

Oracle® SD-WAN

Service Chaining Installation Guide



Original Publication Date: Nov 1, 2019



Copyright © 2019, 2007 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. Windows® 7 and Windows® XP are trademarks or registered trademarks of Microsoft Corporation.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

About This Document	4
Audience	4
References	4
Talari Service Chaining UI	5
Overview	5
Supported Topologies and Recommendations	5
Talari E100 with WAN side Guest VM (Firewall)	6
Talari E100 with LAN side Guest VM (Firewall)	7
Guest VM Installation Process	8
Guest VM Configuration	9
pfSense	10
Palo Alto	11
Summary	12
Appendix A: Configure PuTTY and Xming for Guest VM Access on Windows	13
Configure Xming	13
Configure PuTTY	16

About This Document

This guide illustrates how to install a Guest VM using the new APN 6.1 GA feature, Service Chaining UI. This guide will walk the user through how to install the Guest VM software and access the console port for configuration of the Guest VM, as well as discuss supported topologies.

My Oracle Support

My Oracle Support (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.

3. Select one of the following options:

- For technical issues such as creating a new Service Request (SR), select 1.
- For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability

- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click Industries.
3. Click the Oracle Communications link.

Under the SD-WAN header, select a product.

4. Select the Release Number.

A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

References

The following documents are available:

- *Talari Glossary*
- *Talari APN 6.1 GA Release Notes*
- *Talari APN 6.1 Configuration File Reference*
- *Talari APN 6.1 New Feature Guide*

Talari Service Chaining UI

Overview

Talari supports Service Chaining on the E100 platforms in the latest APN software release. This capability has been expanded to allow the installation of the Guest VM from the Talari web UI. Moving forward, it is recommended to use the most current APN software release for Service Chaining. 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 web access to the Guest VM for further configuration through the Guest VM web interface.

Currently, the supported Guest VMs include pfSense and Palo Alto.

The Talari Application will operate 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 the user will get from the vendor. Secondly, the user will need an XML configuration file for the Guest VM. The XML file that will be provided from Talari Networks is available on the Talari Support Portal section of our website. 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 Talari Representative.

Note: The pfSense qcow2 image must be a bootable image.

Supported Topologies and Recommendations

The supported topologies of the Guest VM include the options to install the Guest VM on the LAN side or WAN side of the Talari Application. 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 Talari Application?
- If the Talari Application receives the traffic first and the destination is another site with a Talari, the traffic will be Talari encapsulated.
- Talari topologies - Router Mode (L3) or Inline Mode (L2).
 - Router Mode is Fail-To-Block (FTB):
 - Traffic is blocked if the 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 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 Talari configuration.

- If the VM is WAN side – 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 Talari Service must be disabled to install the Guest VM.

Talari E100 with WAN side Guest VM (Firewall)

This topology has the Talari E100 with the Guest VM on the WAN side of the Talari Application. The topology will be similar to Figure 1, depending on the selected configuration within the Talari installation page.

