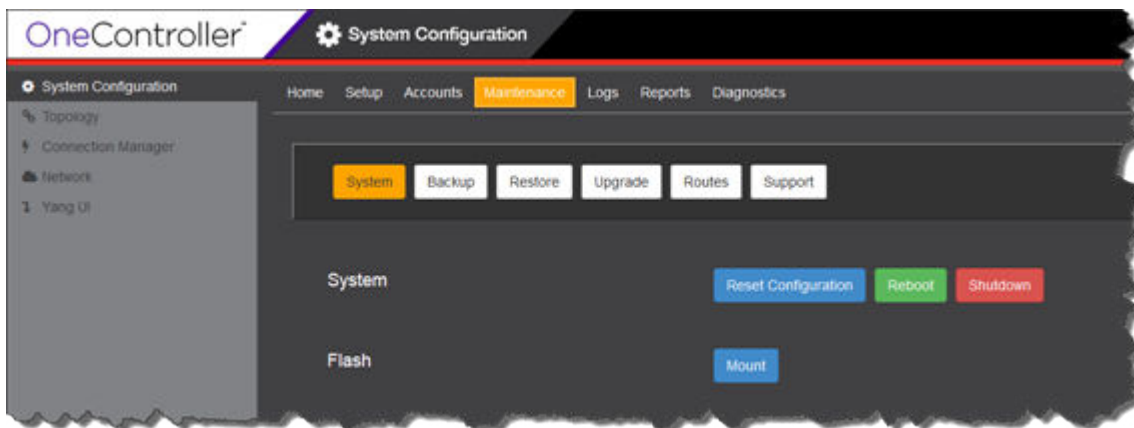


Figure 72: Maintenance System Screen

- 2 Click **Support**. The **Maintenance Support** screen appears (see the following figure).

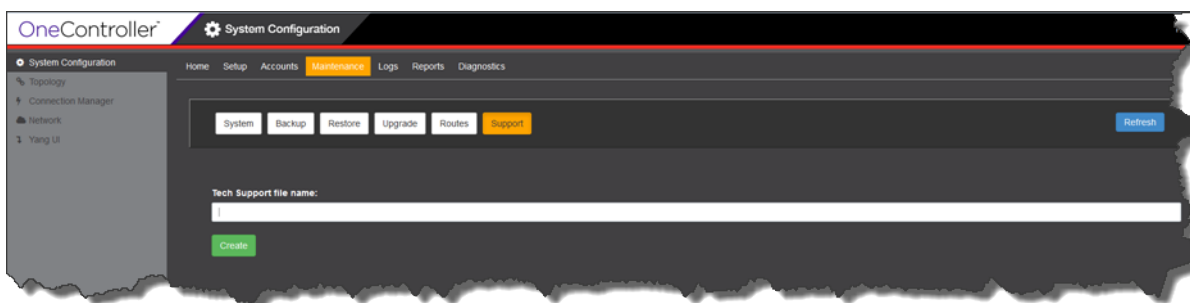


Figure 73: Maintenance Support Screen

- 3 In the **Tech Support File name** box, type the desired name for the resulting file.

4 Click **Create**.

The created file appears in the **Available Technical Support Files** table (see the following figure).

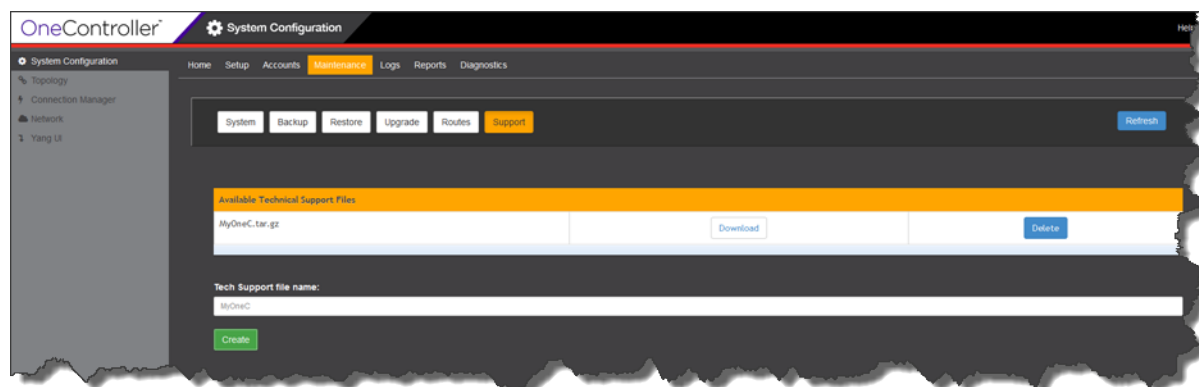


Figure 74: Maintenance Support Screen with Support Files

5 To download the file from OneController to your local machine, click **Download** next to the file, and save or open the file, as desired.

If you want to delete any of the support files, click **Delete** next to the desired file.