

Juniper vLabs User Guide

v1.7

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.
Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.
The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://www.juniper.net/support/eula/>.
By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper vLabs User Guide
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

Table of Contents

Table of Contents	2
Juniper vLabs Overview	3
Introduction	3
Prerequisites	3
Other Resources	3
Starting a Session	3
Launch a Topology	3
Verify your Time Zone	4
Reserve a Session	5
Verify the Sandbox is Ready to Use	6
Access The Sandbox	6
Accessing Resources (Devices) in a Sandbox	7
Accessing a Device via SSH in the Web Browser	7
Accessing a Device via SSH Using Local Tools	7
Accessing a Device via HTTPS	9
Accessing a Device Through its Console Port	11
Managing Active Sandbox Reservations	13
Extending a Sandbox Reservation	13
Ending a Sandbox Reservation	13
Monitoring/Troubleshooting Sandbox Resources	14
Monitoring Resource Health	14
Restarting a Resource	15
Reinitializing a Resource	15
Usage Notes	16
Restarting a Sandbox	16
Support	16

Juniper vLabs Overview

Introduction

Juniper vLabs is a web-based platform that provides a place to test drive Juniper products and solutions at any time in a safe, sandbox environment. Leveraging several Juniper product lines, vLabs provides a variety of pre-configured topologies covering routing, switching, security, automation, and network management and analytics. Reservable both in advance and on-demand, vLabs sessions are free and open to everyone with a Juniper account.

vLabs topologies were created by assembling resources (virtual devices, etc.) into *blueprints*. When you reserve and start up a blueprint topology, it becomes an active topology—or *sandbox*—with running resources you can access, configure, send traffic, etc. The automated setup procedure typically takes about 15 minutes.

Prerequisites

The Juniper vLabs environment has the following prerequisites:

- A Juniper account (sign-up instructions are [here](#))
- A Web browser. Juniper vLabs was tested using Mozilla Firefox and Google Chrome, but should generally work with any web browser. There is no need for any plug-ins, etc.
- (Optional) Local SSH clients. You can use these tools to access sandbox resources directly (once enabled)

Other Resources

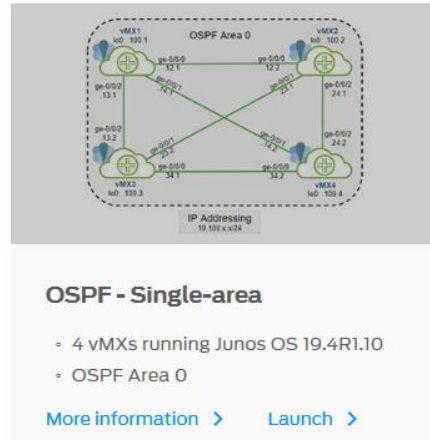
Be sure to also check out the [How-to Videos](#).

Starting a Session

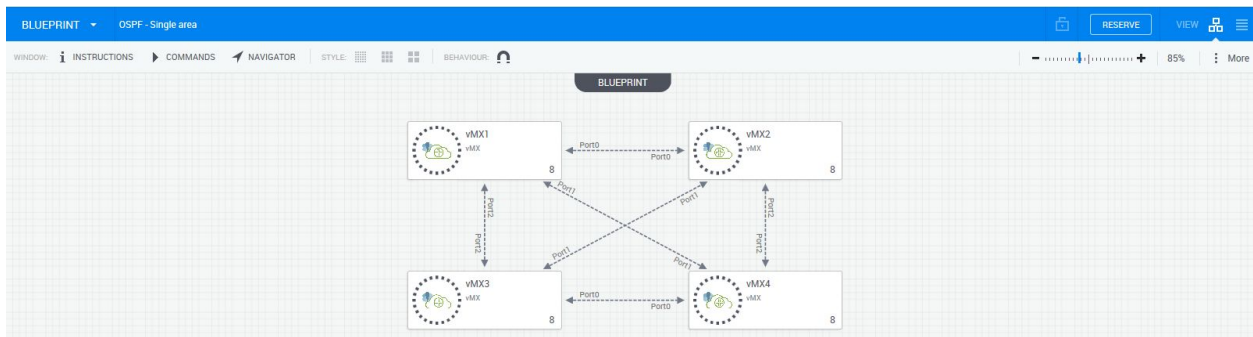
This section describes the steps to start a sandbox session.

Launch a Topology

On the [Topology catalog](#) page, browse the list and click **Launch** for the desired topology.