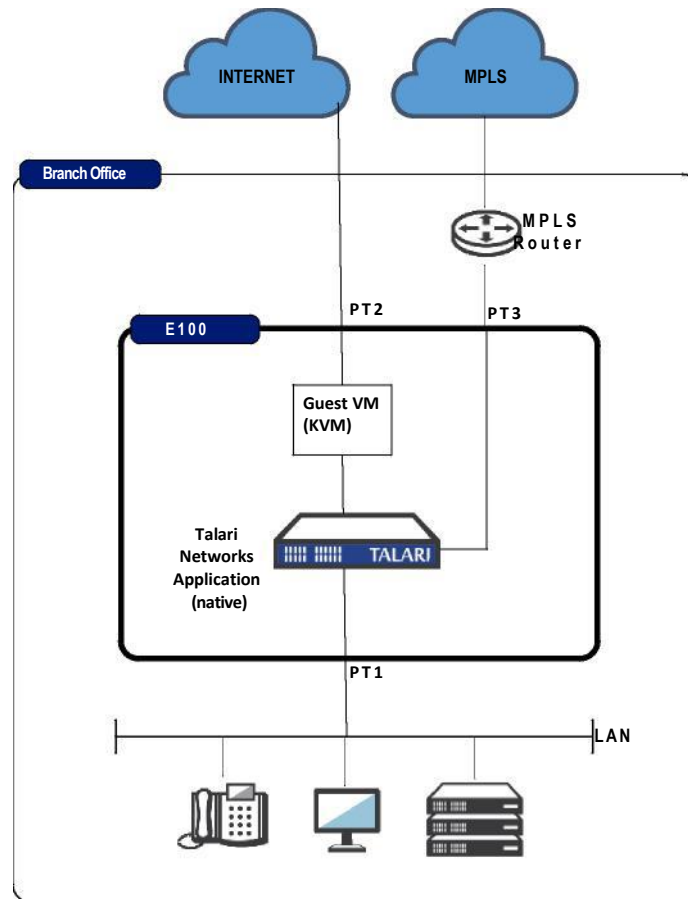


Figure 1

In this topology example, traffic from the physical LAN port 1 is received by the Talari Application prior to the Guest VM. The user must understand what function the Guest VM is performing, as the Talari Application will encapsulate any traffic destined for another Talari site. Because the Talari Application encapsulates 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 Talari Conduit traffic. The traffic is then mapped out port 2 of the Talari Appliance.

Talari E100 with LAN side Guest VM (Firewall)

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

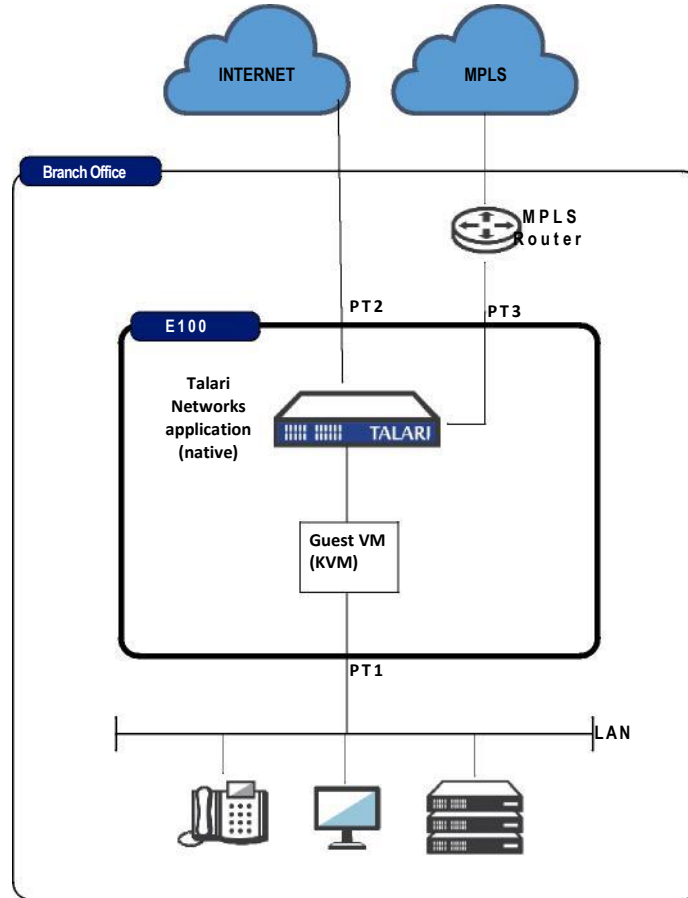


Figure 2

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

- Login into the Talari E100 Appliance and ensure the Talari service has been disabled. If not, disable the Talari service through Manage **Network > Service/WAN Links**.
- Proceed to **Integrate > Service Chaining**.
- Select the VM type to be used.
- Select WAN or LAN side topology and physical 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.

