Oracle® SD-WAN Edge

Service Chaining Guide

Release 9.1
F38219-03
June 2021

Oracle SD-WAN Edge Service Chaining Guide, Release 9.1

F38219-03

Contents

1 SD-WAN Edge Service Chaining UI

Overview 1-1
Supported Topologies and Recommendations 1-1
Oracle Talari E100 with WAN side Guest VM (Firewall) 1-2
Oracle Talari E100 with LAN side Guest VM (Firewall) 1-3
Guest VM Installation Process 1-4
Guest VM Configuration 1-6

2 Oracle ESBC Service Chaining

Install ESBC VM on E100 2-1
Access ESBC VM 2-2
Interface Mapping Corrections on ESBC VM 2-2

3 Check Point VNF Applicance Service Chaining

Check Point VNF Applicance Service Chaining 3-1
Access Check Point VM 3-2

4 pfSense

A Configure PuTTY and Xming for Guest VM Access on Windows

Configure Xming A-1
Configure PuTTY A-3

About This Guide

The purpose of this document is to provide the reader with an understanding of current security methods within the Oracle SD-WAN Edge solution. The reader of this document is expected to be a network architect or a network administrator.

This table lists related documentation.

Document Name	Document Description
Oracle SD-WAN Edge Release Notes	Contains information about added features, resolved issues, requirements for use, and known issues in the latest Oracle SD-WAN Edge release.
Oracle SD-WAN OS Release Notes and Upgrade Guide	Contains information about inserting an OS Partition Image or OS Patch on an appliance in order to migrate to a new OS version or apply fixes to an existing version.
Oracle SD-WAN Security Guide	Contains information about security methods within the Oracle SD-WAN solution.
Oracle SD-WAN Edge Features Guide	Contains feature descriptions and procedures for all incremental releases of Oracle SD-WAN Edge. This guide is organized by release version.
Oracle SD-WAN Edge High Availability Guide	Contains information about implementing High Availability, as well as deployments and configuration.
Oracle SD-WAN Edge Virtual Appliance Installation Guide	Contains information about how to install a Virtual Appliance on a supported hypervisor.
Oracle SD-WAN Edge Service Chaining Guide	Contains information about installing a Guest Virtual Machine using the Service Chaining UI.

Revision History

This section provides a revision history for this document.

Date	Description
April 2021	• Initial release
June 2021	• Fixes Check Point VNF image location in "Check Point VNF Applicance Service Chaining"

1

SD-WAN Edge Service Chaining UI

Overview

Oracle SD-WAN Edge supports Service Chaining on the E100 platforms. This capability allows the installation of the Guest VM from the web UI. This guide covers the installation of the Guest VM. Each Guest VM has a different configuration method that is not included in this guide, however, gaining access to the console interface of the Guest VM will be included as a first step to configuring the Guest VM. Once console access is provided, the user can configure access to the Guest VM for further configuration through the Guest VM web interface.

Currently, the supported Guest VMs include pfSense.

Oracle SD-WAN Edge operates in native mode while the Guest VM will run in the KVM Linux space. Understanding the supported topologies is important prior to installing the Guest VM. The next section will provide an overview of the topologies and recommendations on deployment scenarios.

The supported Guest VMs will require an image for the KVM environment (qcow, qcow2) which you will need to obtain from the vendor. You then need an XML configuration file for the Guest VM. The XML file provided by Oracle is available in this release's software zip file. The XML configuration file will include the RAM, disk, and VCPU required for the Guest VM. The properties of this file should not be changed without consulting a support representative.

Supported Topologies and Recommendations

The supported topologies of the Guest VM include the options to install the Guest VM on the LAN or WAN side of an SD-WAN Edge instance. There are design considerations and recommendations that pertain to each design which are outlined below:

- What services is the Guest VM providing?
- Does the Guest VM need to see the user native traffic prior to the Oracle Talari Application?
- If the Oracle Talari Application receives the traffic first and the destination is another site with an Oracle Talari, the traffic will be Oracle Talari encapsulated.
- Oracle Talari topologies - Router Mode (L3) or Inline Mode (L2).
  - Router Mode is Fail-To-Block (FTB):
    - Traffic is blocked if the Oracle Talari Service or Guest VM is down.
    - More secure solution when using a Firewall as the Guest VM.
  - Inline Mode is Fail-To-Wire (FTW):
    - Traffic will flow through the Oracle Talari Appliance.
    - This may pose a potential security issue for certain users.

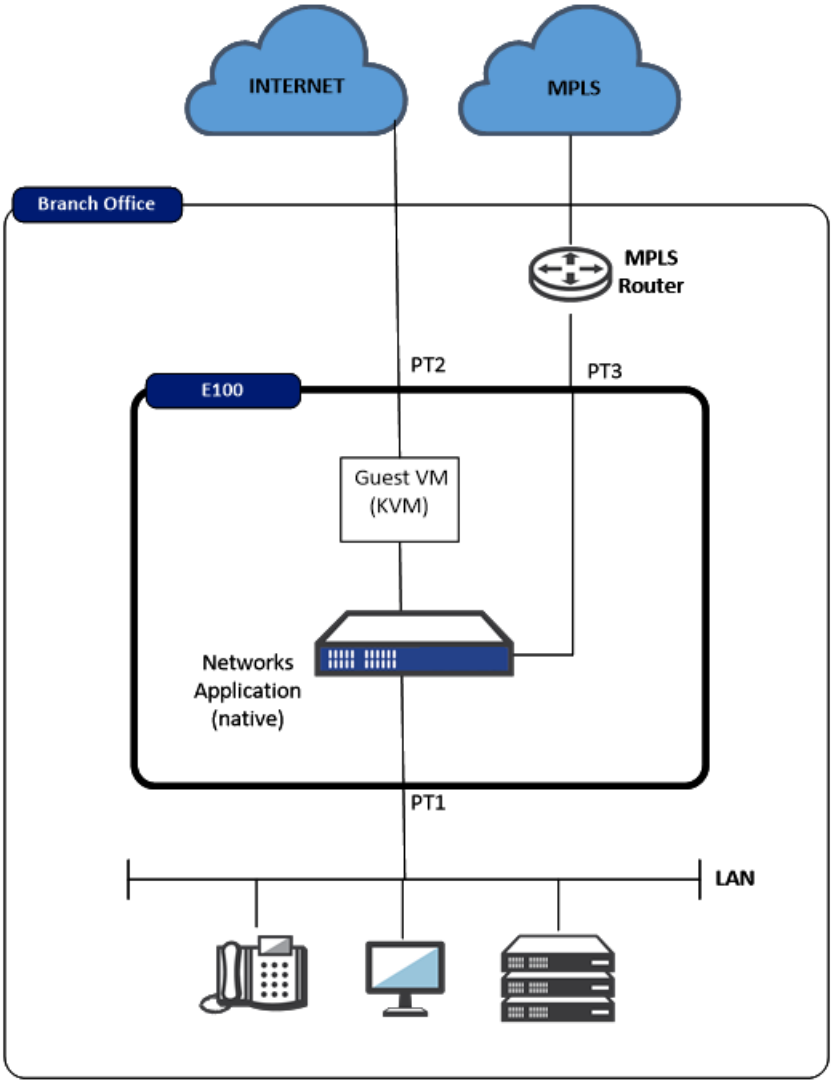
> **Note:**
>
> Traffic flowing through the Appliance while in FTW mode is still being tested as of the time this document was compiled.

