Dell EMC OpenManage Network Manager Version 6.5

Installation Guide



Notes and Cautions

A NOTE indicates important information that helps you make better use of your computer.

A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

© 2017 Dell Inc.

Trademarks used in this text: Dell EMC™, the DELL EMC logo, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

2017-9
Rev. A01

Contents

1 Introduction 7

In This Guide 7

Intended Audience 7

Installation Overview 8

Related Documents 8

2 Preparing for Installation 9

Reviewing Pre-Installation Checklist 10

Verifying Software Package 12

Verifying System Requirements 13

System requirementsvary depending on how you plan to use the OMNM application. Software Requirements 13

Hardware Requirements 14

Single Server Hardware Requirements 14

Distributed Server Hardware Requirements 16

Preparing Linux for Installation 18

Installing Third-Party Software 19

Installing Perl 20

Perl 20

Basic Network Considerations 21

Windows Prerequisites 22

LinuxPrerequisites 22

System Capacity 23

Paths 23

Hardware Requirements on page 14, whether embedded (MySQL) or Oracle,Enterprise (Distributed) Edition 24

Adding Mediation Servers 25

Clustered Edition 25

Db High Availability Edition 26

Clustered Mediation Servers 27

Web Portal Installation 27

Application Server Installation 27

Compatibility with Previous Versions 27

Configuration Options 28

Setting Up User Accounts?? 29

Setting Up Your RDBMS 30

Collecting License Information 31

Obtaining Info 32

Understanding Best Practices 33
Ports Used. 33
Linux Disk Partition Information 34

3 Installing OMNM 37
Installing the Application 38
Installing on Linux 38
Completing Post-Installation Tasks 41
Verifying Your Installation 41
Installing on Linux 41
Installing on Windows 43
Installing OMNM Silently 47
Silent Installation 47
Installing Licenses 48
Starting Linux Installations 49
Web Services 50
Application Password 50
Starting Application Server 50
Installing Server Manager 51
pmgetstatus 52
Windows Server Monitor 52
Web Server Parameters 53
Startup Properties 54
Proactive Runtime Management 55
Using Two Interfaces 56
Installing on Linux from the Command Line 56
Performing Complex Installations 57
Oracle RAC Property 60
Startup Sequence for Initial Testing 60
E-Mail 61
Verifying Your Installation 61
Uninstalling the Application. 63
Stopping Servers 64

4 Updating an Existing Installation 65
Upgrading from a Previous Version 66
User Validation 66
Upgrading Your Operating System 66

General Upgrade Advice/Information 66
Handling Missing Users 67
Backing Up the Database 68
Restoring Databases 68
Upgrading on Linux 70
Preparing to Upgrade on Linux 70
Running the Installer 70
Upgrading on Windows 71
Importing the OMNM MySQL Database 72

5 Troubleshooting Installation Issues 75

Appendix A: Installation User Interface 77

Index 81

1

Introduction

Introducing Product Installation

This section provides a high-level understanding of the tasks required to install or upgrade Redcell and the order in which to complete the tasks.

In This Guide – 7
Intended Audience – 7
Installation Overview – 8
Related Documents – 8

In This Guide

This guide covers the following topics related to the OpenManage Network Manager (OMNM) product installation:

- Introduction provides the guide content, intended audience, installation overview, and any related documents required.
- Preparing for Installation provides the tasks needed before you start the installation to ensure that you have all the system requirements in place to ensure a smooth installation.
- Installing OMNM provides the steps to install the product and verify the installation.
- Troubleshooting Installation Issues provides a list of issues that could occur during the installation process and how to resolve them.
- Installation User Interface describes all wizard fields and options where you need to input, select, or modify settings related to the installation process.

Intended Audience

This guide is intended for a system administrator, database administrator, and/or anyone else responsible for the installation and migration of the OpenManage Network Manager product.

The preparing for installation and preparing for migration information in this guide is useful for those responsible for planning a migration project or upgrading their system.

Installation Overview

The installation process installs the OpenManage Network Manager (OMNM) application, including its foundation class software. See Preparing for Installation on page 9 for system requirements and other prerequisites.

The OMNM application is not compatible with other software using the standard SNMP ports (such as 162), or other raw sockets. Either stop the conflicting application before starting the OMNM installation, or stop the OMNM application when you want to use the conflicting application. You may need to reboot your system to close conflicted sockets. To stop the OMNM application, close the Web client and stop the Application Server (see Stopping Servers on page 64).