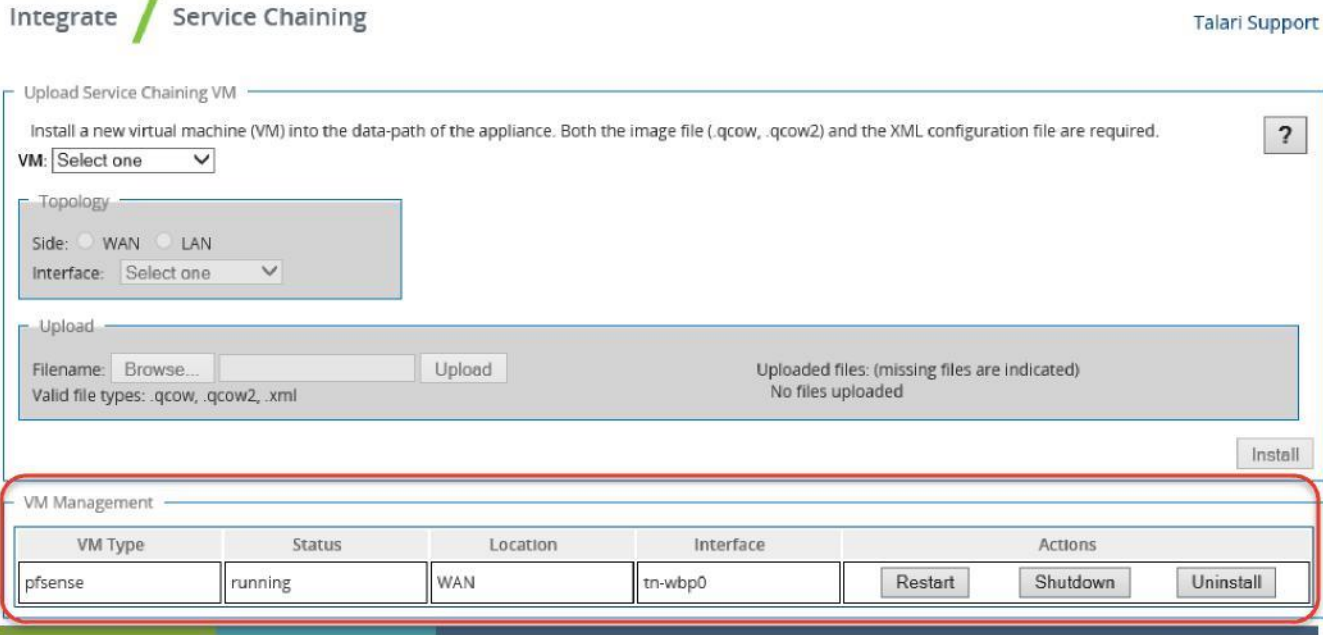
The screenshot displays the 'Integrate / Service Chaining' configuration page. At the top right, it says 'Talari Support'. The main section is titled 'Upload Service Chaining VM' and contains the following elements:

- A red-bordered box highlights the 'VM' dropdown menu (set to 'pfSense'), the 'Topology' section (with 'WAN' selected), and the 'Interface' dropdown menu (set to '2').
- Below this, another red-bordered box highlights the 'Upload' section, which includes a 'Browse...' button, an 'Upload' button, and the text 'Valid file types: .qcow, .qcow2, .xml'.
- To the right of the upload section, it indicates 'Uploaded files: (missing files are indicated) No files uploaded'.
- An 'Install' button is located at the bottom right of the main form area.
- At the bottom of the page, there is a 'VM Management' section showing 'No guest VM installed' and a footer with 'Powered by Talari'.

Figure 3

Note: The XML file is provided by 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 Talari Representative for any required changes to these properties.

Once the VM has been successfully installed, the user will see a row resembling Figure 4 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 screenshot shows the 'Integrate / Service Chaining' interface. The 'Upload Service Chaining VM' section includes a dropdown for 'VM', a 'Topology' section with 'Side' (WAN/LAN) and 'Interface' (Select one) options, and an 'Upload' section with a 'Browse...' button and 'Upload' button. Below this is the 'VM Management' section, which is highlighted with a red box. It contains a table with the following data:

VM Type	Status	Location	Interface	Actions
pfsense	running	WAN	tn-wbp0	Restart Shutdown Uninstall

At the bottom of the interface, there is a copyright notice '© 2016 Talari Networks' and a 'Powered by Talari' logo.

Figure 4

The user may now enable the Talari Service under **Manage Network > Service > Enable**.

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, entering the credentials:
 - Username: talariuser
 - Password: talari
- Issue the command **vncviewer**

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.



Figure 5

The user may now configure the Guest VM based on the instruction provided by the specific vendor. Below are some basic instructions for the vendors that are currently supported. These instructions are to provide management access to the Guest VMs only.

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.

```
*** Welcome to pfSense 2.3-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> vtnet1      -> v4: 10.6.2.10/24
LAN (lan)      -> vtnet2      ->
MGT (opt1)    -> vtnet0      -> v4: 192.168.47.65/20

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Figure 6

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.

Palo Alto

Once the console to the Palo Alto Firewall is available (VM models for KVM), use the command line interface displayed in Figure 7 for network configuration. The Palo Alto version 7.1.0 was used for verification, but Talari recommends using the 8.0 software release as this provide an increase in performance. The configuration of the Palo Alto next generation firewall consists of policies to allow only Talari conduit traffic as well as Internet traffic.

```
PA-UM login: admin
Password:
Last login: Thu Jan  5 09:16:45 on tty1

Number of failed attempts since last successful login: 0

Warning: Your device is still configured with the default admin account credentials. Please change your password prior to deployment.
admin@PA-UM>
```

Figure 7

Configure the management IP address, gateway and DNS information. Once in configuration mode, apply commands similar to the examples below and commit the changes.