- Guest VM configuration is supported on the E100 bypass segments only.
- Guest VM configuration is independent of the Oracle Talari configuration.
  - If the VM is WAN side – Oracle Talari would use the Guest VM IP as a gateway.
- When using Internet Explorer, the image size cannot exceed 4GB (use sparse image).
- After installation of the image and XML files, the system will need to restart the networking process to configure the network interfaces and routing table properly (Management Interface and Management bridge group).
- The user should have a console connected to the E100 when enabling the Service Chaining feature.
- The Oracle Talari Service must be disabled to install the Guest VM.

Oracle Talari E100 with WAN side Guest VM (Firewall)

This topology has the Oracle Talari E100 with the Guest VM on the WAN side of the Oracle Talari Application. The topology will be similar to the image below, depending

on the selected configuration within the Oracle Talari installation page.

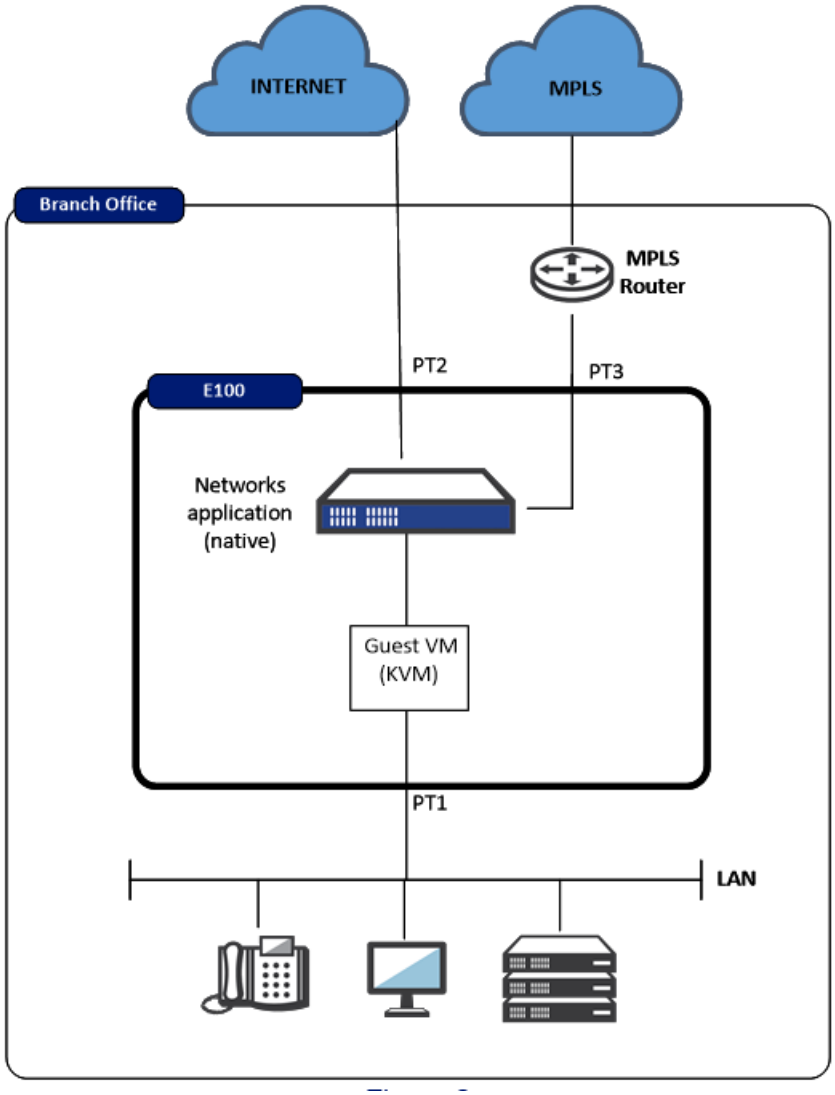


In this topology example, traffic from the physical LAN port 1 is received by the Oracle Talari Application prior to the Guest VM. The user must understand what function the Guest VM is performing, as the Oracle Talari Application will encapsulate any traffic destined for another SD-WAN Edge site. Because the Oracle Talari Application encapsulates Oracle Talari site-to-site traffic, the Guest VM can provide Firewall services. This may include security for Internet traffic, as well as Firewall services for Oracle Talari Conduit traffic. The traffic is then mapped out port 2 of the Oracle Talari Appliance.

Oracle Talari E100 with LAN side Guest VM (Firewall)

This topology has the Oracle Talari E100 with the Guest VM on the LAN side of the Oracle Talari Application. The topology will be similar to Figure 2, depending on the selected

configuration within the Oracle Talari installation page.



In this topology example, traffic from the physical LAN port 1 is received by the Guest VM prior to the Oracle Talari Application. The user must understand what function the Guest VM is performing, and configure the Guest VM appropriately. Once the Oracle Talari Application receives the user traffic, it will encapsulate any traffic destined for another Oracle Talari site into the Oracle Talari Conduit. The user may then also use other Oracle Talari services for non-Conduit traffic, such as Internet, Intranet, etc. The traffic is then mapped out port 2 of the Oracle Talari Appliance.