Once you finish Installing the Application, you are ready to:

- **Discover Network Devices**
  Refer to the User Guide for detailed instructions, or right-click to create or use a profile in the *Discovery* portlet and enter the IP addresses you want to discover. You may need to enter SNMP and Telnet login/password combinations to fully discover equipment. Once you discover equipment, you can manage it.
- **Begin Managing your network**
- **Administer your application** (set up users, equipment access passwords, and groups for both users and equipment, as you begin to use it)

NOTICE

If you have complied with the prerequisites for installation and do not need basic instructions, see Performing Complex Installations on page 57 for instructions about how to install the application in complex environments that have distributed application, database and/or mediation servers, or clusters of these.

Related Documents

Here are the OMNM and third-party documents containing additional information related to the OMNM installation and migration tasks.

OMNM Guides

The following OMNM product documents contain additional information needed during OMNM installation:

-

Other Guides

You need not consult any third-party documentation during the OMNM installation.

2

Preparing for Installation

Preparing for Installation

This section provides what you need to prepare for Redcell installation or upgrade and how to start the applications used to do the preparation tasks.

Reviewing Pre-Installation Checklist – 10
Verifying Software Package – 12
Verifying System Requirements – 13
Setting Up User Accounts?? – 29
Installing Third-Party Software – 19
Setting Up Your RDBMS – 30
Collecting License Information – 31
Obtaining Info – 32
Understanding Best Practices – 33
Ports Used – 33
Linux Disk Partition Information – 34

Reviewing Pre-Installation Checklist

Table 2-1. Pre-Installation Checklist (Sheet 1 of 2)

Item	Task	Done
	Select devices (IP addresses) and ports to monitor.	
	Select an IP address for the OMNM server and then configure IP address as a management station and receiver of SNMP traps on each device.	
	Determine IP range of devices being discovered.	
	Determine if OMNM used SNMP V1, V2 or V3 to communicate with the device.	
	Determine telnet or SSH credentials for devices being discovered.	
	Determine HTTP/HTTPS credentials for devices being discovered (applicable only for campus devices).	
	Determine WMI credentials for server discovery.	
	Determine SNMP credentials for storage discovery.	
	Verify that firewalls have open ports between devices and your OMNM server. • Best Practice is to take down the firewall, install the application, then enable the firewalls)	
	Set up SNMP and telnet/ssh username and password credentials for the devices. OMNM uses these credentials to manage the devices.	
	Review device and OMNM release notes.	
	Make sure that the required software is installed.	
	Make sure you have an FTP/TFTP server for production systems. The OMNM internal FTP/TFTP server is for testing only.	
	Create an administrative user account and password on target installation server. **Note:** The user name **cannot** be admin, administrator, or root (Linux) or have spaces (Windows). Any of these conditions prevent the installer from running.	

	Create the install location with the proper permissions.
	The installer stops if the directory is not found. For sure on a linux system and you have to create it before the installation can continue.
	`sudo mkdir -p /dellemc/openmanage/networkmanager`
	`sudo chown :synergy /dellemc/openmanage/networkmanager`
	`chmod 770 /dellemc/openmanage/networkmanager`
	Note: The source directory should not be the same as the target installation directory.	

	Obtain the installer (media/download)	

Table 2-1. Pre-Installation Checklist (Sheet 2 of 2)

Item	Task	Done
	Synchronize clocks on all hosts where you install OMNM.	
	Make sure that you disable User Account Control before installing on a **Windows Server 2008** system. **Note:** Windows Terminal Server is not supported. The installer becomes no-responsive when the Data Execution Prevention (DEP) option is enabled. By default, the DEP option is disabled on Windows Server 2008, but is enabled on a Windows Server 2008 system running Terminal Server. Temporarily disable Windows Server DEP systems before installation. Set the win_install.exe file to Windows 7 or Vista compatibility mode if installing on **Windows Server 2012**.	
	Temporarily disable the system firewalls and any antivirus software before installation.	
	Close all other applications to eliminate port conflicts that prevent the installer from completing properly. For example, some applications use common ports for FTP, TFTP, Trap services, and Syslog services. **Note:** Any bash or cmd sessions left open may halt the installer.	
	Close and stop any additional OMNM processes before installation.	
	Allow time for the OMNM application, which installs as a service and starts automatically, to become fully operational after the initial installation.	
	Make sure that the source and target installation directories **are not** the same.	
	Start OMNM to test your installation.	
	Create a user and prepare for installation.	
	Make sure that the license has not expired. Once OMNM is downloaded, unzip the files to your system. Open the “license.xml” file located in the “install” subdirectory with WordPad and verify the license has not expired. Using an expired “license.xml” file prevents OMNM from operating properly. Contact your Dell Representative for a purchased or an extended trail license	
	Determine operating system’s default language. If the default language is not English and you want to install in Englise, remove the SynergyI8N.jar file from Synergy.zip file before installation.	