```
admin@PA-VM>configure
```

```
admin@PA-VM#show (to view the current configuration).
```

```
admin@PA-VM# set deviceconfig system ip-address 1.1.1.1 netmask 255.255.255.0  
default-gateway 1.1.1.5 dns-setting servers primary 1.1.1.50
```

IP address - 1.1.1.1

Gateway - 1.1.1.5

DNS server - 1.1.1.50

admin@PA-VM#**commit** (which allows the change to take effect).

admin@PA-VM#**exit**

admin@PA-VM>**ping host 1.1.1.100** (a host on the external LAN network).

Note: When installing with version 8.0 software, make sure DHCP is disabled on the management interface – in configuration mode: `set deviceconfig system type static`

Once you have verified an external host is reachable, use the GUI interface of the Palo Alto to complete the configuration.

Summary

The Service Chaining UI capability of the E100 Appliance allows flexibility at branch locations that Talari Networks has not offered in the past. As Talari Networks moves forward with this solution, the number of Guest VMs supported will be expanded. Any feedback on supported Guest VMs is welcome as the user becomes familiar with this new feature.

Appendix A: Configure PuTTY and Xming for Guest VM Access on Windows

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

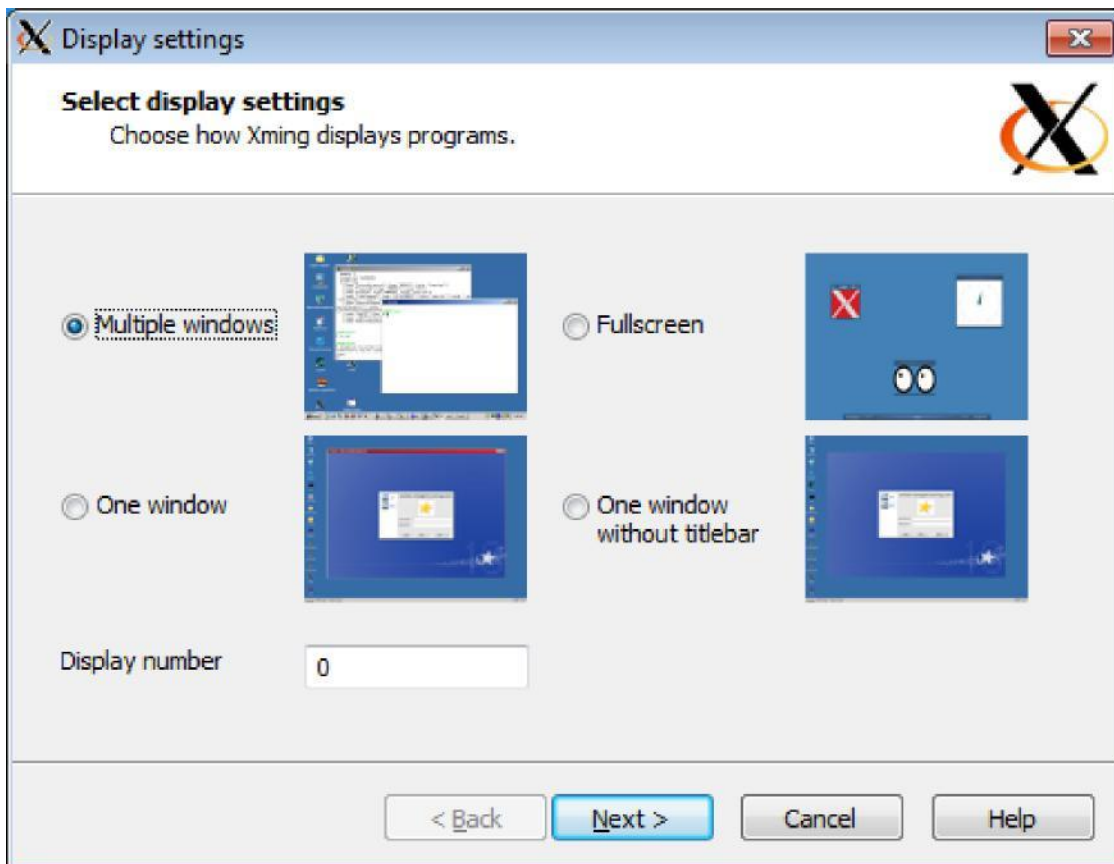
PuTTY can be downloaded from