Guest VM Installation Process

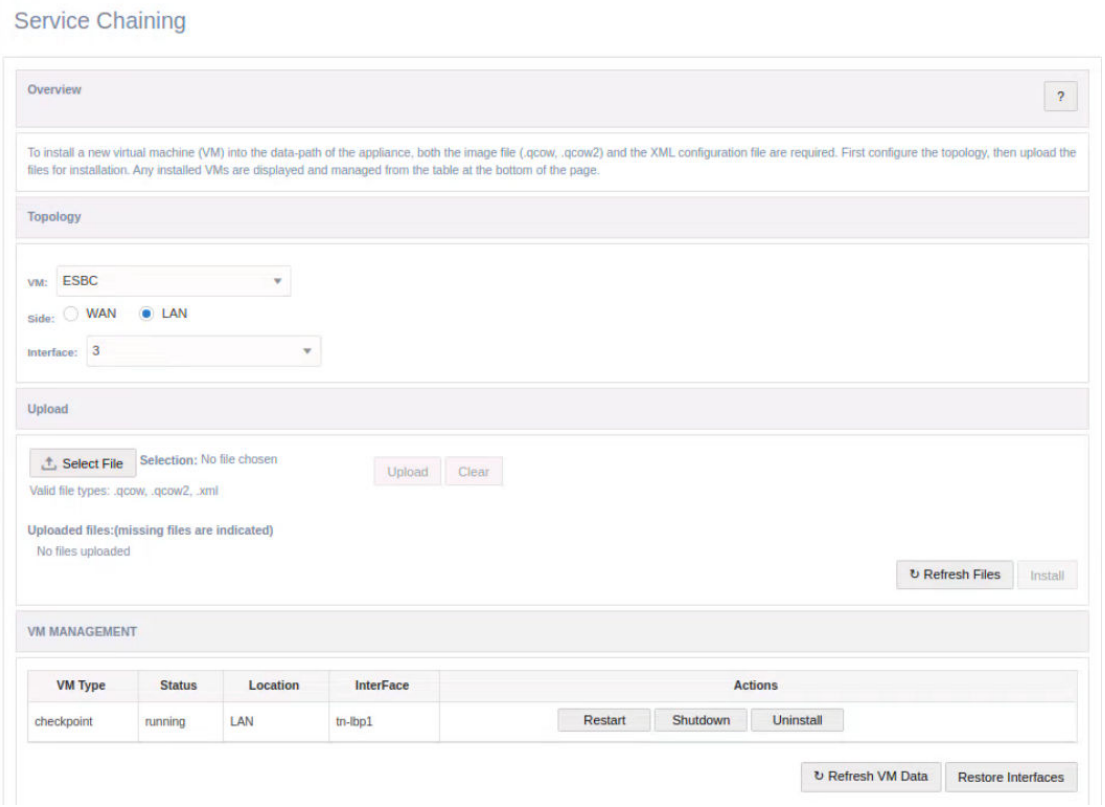
The process to install the Guest VM is defined by the following steps once a topology decision has been made.

- Log into the Oracle SD-WAN Edge Controller appliance and ensure the Talari service has been disabled. If not, disable the Oracle Talari service through **Manage SD-WAN Edge**, **Enable/Disable Services**.
- Proceed to **Configuration**, **Service Chaining**.

- Select the VM type to be used.
- Select WAN or LAN side topology and physical Oracle Talari interface to be used to communicate with the Guest VM.
- Upload the qcow or qcow2 image.
- Upload the XML configuration file.
- Select Install.
- The Guest VM should now be installed and running. Proceed to the next section for directions on establishing Guest VM console access in order to configure the Guest VM.

> **Note:**
>
> The XML file is provided by Oracle Talari Networks and can be downloaded. The file has basic properties that are proven to work with the supported Guest VMs. The MAC addresses used are locally administered addresses. The CPU and memory are configured per Guest VM requirements. Please consult a support representative for any required changes to these properties.

Once the VM has been successfully installed, the user will see a row resembling the figure below in the VM Management section and the status should say “running”. At this point, the user has the option to Restart, Shutdown, or Uninstall the VM. The installation process will also notify the user that connectivity to the management interface maybe lost while the Guest VM is being activated.



The user may now enable the Oracle Service under **Manage SD-WAN Edge**, **Enable/ Disable Services**.

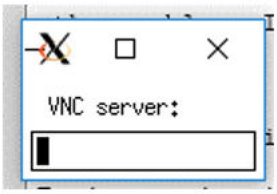
Guest VM Configuration

Now that the Guest VM is up and operational, the user must configure it. Steps to gain access to the console interface are as follows.

- SSH into the E100 using an X Windows interface, such as X11 forwarding, with the **talariuser** username.
- Issue the command **vncviewer**

> **Note:**
>
> Note: The Guest VM must be running for this step to work as expected.

- The VNC Viewer popup window will now appear. Hit enter. The user should now have a terminal window for the Guest VM.



The user may now configure the Guest VM based on the instruction provided by the specific vendor.

2 Oracle ESBC Service Chaining

The Oracle Enterprise Session Border Controller (ESBC) can be deployed as a guest VM on the E100 appliance. The ESBC is instantiated as a small-footprint VM using 4GB RAM, 2 cores, and 2 Virtio-based media ports. This section covers how to install the VM through initial sign-on, as well as configure it.

Install ESBC VM on E100

Before installing ESBC on the E100, you must do the following:

- ESBC VM should be installed on the LAN side. The port used to bridge ESBC should not be part of a bypass pair.
- VLANs cannot be configured on the port connecting the ESBC.
- You can find the XML file in this release's software zip file for the Oracle Talari E100 platform. Then, download the ESBC KVM image file from OSDC or MOS.
- Disable service on this Oracle Talari E100 appliance.
- Navigate to **Configure**, **Service Chaining** page.
- Stop any running VMs, and then uninstall them. Refer to the VM Management section for details.
- Click on the **Restore Interfaces** option. If the previous install failed due to unsupported installs, you may need to clean up using the factory default option.

To install:

1. On the Service Chaining page, select **ESBC** from the VM drop-down.
2. Select **LAN** side.
3. Select the Interface number used by this guest VM.
4. Upload the esbc.xml file you downloaded from MOS by doing the following:
    a. Select the esbc.xml file from the file browser
    b. Click on **OK**.
    c. Click on **Upload**.
5. Upload the ESBC image file in qcow2 format with a qcow2 file extension by doing the following:
    a. Select the file from the file browser.
    b. Click on **OK**.
    c. Click on **Upload**.
6. Click on **Install**.