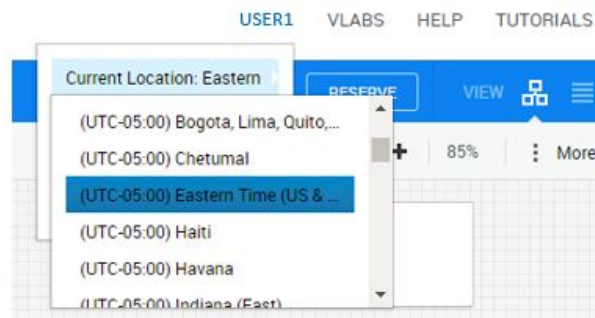


You should now see the topology in the vLabs UI as a blueprint.



Verify your Time Zone

By default, your time zone is set to UTC. Change the time zone by clicking your username at the upper right of the vLabs UI.

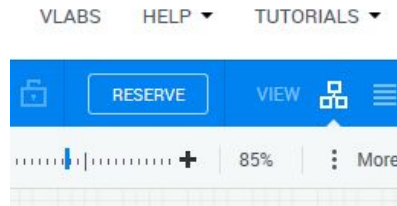


Once you select your timezone, any reservations you make will be based on this timezone.

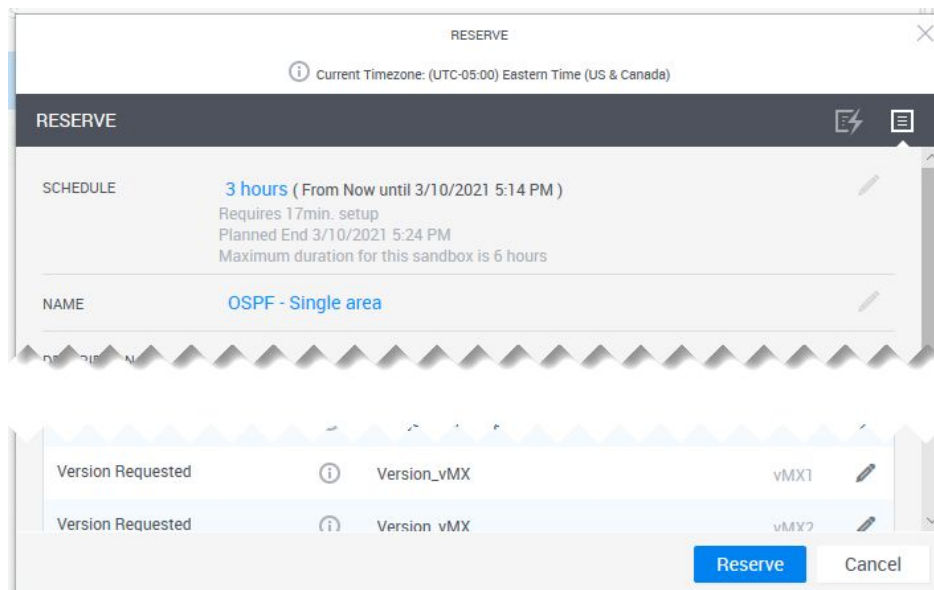
NOTE: If you clear your browser cache, this setting will be reset to UTC.

Reserve a Session

In the vLabs UI, you start a session by making a reservation. Click the **RESERVE** button at the upper right of the UI.



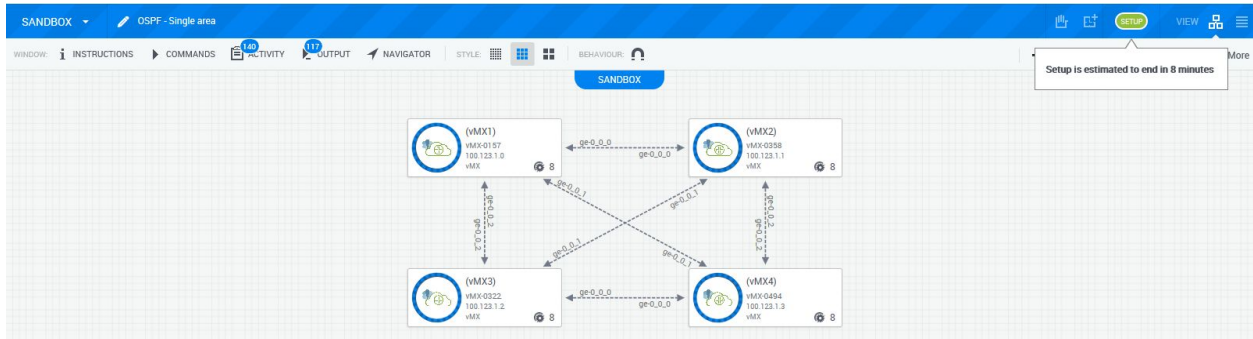
In the Reserve window that appears, only the first section—**SCHEDULE**—requires your attention. By default, the session will start immediately and run for three hours. If you wish to change the start date, start time, or session length, alter them as needed. Then click **Reserve** at the bottom of the window.