Verifying Software Package

Verifying System Requirements

System requirements depend on how you use the application and the operational environment. Your specific network and devices may require something different from the recommendations for typical installations.

Base the minimum configuration of any system on its expected peak load. Optimally, your installation should spend 95% (or more) of its time idle and 5% of its time trying to keep pace with the resource demands.

Make sure that you have all the required software installed and that you have adequate hardware to support your OpenManage Network Manager (OMNM) installation.

There is a conditional text problem here.

System requirementsvary depending on how you plan to use the OMNM application. Software Requirements

You must have the following software installed and operational before installing or upgrading the OpenManage Network Manager (OMNM) application. Refer to the product *Release Notes* for any last minute changes that occured after this guide was released.

Table 2-2. OMNM Software Requirements (Sheet 1 of 2)

Software	Requirements
Operating Systems	• Linux 64-bit versions 6.5, 6.6, 6.7, and 7.2 for Red Hat (Enterprise versions) or CentOS **Caution:** Can install only on an Solaris End User System level installation. You cannot install on a Solaris Core System Support installation. • Microsoft Windows Server 2008 R2, Windows Server 2012, or Windows Server 2016 **Note:** The OMNM installer validates operating system requirements during installation.
Web Browsers	• Chrome (V59 and above) • Safari (V10 and above) • Firefox (V54 and above) • Internet Explorer (V11 and above)
Databases	• MySQL 5.7.16 • Oracle 9i (9.2.0.5) up to Oracle 12c R1 (12.1.0.2.0) note that: **Note:** Oracle 12c does not support the miltitenant feature. And the OMNM application does not include Oracle JDBC drivers. You must set the ORACLE_HOME environment variable to the local Oracle installation directory. The OMNM application expects the Oracle home directory to contain bin and jdbc subdirectories. • Oracle 10g RAC or later for High Availability installations
VMware	• Linux Redhat/CentOS supported versions • Windows 2008R2 **Note:** System requirements for virtual machines are the same as physical machines, except the hardware must have the capacity for its own requirements and the virtual machine.
Perl	Version 5.10 or later (excluding 5.16) **Note:** This is not required for OMNM installation but it is required if you to take advantage of the Perl script capabilities

Table 2-2. OMNM Software Requirements (Sheet 2 of 2)

Software	Requirements
Protocols	• TCP/IP • SNMP • HTTP/HTTPS • UDP Multicast • CIDR
Adobe	• Flash Player (32-bit or 64-bit) • Reader
Java	• 1.6 or later

Hardware Requirements

Optimally, base the minimum configuration of your system on expected peak load. Typically a configuration running all elements of a system on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that creates, modifies, or deletes rules on tens or hundreds of thousands of business objects, your real system needs could be higher.

Hardware requirements vary depending on whether you have a single server installation or a distributed server installation.

Screen resolution must equal or exceed 1280 x 1024 pixels. Your screen must be at least 1250 pixels wide. Even in these circumstances, some cosmetic aberrations may occur (duplicate forms for one example). You can safely ignore such aberrations.

Single Server Hardware Requirements

The single server hardware guidelines provide suggested sizing for your OpenManage Network Manager system (Table 2-3).

△ CAUTION:
These hardware requirements assume you have a host dedicated to **only** the Redcell application. Other applications may compete for ports or other resources and can impair the system's performance.

When estimating the size of a deployment, it is important to understand the applications configurations in the target environment. For example, the most resource-intensive, demanding applications are Traffic Flow Analyzer (TFA), Event Management, and Performance Monitoring.

The **minimum hardware required** is 8-GB RAM, dual core CPU (2.8-GHz or better), 200-GB 10,000-RPM disk, which supports:

- Standalone single-server installations with **minimal** use of high-resource demanding applications
- Distributed installation of a single component server, such as application server only, Mediation server only, database server only, or Web server only.

The **minimum hardware recommended** is 10-GB RAM, four-core or more CPU (2.8-GHz or better), 400-GB 10,000-RPM disk, which supports:

- Standalone

If the network you manage exceeds these parameters, or your system monitors more devices than your hardware can handle, consult your sales representative about upgrading to a more robust or multi-server Redcell version.