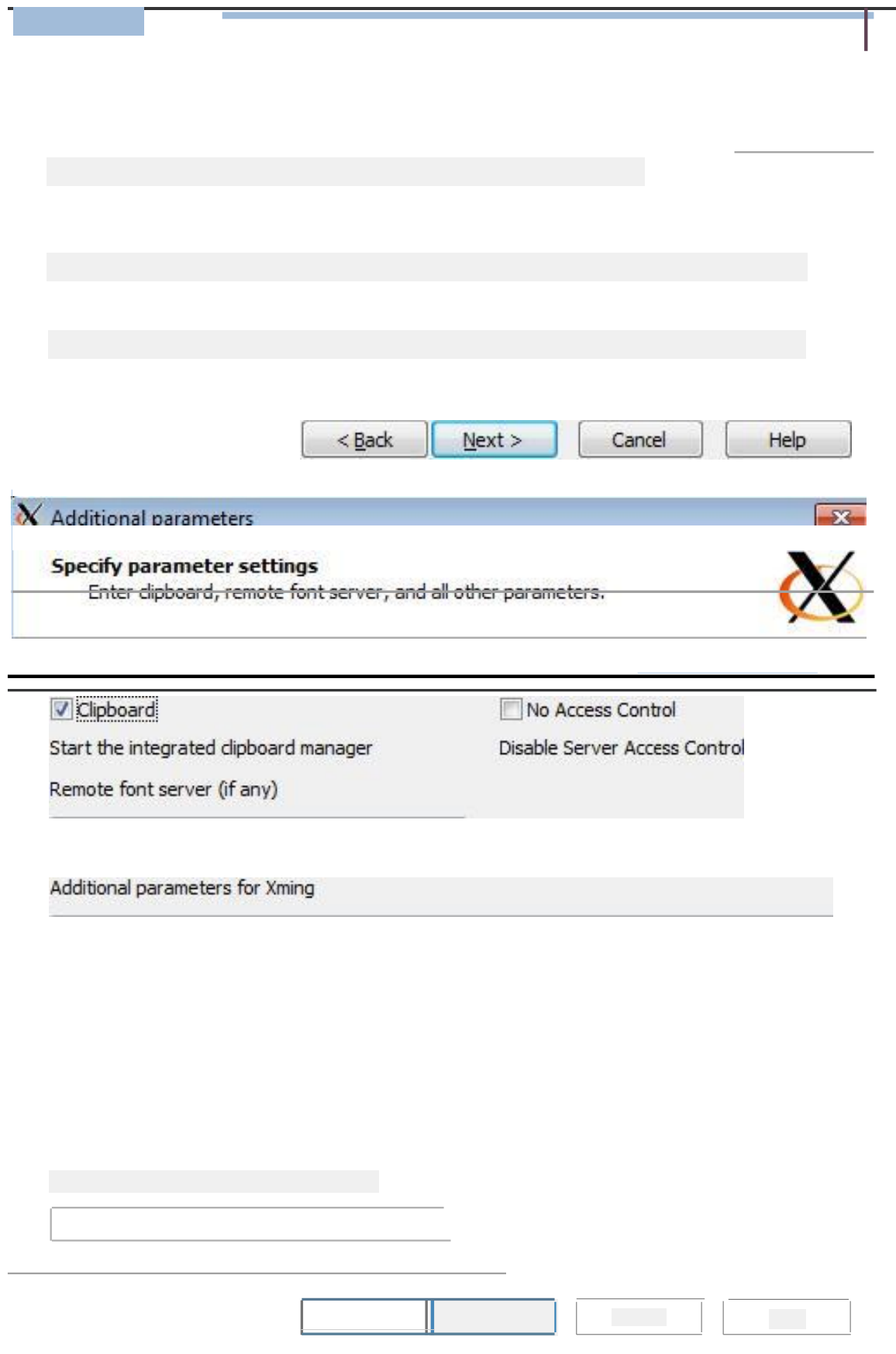
<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.

Xming can be downloaded from <https://sourceforge.net/projects/xming/files/Xming/>.

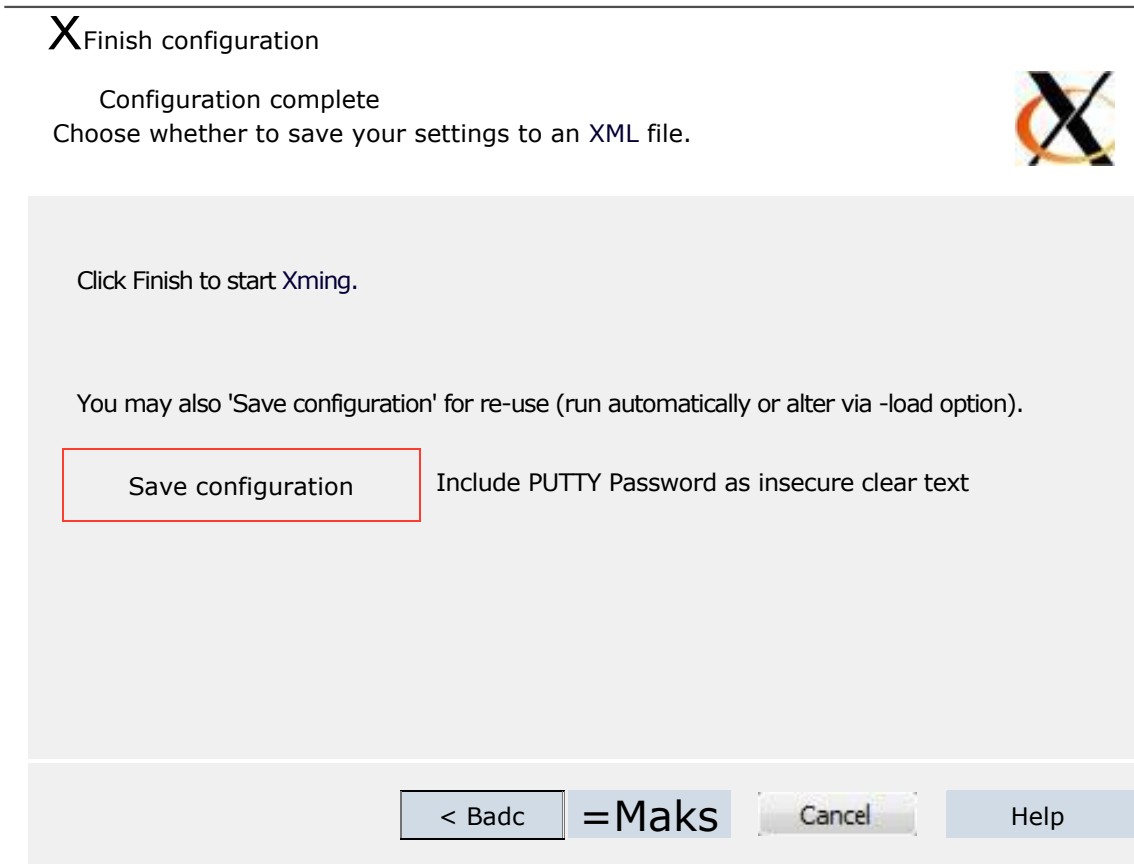
Configure Xming

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





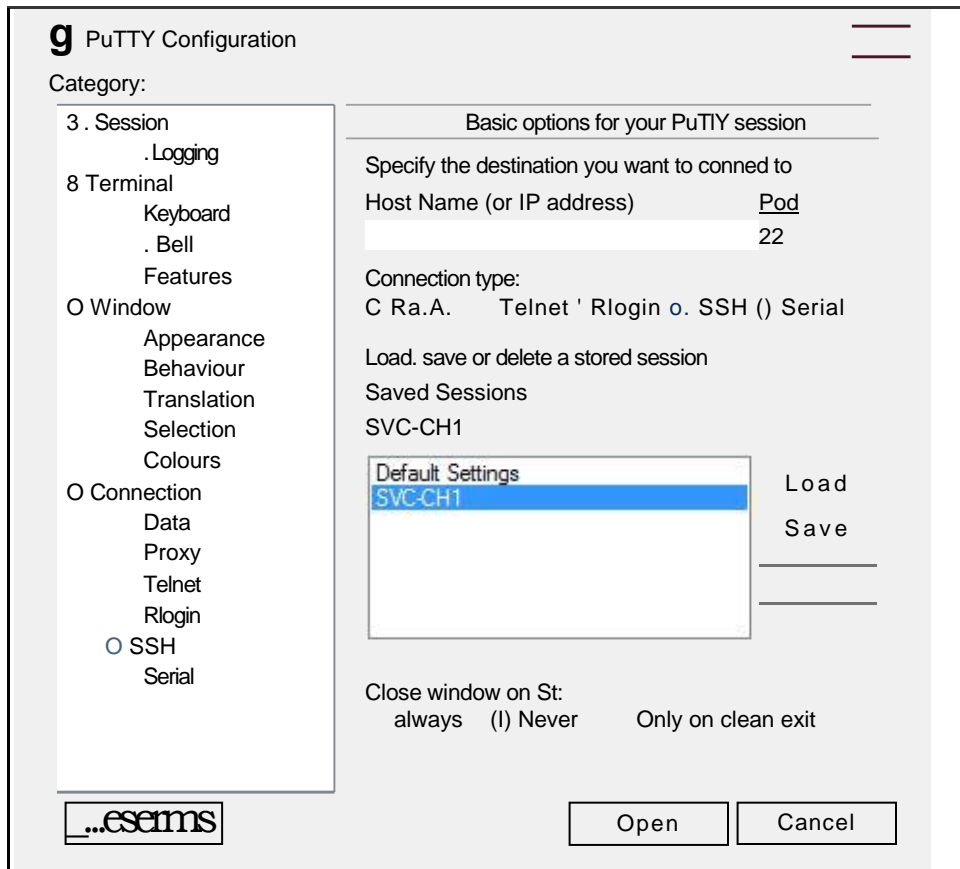
On the final screen on the configuration dialogue, save the configuration for future use before clicking "Finish":