NOTE: Do not change any fields related to a device's software version. While these are text-editable fields, changing them will cause the devices to have issues on startup.

The sandbox setup process then begins. There are several indicators to confirm that your sandbox is being setup:

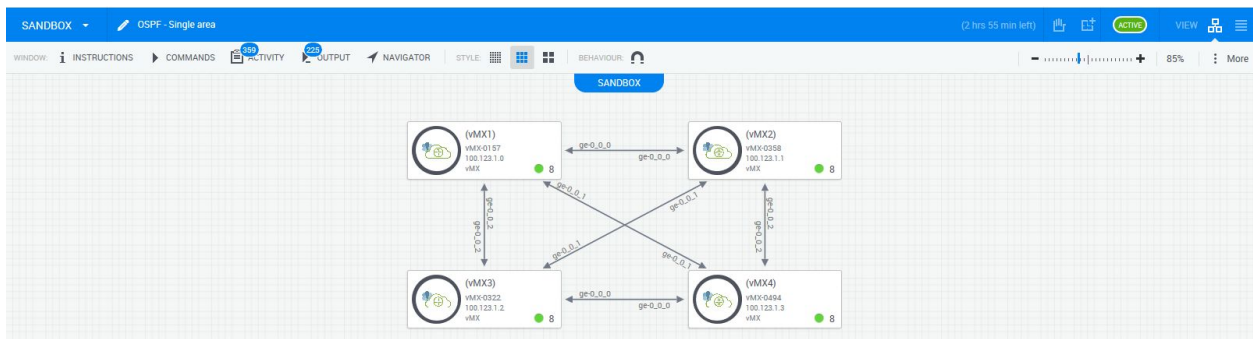
- A status icon in the upper right corner of the interface indicates the status as **Setup**. Hover your mouse over this icon to receive the estimated amount of time needed to complete the setup process.
- The *Sandbox* header changes to a striped pattern.
- The resources in the sandbox have a moving circle around them.
- You receive an email indicating the setup process has started.



Verify the Sandbox is Ready to Use

There are several indicators to confirm that your sandbox is setup and ready to use:

- The status icon in the top right corner changes from **Setup** to **Active**.
- You receive an email indicating the sandbox is ready for use.
- The resources have a small green circle at their bottom-right corner.



Access The Sandbox

If you are currently in the vLabs UI and the sandbox shows ACTIVE, you are all set! If you don't have the page open, you can access it through the email you receive when the sandbox is ready to use.

ACCESSING YOUR SANDBOX

Access your vLab sandbox [here](#).

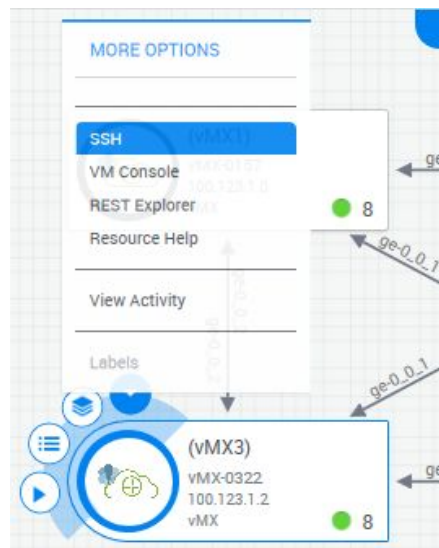
Accessing Resources (Devices) in a Sandbox

Accessing a Device via SSH in the Web Browser

You can open an SSH session to devices in your vLab sandbox (once it is active) through the Web browser.

To access a resource through the Web browser:

1. Mouse over the icon for the resource. Multiple icons appear.



2. Click the **down arrow** icon.
3. Select **SSH** from the menu. A new browser tab opens using an SSH connection to the out-of-band management interface.