Table 2-3. Single Server Hardware Requirement Guidelines (Sheet 1 of 2)

Max. Managed Devices	64-bit Operating System: Disks/RAM/ Hardware	Max. Concurrent Users	Performance Monitor Max. Targets	Max. Traffic Flow Exporters	Installation Changes to Heap Memory Settings
25	8GB RAM, single disk, consumer level PC	5	2500	5	Use defaults: (3GB application server heap, 512M database, 2GB Synergy Web Server)
50	10GB RAM, single disk, consumer level PC	8	5000	5	3-6GB application server heap, 512M database buffer, 2G Synergy Web Server
100	12GB RAM, single disk, consumer level PC	10	10000	10	4-7GB application server heap, 1GB database buffer, 3GB Synergy Web Server
175 - 250	14GB RAM, single disk, business level PC	15	25000	25	4-9GB application server heap, 1GB database buffer, 3GB Synergy Web Server
300 - 500	16GB RAM, single disk, business level PC	25	50000	50	5-10GB application server heap, 2GB database buffer, 3GB Synergy Web Server
1000	18GB RAM, multi-disk, server level PC	50	100000	100	8-12GB application server heap, 3GB database buffer, 5GB Synergy Web Server
2000	32GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	100	200000	100	10-14GB application server heap, 8GB database buffer, 8GB Synergy Web Server
2500	40GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	125	250000	125	12-16GB application server heap, 10GB database buffer, 12GB Synergy Web Server

Table 2-3. Single Server Hardware Requirement Guidelines (Sheet 2 of 2)

Max. Managed Devices	64-bit Operating System: Disks/RAM/ Hardware	Max. Concurrent Users	Performance Monitor Max. Targets	Max. Traffic Flow Exporters	Installation Changes to Heap Memory Settings
3000	48GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	150	400000	150	14-16GB application server heap, 10GB database buffer, 12GB Synergy Web Server
5000	64GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	175	600000	200	20-24GB application server heap, 16GB database buffer, 16GB Synergy Web Server
7500	80GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	200	850000	250	28-32GB application server heap, 20GB database buffer, 20GB Synergy Web Server
10000	128GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	225	1000000	300	38-44GB application server heap, 24GB database buffer, 24GB Synergy Web Server
Unlimited/ HA	RC Synergy can support an unlimited RTM license where there is no limit on the number of managed devices in inventory. The unlimited license is not sized or suggested for Standalone deployments. There are many factors to consider when sizing with an unlimited license. Refer to the install guide section "Sizing Overview" for more information on sizing..				

Distributed Server Hardware Requirements

The distributed server hardware guidelines are based on average OpenManage Network Manager application use on your managed network (Table 2-4). These guidelines include number of users, number of devices managed, Traffic Flow Analysis (TFA), Performance Management (PM), and Event Management (EM) as the most demanding elements.

Distributed installations consist of separate servers for separate functions within the OpenManage Network Manager system. Web Server (WS), Application Server (AS), Mediation Server (MS), and Database server (DB) are on separate hosts. The RAM, CPU and hard drive (HD) sizes for these are provided. All CPUs and/or cores should be 3.0GHz or faster.

For sizing recommendations not covered here, contact your sales representative.

Table 2-4. Distributed Server Hardware Guidelines

OpenManage Network Manager Use	Web Server (WS)			Application Server (AS)			Mediation Server (MS)			Database Server (DB)			Memory Allocation (Changes to default heap settings)			
	RAM (GB)	CPU	HD (GB)	RAM (GB)	CPU	HD (GB)	RAM (GB)	CPU	HD (GB)	RAM (GB)	CPU	HD	WS (GB)	AS (GB)	MS (GB)	DB (GB)
10 users 500 devices TFA [1] PM[4] EM[5]	4	Dual Core	40	4	Dual Core	40	4	Dual Core	40	4	Dual Core	1x 200 GB 7200RPM	2	3	3	3
50 users 1000 Devices TFA [2] PM[4] EM[5]	8	Quad Core	40	8	Quad Core	40	6	Dual Core	40	8	Quad Core	2x100GB 10K RPM RAID 0 or better striping or SSD	6	6	4	6
150 users 5000 Devices TFA[3] PM[4] EM[5]	16+	8 core	40	16+	8 core	40	6	5 x Dual Core [6]	40	16+	8 core	High Perf Disk Array 4 x 100GB 10K RPM or better. RAID 0 or better or SSD	14	14	4	14
150 users 10000 Devices TFA[3] PM[4] EM[5]	64+	8 Core	200	64+	8 Core	200	32	4 Core	200	32	8 Core	High Perf Disk Array 4 x 100GB 10K RPM or better. RAID 0 or better or SSD	20	20	6	20

[1] <2Mbs Internet egress and a 1:1000 sample rate.

[2] <10Gbs Internet egress and a 1:1000 sample rate.

[3] <200 Gbs Internet egress and a 1:1000 sample rate.