The ESBC VM should be running now. Any errors will be reported in /home/talariuser/log/APN_webconsole.log

Access ESBC VM

After installing, follow these steps to sign into the ESBC VM from your local system. This procedure explains how to use vncviewer to access the ESBC VM.

1. SSH into the E100 Appliance as talariuser.

```
ssh  -X talariuser@10.75.134.24
password
```

2. Enter the following command to find the vncviewer connector:

```
 sudo virsh vncdisplay esbc
127.0.0.1:0
```

3. Enter the following command to start the vncviewer:

```
vncviewer 127.0.0.1:0
Note: Use <Shift>PageUp or <Shift>PageDown to scroll up or down in
vncviewer
esbc password:acme
Enter new Password: <ESBC Password>
Confirm new Password: <ESBC Password>
enable password: packet
Enter new Password: <ESBC Password>
Confirm new Password: <ESBC Password>
Command to enable debug and get in to shell
debug-enable
Password: <ESBC Password>
shellPassword: <ESBC Password>
exit
```

Interface Mapping Corrections on ESBC VM

This section explains how to make corrections to interface mapping on ESBC VM.

Use the following command to show the current interface mapping on the ESBC

```
show interfaces mapping
```

Example:

```
ESBC1# show interfaces mapping
Interface Mapping Info
------------------------------------------
Eth-IF MAC-Addr Label
wancom0 52:54:00:32:F4:65 #generic
wancom1 52:54:00:56:7C:31 #generic
s0p0 52:54:00:B2:E7:C6 #generic
wancom2 FF:FF:FF:FF:FF:FF #dummy
spare FF:FF:FF:FF:FF:FF #dummy
s1p0 FF:FF:FF:FF:FF:FF #dummy
```

```
s0p1 FF:FF:FF:FF:FF:FF #dummy
s1p1 FF:FF:FF:FF:FF:FF #dummy
s0p2 FF:FF:FF:FF:FF:FF #dummy
s1p2 FF:FF:FF:FF:FF:FF #dummy
s0p3 FF:FF:FF:FF:FF:FF #dummy
s1p3 FF:FF:FF:FF:FF:FF #dummy
```

> **Note:**
>
> Note that s1p0 does not show any valid MAC Address.

Find the sbWAN MAC interface name (wancom1 in this example) in the mapping. You can swap that interface with s1p0 with the following commands:

```
interface-mapping
 swap wancom1 s1p0
```

Example:

```
SBC1# interface-mapping
ESBC1(interface-mapping)#
ESBC1(interface-mapping)# swap wancom1 s1p0
Interface Mapping Info after swapping
-----------------------------------------
Eth-IF MAC-Addr Label
wancom0 52:54:00:32:F4:65 #generic
wancom1 FF:FF:FF:FF:FF:FF #dummy
s0p0 52:54:00:B2:E7:C6 #generic
wancom2 FF:FF:FF:FF:FF:FF #dummy
spare FF:FF:FF:FF:FF:FF #dummy
s1p0 52:54:00:56:7C:31 #generic
s0p1 FF:FF:FF:FF:FF:FF #dummy
s1p1 FF:FF:FF:FF:FF:FF #dummy
s0p2 FF:FF:FF:FF:FF:FF #dummy
s1p2 FF:FF:FF:FF:FF:FF #dummy
s0p3 FF:FF:FF:FF:FF:FF #dummy
s1p3 FF:FF:FF:FF:FF:FF #dummy
Changes could affect service, and Requires Reboot to become effective.
Continue [y/n]?: y
WARNING: This change requires a reboot to become effective.
reboot
```

3

Check Point VNF Applicance Service Chaining

Check Point Firewall can be deployed as a guest VM on the E100 appliance. This section covers how to install the VM, as well as configure it.

Check Point VNF Applicance Service Chaining

Before installing Check Point VNF, make sure you do the following:

- Checkpoint VM should be installed on the WAN side for example port4 (wbp1).
- The port used to bridge with Checkpoint should not be part of a bypass pair.
- VLANs cannot be configured on the port connecting the Check Point VM.
- You can find the XML file in this release's software zip file for the Oracle Talari E100 platform. Then, download the Check Point Cloudguard VNF qcow2 image file by going to the Check Point customer support center and searching for article "sk171497."

To install:

1. Disable Service on SD-WAN Edge E100.
2. Navigate to the **Configure**, **Service Chaining** page.
3. Stop any running VMs, and then uninstall them.
4. Click on the **Restore Interfaces** option.

   If the previous install failed due to unsupported installs, you may need to clean up using the factory default option.
5. On the Service Chaining page, select **Check Point**.
6. Select **WAN**.
7. Select a port.
8. Upload the checkpoint.xml file by doing the following:
   a. Select the checkpoint.xml file from the file browser
   b. Click on **OK**.
   c. Click on **Upload**.
9. Upload the Check Point VNF image file in qcow2 format with a qcow2 file extension by doing the following:
   a. Select the file from the file browser.
   b. Click on **OK**.
   c. Click on **Upload**.

> **Note:**
>
> Only use the most current checkpoint image from Oradocs.

10. Click on **Install**.

The Check Point VM should be running.

Access Check Point VM

After installing, follow these steps to set up and configure the Check Point VM using vncviewer.

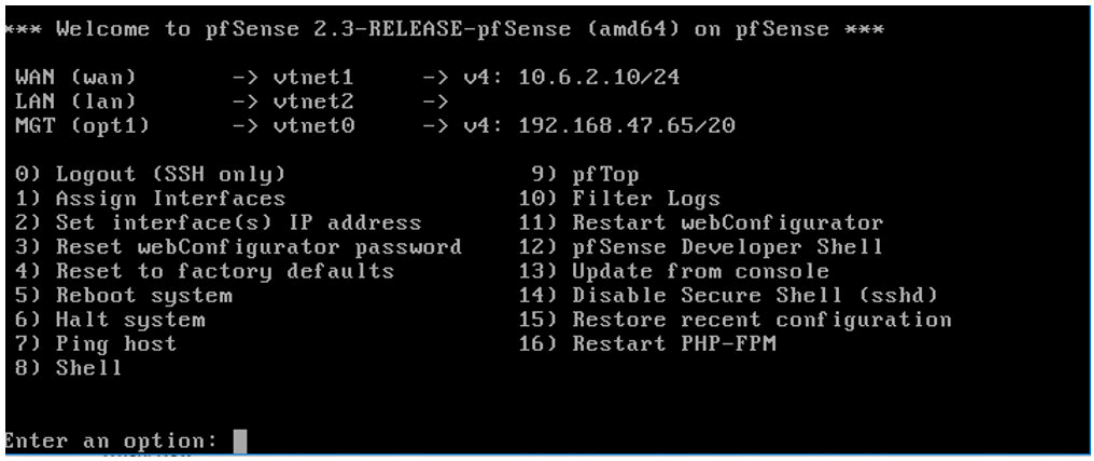
1. Wait for the boot to complete.
2. Log into the system using **admin** / **admin** as the username and password.
3. Enter the following command to ensure you do not lose your configuration once you get to the Web interface:

   ```
   set property first-time-wizard off
   ```

4. Use the following example to set the management interface:
   a. set admin-access interfaces any access allow
   b. set admin-access allowed-ipv4-addresses any
   c. set security-management mode locally-managed
   d. add internet-connection interface WAN type static ipv4-address 10.75.135.6 subnet-mask 255.255.254.0 default-gw 10.75.134.1 conn-test-timeout 0 name Management
5. Once the management interface is configured, the rest of the configuration can be performed through the web interface.

4
pfSense

Once the console to the pfSense Firewall is available, use the shell console displayed in Figure 6 for network configuration. The pfSense version 2.3 was used for verification.



The user should configure an IP address for the Guest VM. This guide uses the MGT (opt1) interface on the pfSense Firewall, but you may also use the LAN interface if desired.

To assign an IP address, select option 2. You may verify the MAC addresses assigned to the logical port via option 1, as well as with the `sudo /sbin/ifconfig` command on the Talari.

Once an IP address has been assigned, you may also define a gateway for the MGT (opt1) interface from the shell using option 8 from the menu. This command will add a route into the route table for initial off subnet access to the web console of the pfSense interface, similar to the following example (Subnet: 192.160.0.0/16, Gateway: 192.168.44.1).

- Route add -net 192.168.0.0/16 192.168.44.1

The MGT (opt1) interface blocks all traffic by default, so you must allow traffic for the initial configuration. When using option 8, the user should enter the following commands.

```
echo pass in on vtnet0 all >> /tmp/rules.debug
echo pass out on vtnet0 all >> /tmp/rules.debug
pfctl -F all -f /tmp/rules.debug
```

Verify connectivity with the ping command to the MGT IP address, and if successful, you should now have access to the GUI of the pfSense Firewall.

Within the GUI, the user must configure and save rules before rebooting pfSense. Otherwise, access to the pfSense GUI will be lost if using the MGT (opt1) interface for Management access.