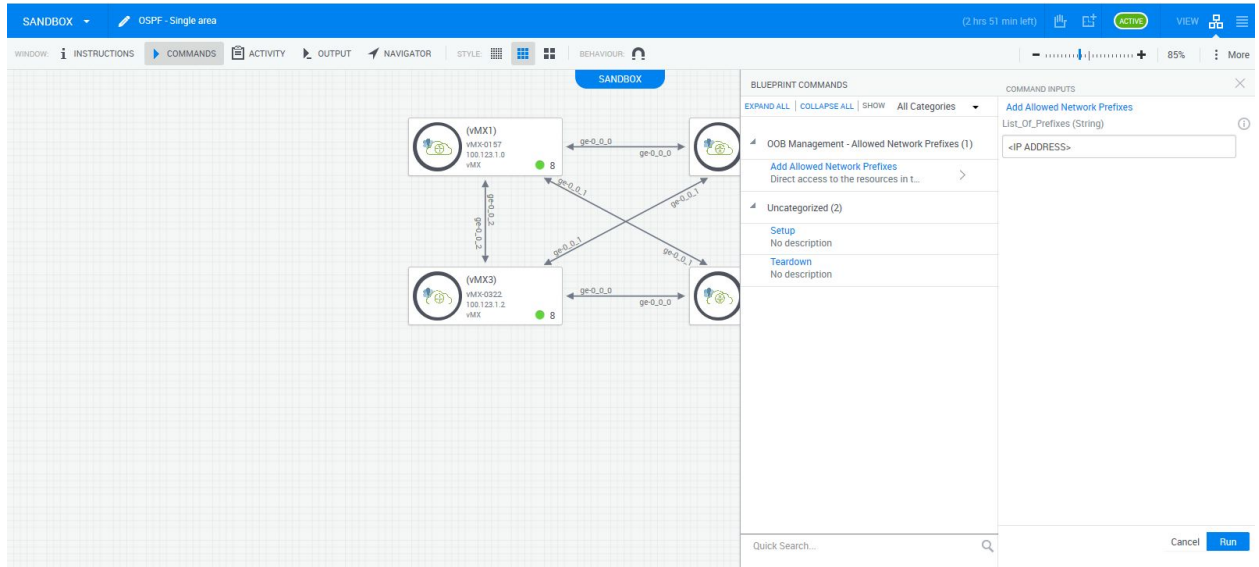
NOTE: If the device has a graphical interface, see the section [Accessing a Device via HTTPS](#) below.

Accessing a Device via SSH Using Local Tools

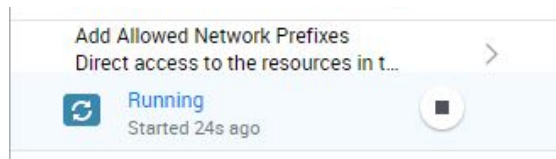
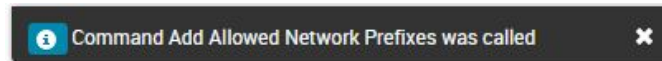
You can also access devices in your vLab sandbox directly, using a local SSH tool. To use this option, you must adjust the sandbox's firewall rules to allow your machine to connect directly to the devices.

To enable 'direct access':

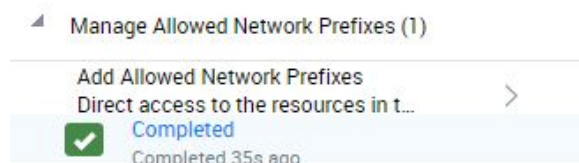
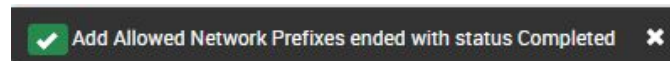
1. Open a new browser tab and do a Google search for "what is my ip". Copy the displayed IP address.
2. In the vLabs UI, click on **COMMANDS** in the toolbar.



3. Find the **Add Allowed Network Prefixes** option and click the **>**.
4. Enter your IP address in the **List_of_Prefixes** field.
NOTE: Only IPv4 addresses are supported.
5. Click the **Run** button.
6. The interface shows a banner at the top-center of the screen, and the Blueprint Commands area shows **Running** while the script is doing its work.

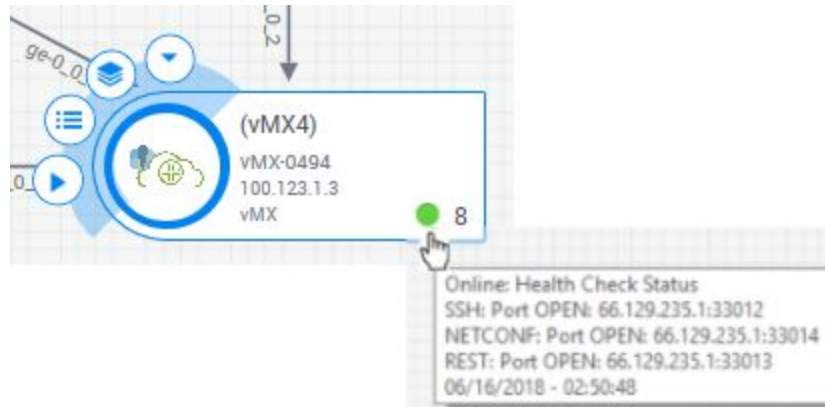


7. When the script is complete, the interface shows a banner at the top-center of the screen, and the Blueprint Commands area shows **Completed**. You will also receive a confirmation email.



You can now access the devices:

1. In the vLabs UI, choose a device and hover your mouse over the green circle. Copy down the SSH IP address and port information for the next step.