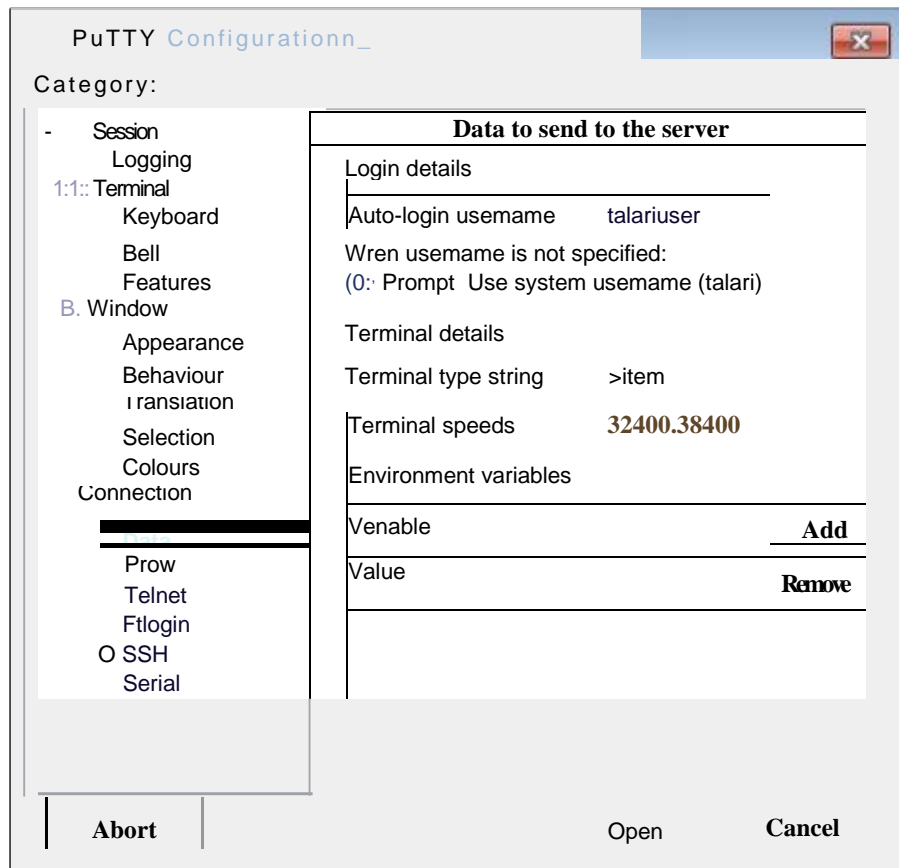
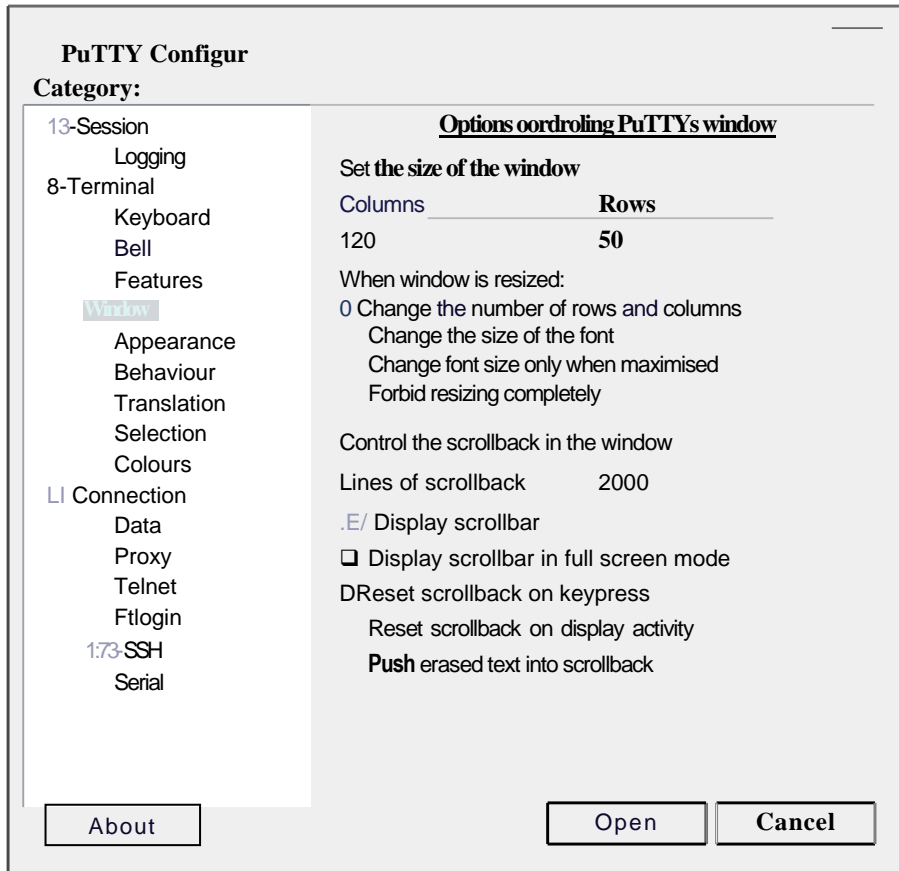


Configure PuTTY

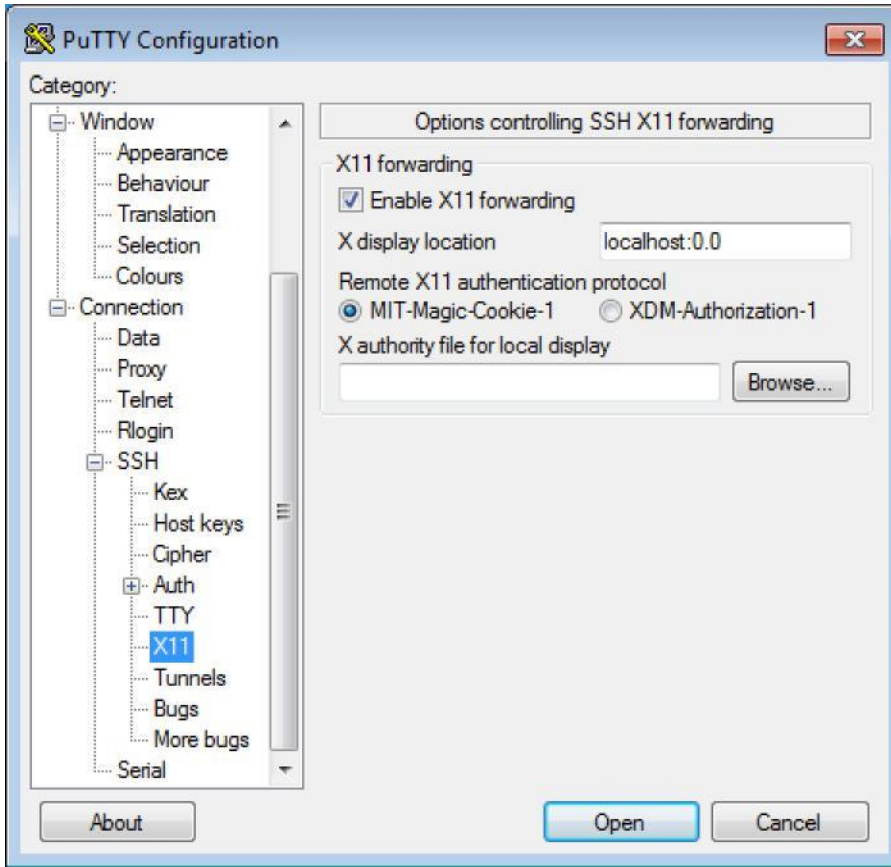
After installing PuTTY, launch the application and configure as shown below.

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





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



Open the SSH connection to the host E100 and proceed with Guest VM configuration as outlined on pages 6 and 7.