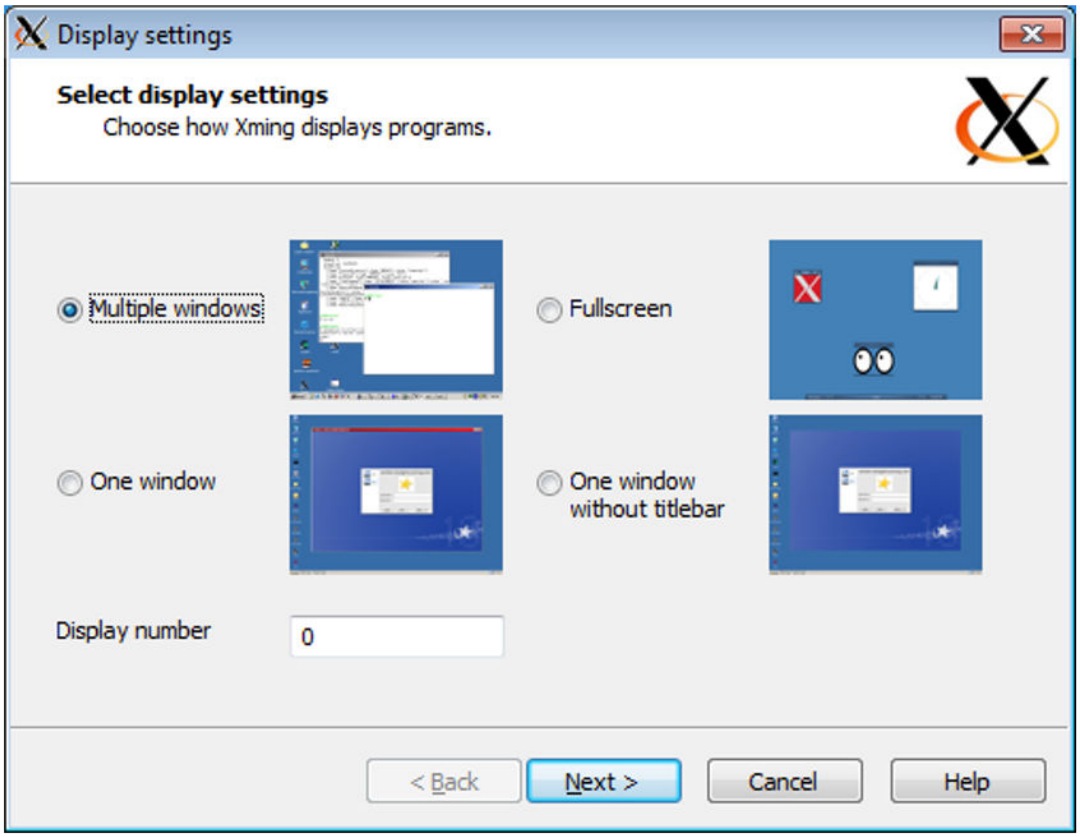
A

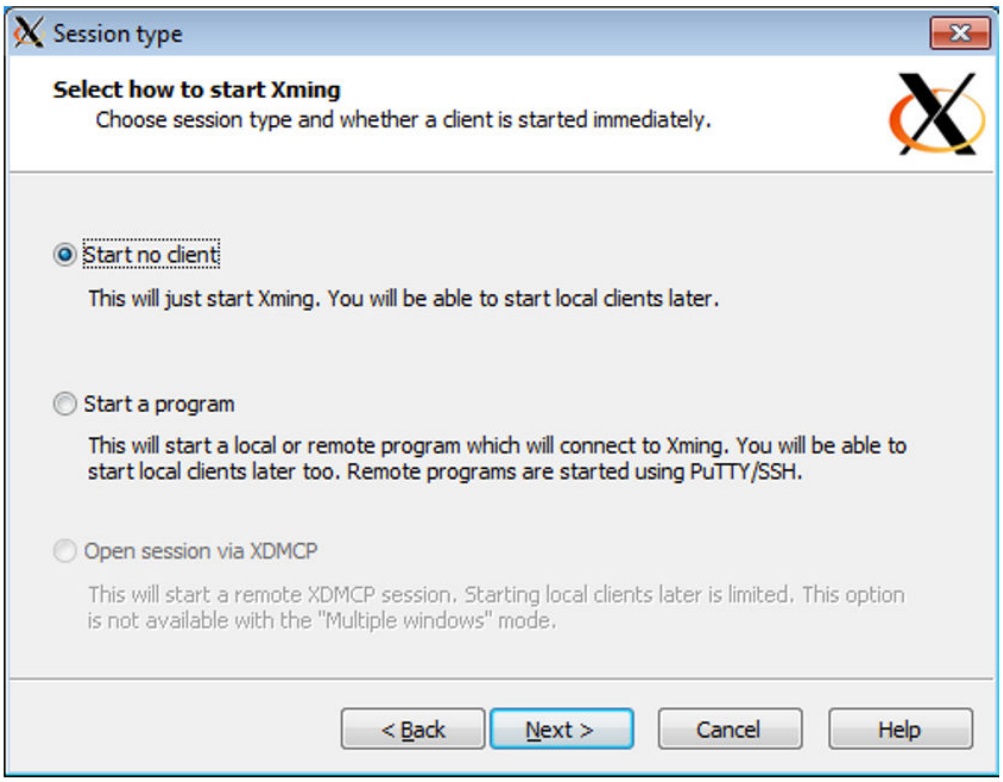
Configure PuTTY and Xming for Guest VM Access on Windows

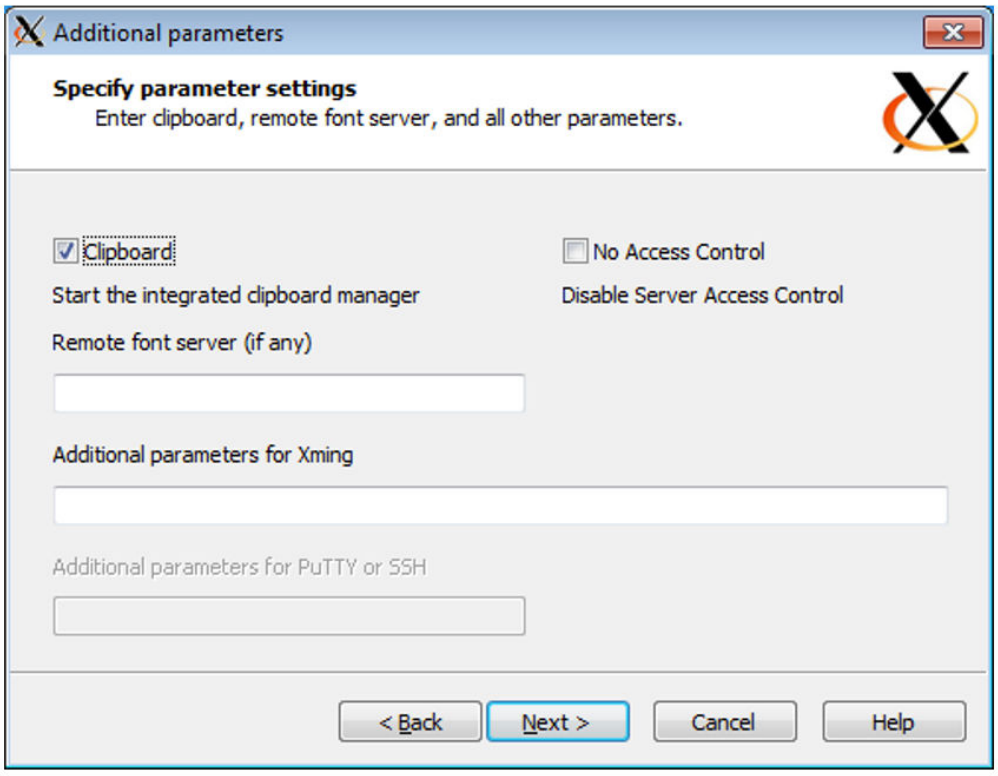
For initial Guest VM configuration, you must SSH to the host E100 using an X Windows interface. On a Windows workstation, you can use PuTTY in combination with Xming for this purpose.

Configure Xming

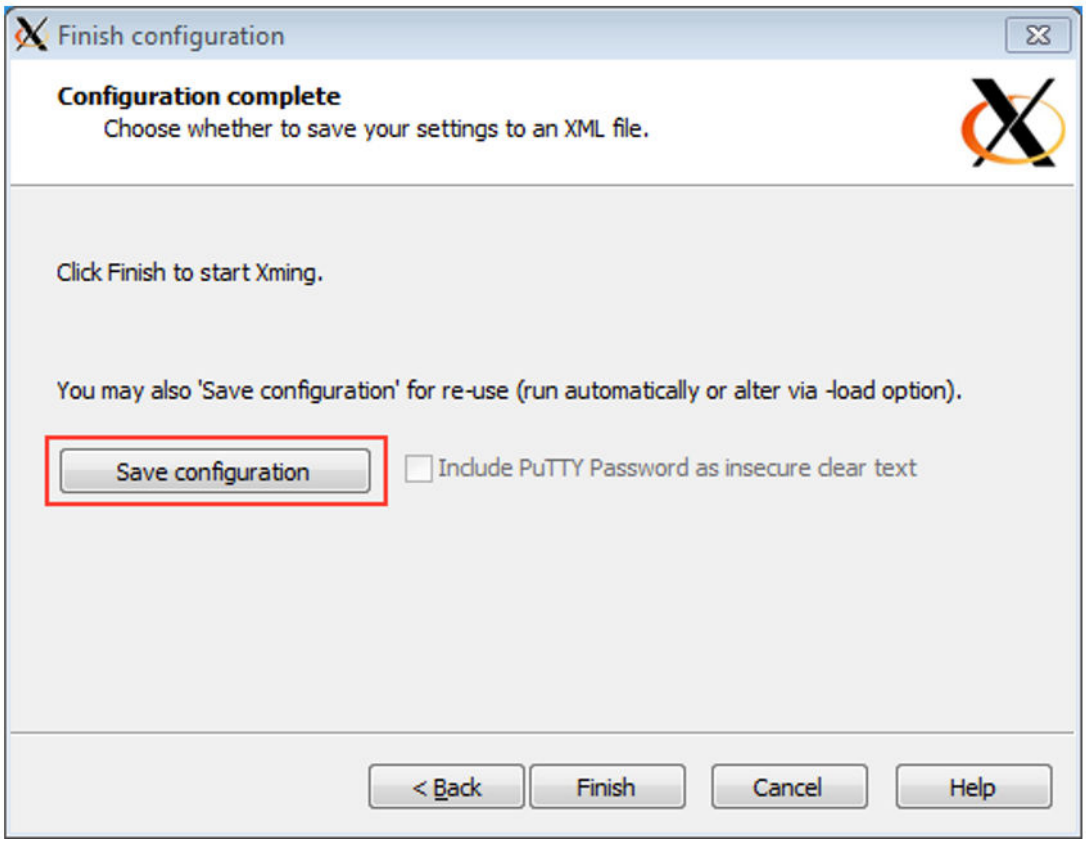
1. After installing Xming, run the application “XLaunch”. Go through the configuration dialogue and confirm that XLaunch is configured as shown below:







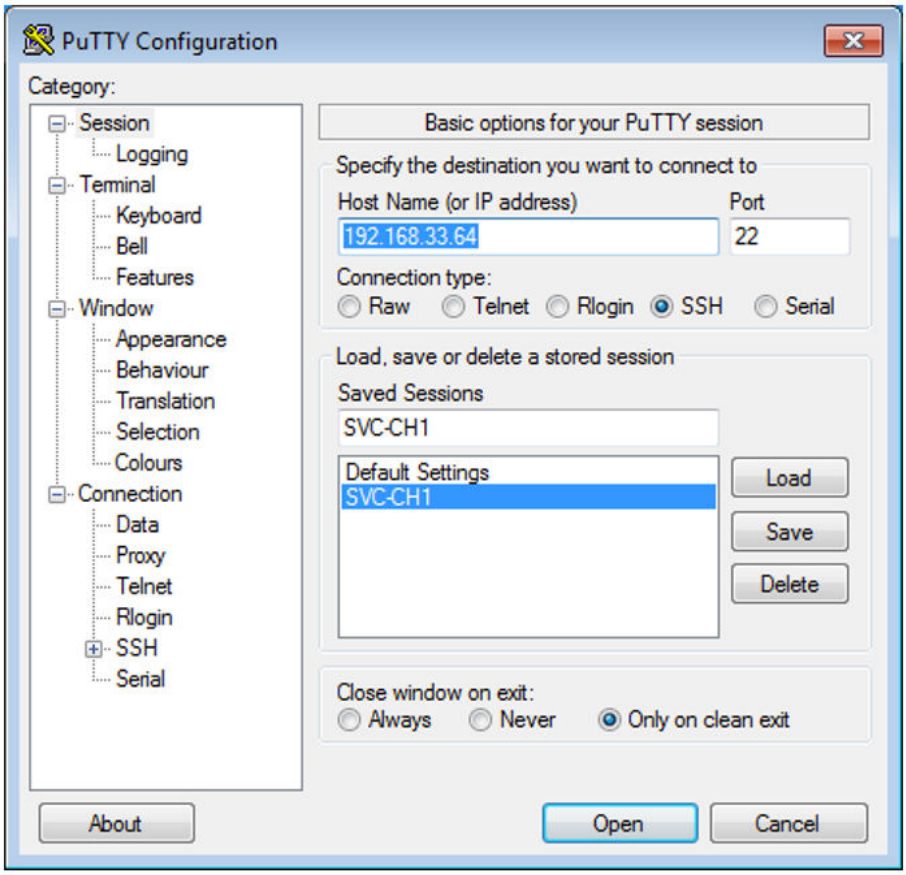
2. On the final screen on the configuration dialogue, save the configuration for future use before clicking **Finish**:

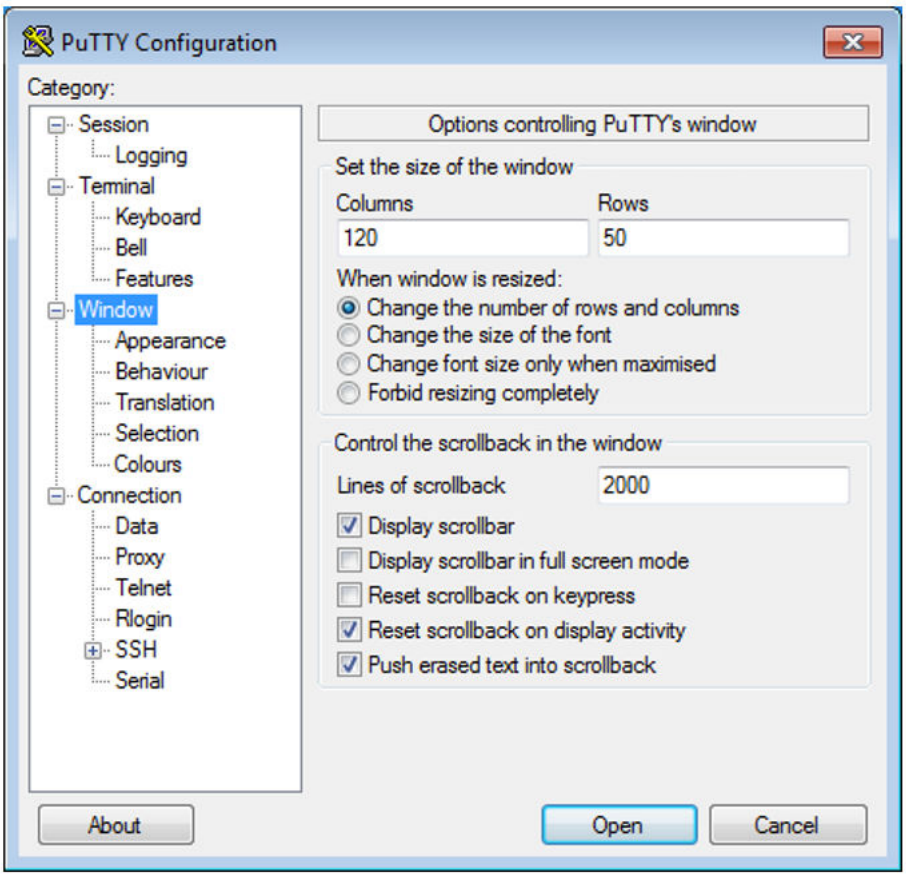


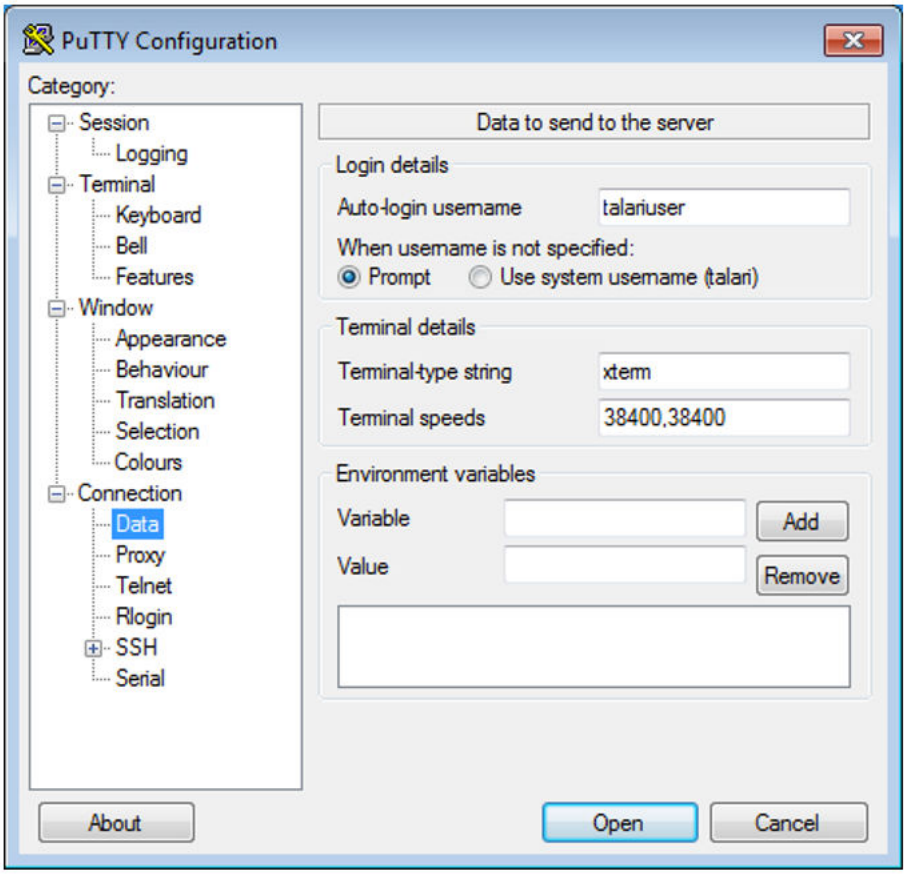
Configure PuTTY

1.After installing PuTTY, launch the application and configure as shown below.

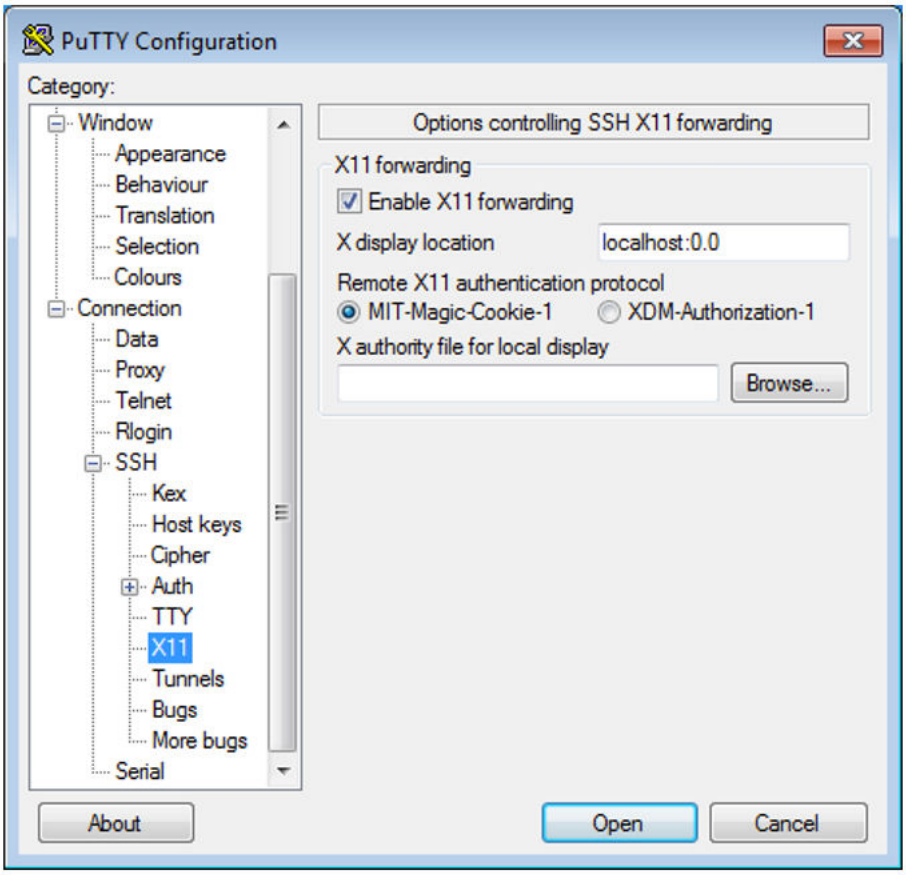
Replace the example IP with the management IP of the host E100:




PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Options controlling PuTTY's window
Set the size of the window
Columns
Rows
120
50
When window is resized:
Change the number of rows and columns
Change the size of the font
Change font size only when maximised
Forbid resizing completely
Control the scrollback in the window
Lines of scrollback
2000
Display scrollbar
Display scrollbar in full screen mode
Reset scrollback on keypress
Reset scrollback on display activity
Push erased text into scrollback
About
Open
Cancel


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Data to send to the server
Login details
Auto-login username
talariuser
When username is not specified:
Prompt
Use system username (talari)
Terminal details
Terminal-type string
xterm
Terminal speeds
38400,38400
Environment variables
Variable
Add
Value
Remove
About
Open
Cancel

2. Expand the SSH menu in the sidebar to find X11 options. Enable X11 forwarding and set the X display location to localhost:0.0.



3. Open the SSH connection to the host E100 and proceed with Guest VM configuration as outlined in the "Guest VM Configuration" section.