2. In your local SSH tool, add a new connection to this address/port.
3. Open a connection and enter the device login credentials. You should gain access to the device.

```
Last login: Fri Jan 24 22:51:37 2020 from 66.129.235.126
--- JUNOS 19.4R1.10 Kernel 64-bit JNPR-11.0-20191115.14c2ad5_buil
jcluser@vMX4> █
```

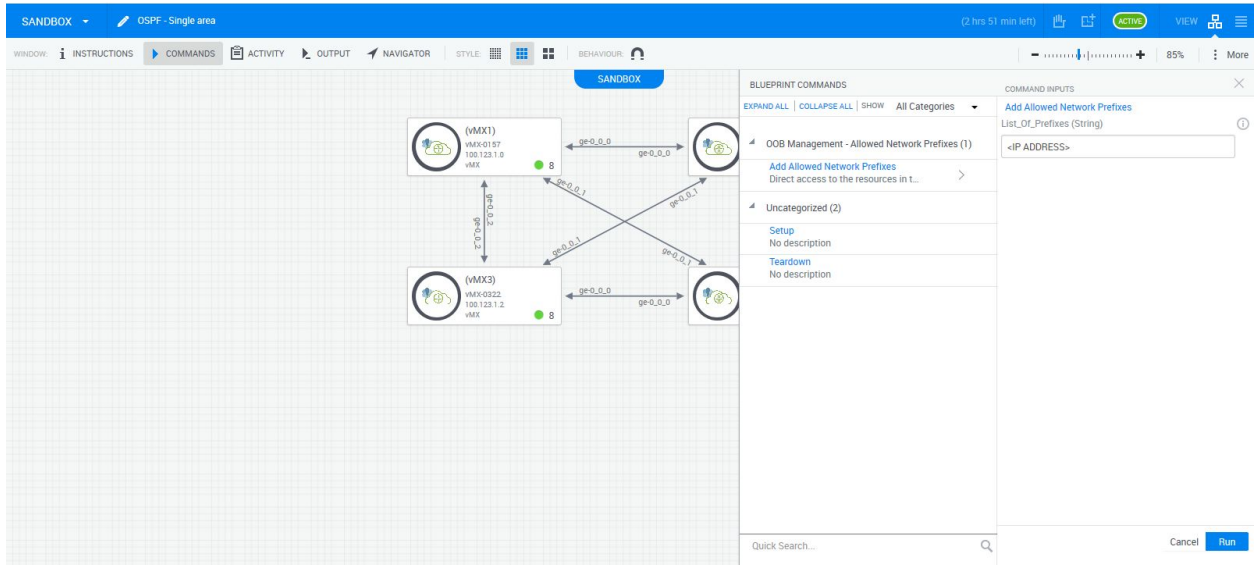
4. Repeat these steps for each device in the sandbox.

Accessing a Device via HTTPS

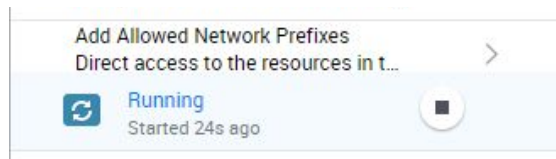
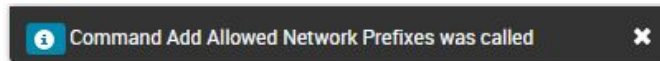
You can also use HTTPS to access some devices. For example, some Junos devices have J-Web browser access, while management solutions like Security Director and Apstra Fabric Conductor are GUI-based platforms. To use this option, you must first adjust the sandbox's firewall rules to allow your machine to connect directly to the devices.

To enable 'direct access':

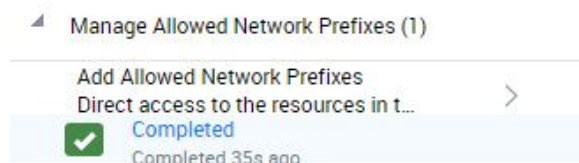
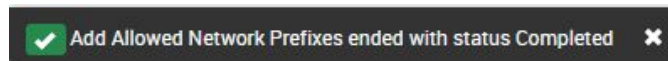
1. Open a new browser tab and do a Google search for "what is my ip". Copy the displayed IP address.
2. In the vLabs UI, click on **COMMANDS** in the toolbar.



3. Find the **Add Allowed Network Prefixes** option and click the **>**.
4. Enter your IP address in the **List_of_Prefixes** field.
NOTE: Only IPv4 addresses are supported.
5. Click the **Run** button.
6. The interface shows a banner at the top-center of the screen, and the Blueprint Commands area shows **Running** while the script is doing its work.

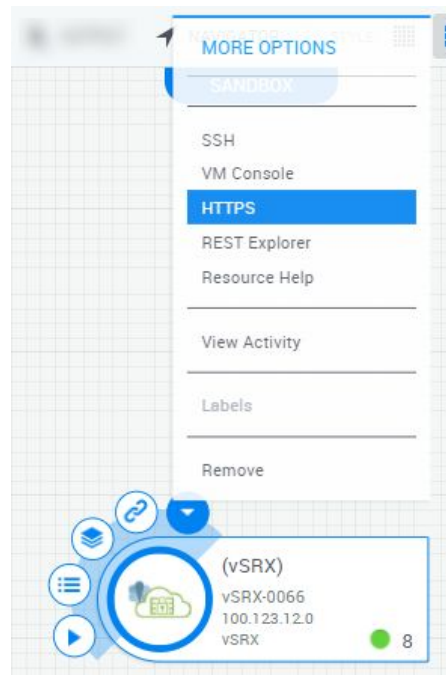


7. When the script is complete, the interface shows a banner at the top-center of the screen, and the Blueprint Commands area shows **Completed**. You will also receive a confirmation email.



You can now access the devices:

1. Mouse over the icon for the resource. Multiple icons appear.



2. Click the **down arrow** icon.
3. Select the **HTTPS** option (or equivalent - the option for GUI-based products can vary) from the menu. A new browser tab opens using an HTTPS connection to the out-of-band management interface.

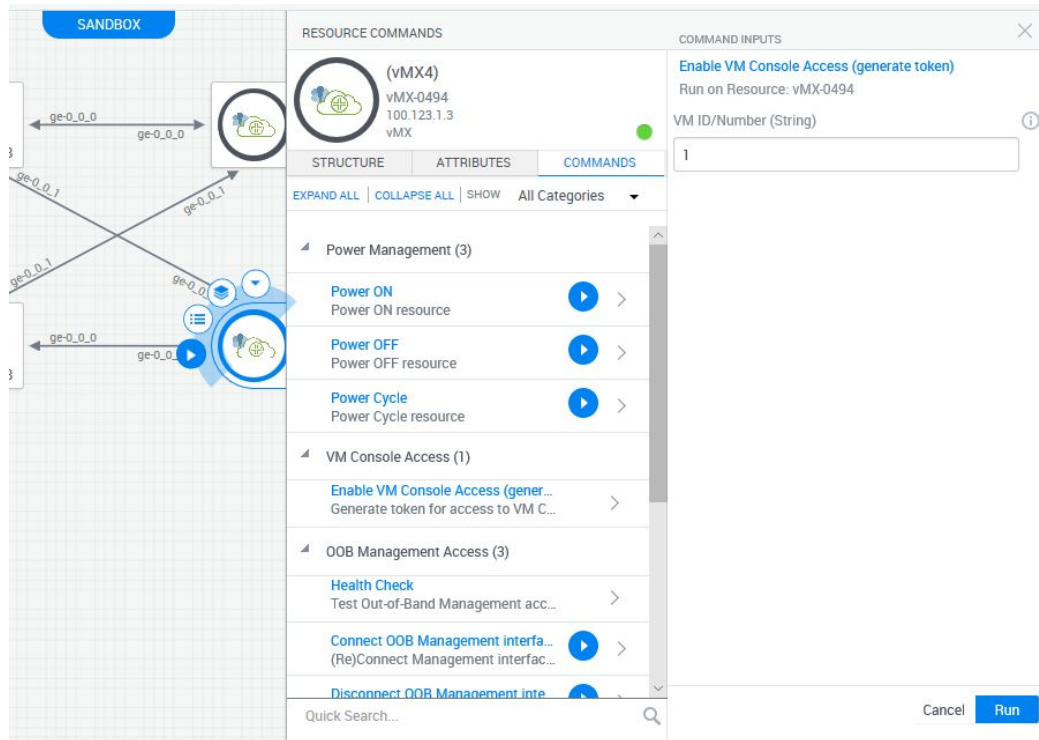
Accessing a Device Through its Console Port

While not typically needed, you can enable console port access to a device. This option can be especially useful if you accidentally delete or overwrite a device's management interface configuration.

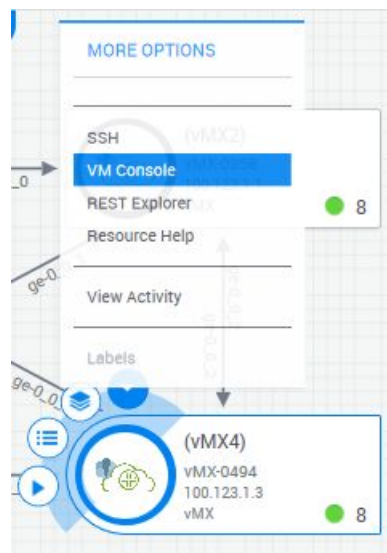
In the vLabs environment, a token is needed to enable console access; if you try to log in to a VM console before generating this token, a new browser tab will open with a message indicating your login attempt is invalid.

To create VM console access to a resource:

1. Mouse over a resource to select it.



2. Click the right arrow *Commands* button. The *Resource Commands* box appears on the right side of the vLabs UI.
3. Find *Enable VM Console Access* and click the >. Then click the **Run** button.
4. Once the token is generated, you can access the VM console login by selecting **VM Console** from the resource's drop-down menu.



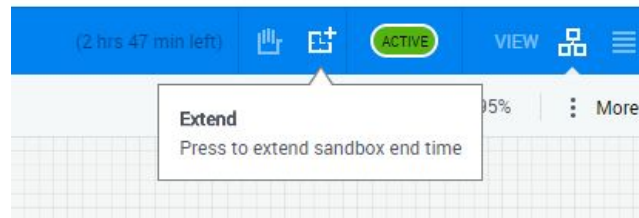
5. In the new browser tab that opens, click in the black area and press the **Enter** key once or twice to get a device login prompt.
Login credentials are the same as used for SSH access.

Managing Active Sandbox Reservations

Extending a Sandbox Reservation

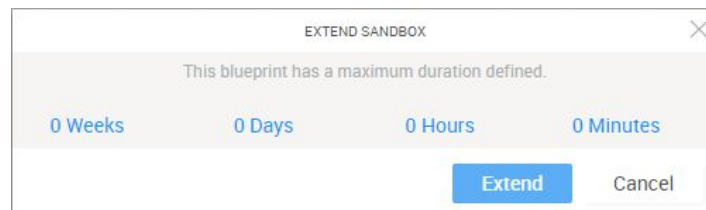
To extend a sandbox reservation:

1. Click the **Extend** icon in the upper right corner of the interface.



2. In the window that appears, click the blue text fields and select the amount of time that you wish to extend the reservation and click **Extend**.

NOTE: The maximum session time is currently six hours.

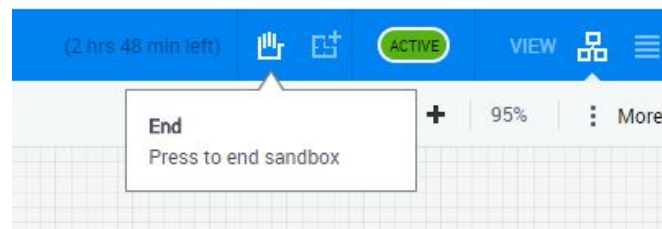


Ending a Sandbox Reservation

A sandbox session will automatically shut down at the reservation end time, or you can manually end it.

To manually end a sandbox reservation:

1. Click the **End** icon in the upper right corner of the interface.

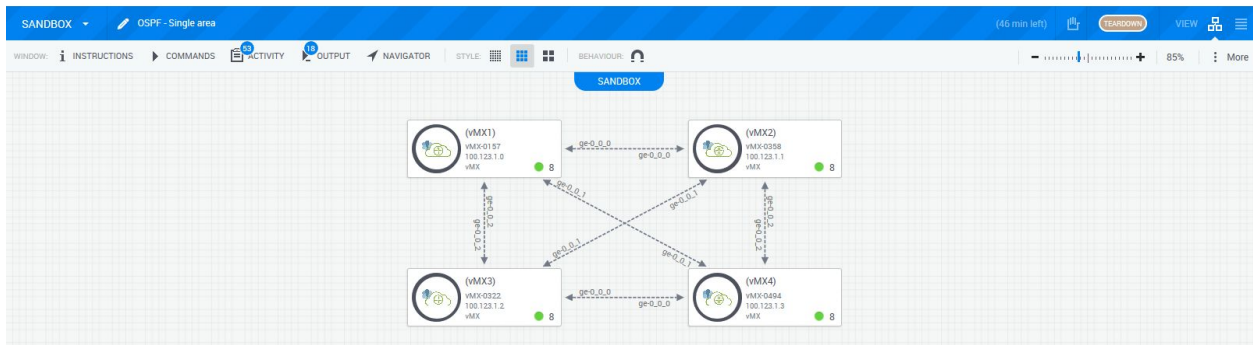


2. In the window that appears, click **OK**.



The following elements confirm the teardown procedure is in progress:

- *The sandbox ending process has started* message is visible in the middle of the interface.
- The status icon in the top right corner indicates **TEARDOWN**.
- You receive an email indicating the sandbox session is ending.



NOTE: You can close the browser after confirming the teardown procedure has started; you do not need to wait for the process to finish.

Monitoring/Troubleshooting Sandbox Resources

Monitoring Resource Health

The health status of each individual resource in any sandbox can be monitored using the health status icon. The health status icon is in the bottom right corner of every resource in a sandbox.

The colors of the health status icon include:

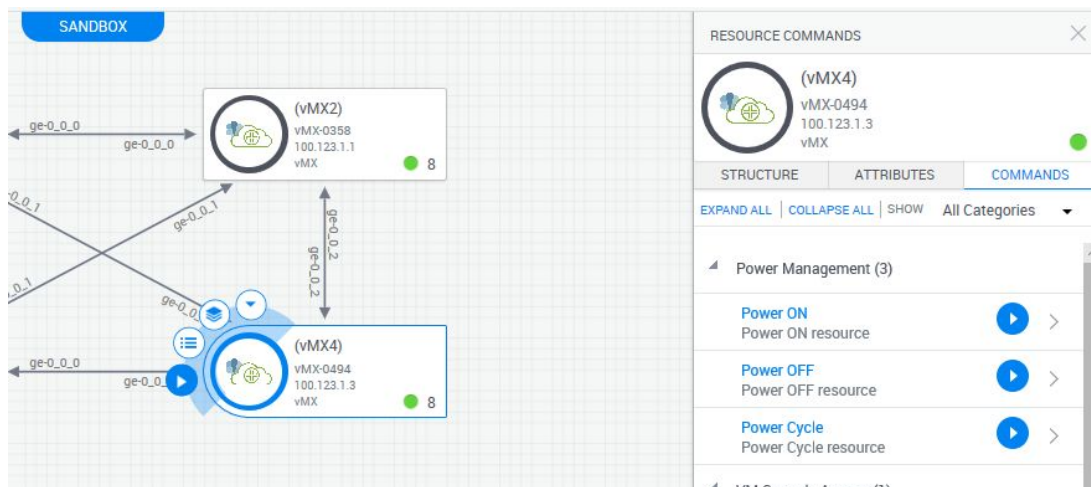
- Green: resource is up and running normally
- Partial green: resource is up, but not all access ports (SSH, HTTPS, etc.) are enabled
- Red or grey: resource has a problem



Restarting a Resource

On occasion, a sandbox resource may not start up properly. While the fix is typically to end and restart the entire sandbox, sometimes restarting just the device can solve the problem.

Resources in a sandbox can be power cycled using the *Power Management* commands. These commands can be accessed by hovering your mouse over the resource and clicking the right arrow (*Commands*) button.

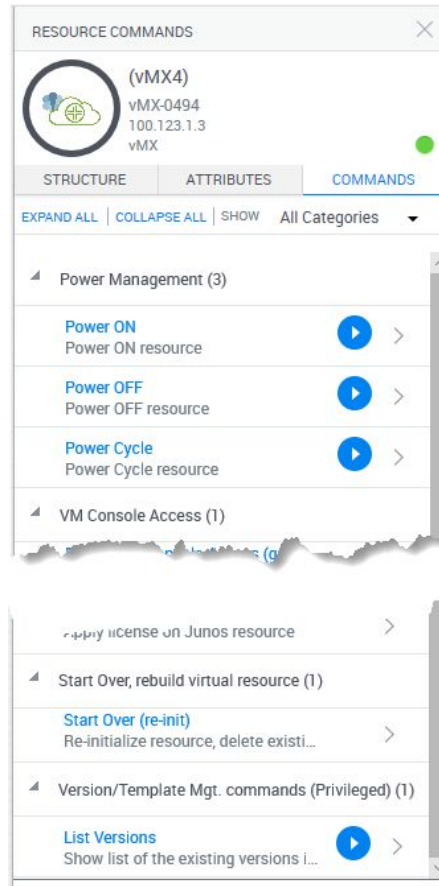


In the Resource Commands section, select the appropriate **Run** button to power on, power down, or power cycle a resource.

Reinitializing a Resource

Another option to 'reset' a sandbox resource that has not started up properly is to re-initialize it, that is, completely tear it down and restart as a new resource..

Resources in a sandbox can be re-initialized by hovering your mouse over the resource and clicking the right arrow (*Commands*) button. In the Commands section, find the Start Over option, click the >, and click the **Run** button.



Usage Notes

- Reinitializing a vMX or vSRX device will *not* reload its starting configs; it will also *not* retain any configuration you have added.
- You will need to copy the configs off the device before reinitializing, and then paste the configs back onto the device once it is up and running again.

Restarting a Sandbox

If your sandbox does not start up properly, and the options above don't help, the fix is to simply end the current session and reserve a new session.

Support

Juniper vLabs is intended as a self-serve offering, therefore we do not offer real-time support.

If you are having issues, feel free to contact us at vlabs@juniper.net.

Note that we are generally not able to support active back-and-forth communication with users, however we do read every email that comes in.

To help us resolve your issue, please as include as much information as possible, including:

- Description of the problem
- Sandbox URL
- Frequency - single occurrence or persistent issue
- Screenshots, if appropriate
- Any other information that could help troubleshoot the problem