[4] PM supports 600 inserts per second using a single disk (SSD) Drive. 1 insert = 1 monitored attribute. Performance improves as you add drives and worsens with slower drives.

[5] EM supports a sustained 1200 traps per second using a single (SSD) drive. Performance improves as you add drives and worsens with slower drives.

[6] Mediation recommendations assume managing <1000 devices per host.

Preparing Linux for Installation

Prepare your Linux system for OpenManage Network Manager installation as follows.

1 Add your IP and hostname to the /etc/hosts file.

For example, add the following for the Test.localdomain host:

```
10.18.0.241 Test Test.localdomain
```

Verify that /etc/hosts file points to the new name. Use the cat command to see output with the correct IP Address/hostname pairs.

```
[qa@Test Desktop]$ cat /etc/hosts
10.18.0.241 Test Test.localdomain
```

Remember that the OpenManage Network Manager application requires a fixed IP address for its host.

2 Login as `root`, create a new user with a home directory, set the password, and add the user to the proper group.

For example, here are the commands to configure the *test* user:

```
useradd -m test
passwd abcxyz
usermod -aG wheel test
```

The wheel user group allows password-less `sudo`.

△ CAUTION:
If you are installing with an Oracle database, do not use `redcell` as the Oracle user name.

3 Copy the installation files to the local system on which you plan to install the OMNM application.

4 Make sure that the installation script has permission to execute:

```
chmod +x /home/test/MyInstallation/linux_install.sh
```

5 Create the target installation directory and set permissions as the root user.

The following are examples, not defaults:

```
sudo mkdir -p /installPath
sudo chown :test /installPath
chmod 770 /installPath
```

If the target install directory does not exist or it does not have write permission, an error message is displayed during installation. You must resolve this issue before continuing with the installation.

6 Disable Firewall with System > Administration > Firewall.

Alternatively, disable the firewall, and configure the Network Interface Card (NIC) with a static IP address from a command shell with the following command:

```
setup
```

You may be prompted to enter the root password. The password dialog may appear behind the Firewall Configuration Startup window.

7 Activate the Network Interface Card (NIC) as follows.

By default, some Linux distributions do not activate the NIC during startup.

```
nano /etc/sysconfig/networking/devices/ifcfg-eth0
```

Change `ONBOOT=no` to `ONBOOT=yes`

8 Set SELINUX to disabled in the `/etc/selinux/config` file.

```
SELINUX=disabled
```

9 Reboot your system from the command line.

This is required for step 7 and step 8 to take effect.

10 Login as root and update the system:

```
yum update -y
```

11 Remove mysql-libs from the system:

```
yum remove mysql-libs -y
```

Linux (CentOS particularly) sometimes installs MySQL libraries by default, this interferes with OpenManage Network Manager since it installs its own MySQL version. The installer checks for conflicting MySQL service and displays an error if conflicts are found. Resolve issues before continuing with the installation.

12 Configure file handle maximums in the /etc/security/limits.conf file and make sure that the following are at minimum 65535:

```
test soft nofile 65536
test hard nofile 65536
test soft nproc 65536
test hard nproc 65536
```

Here, `test` is the installing user login.

Set these limits higher for more heavily used systems. You can check/set file handles temporarily using the `ulimit -H/Sn` command. For example:

```
$ ulimit -Hn
$ ulimit -Sn
```

△ CAUTION:

If you enter ulimit -a in a shell, open files should **not** be 1024, and User Processes should **not** be 1024. These are defaults that **must** be changed. If you do not have enough file handles, an error appears saying not enough threads are available for the application.

13 Restart your Linux system.

```
reboot
```

Installing Third-Party Software

Installing Perl

The OpenManage Network Manager (OMNM) installation does not include the Perl package. If you want to take advantage of the OMNM application's use of Perl scripting capabilities, make sure that you install the Perl package on the application server and the mediation server host. Verify that the Perl executable is on the system path. If you install Perl after you install the OMNM application, reboot the host to ensure the path recognition.

NOTE:

The OMNM product requires the Perl Net::Telnet class. Execute perldoc *packageName* to make sure that you have the correct package. For example:

```
perldoc Net::Telnet
```

For more information about the Perl application, refer to www.perl.com. Follow the downloads link to find the recommended distribution for you platform. One of the recommended Perl packages is from ActiveState.

Beginning with Perl version 5.14, the switch module was deprecated. This version installs with the Cygwin update for Windows. After this update if you still have switch cases/scripts using `switch` statements, you need to install the switch.pm file manually by copying it into the following directories:

installationRoot`\oware3rd\cygwin\lib\perl5\vendor_perl\5.14`
installationRoot`\oware3rd\cygwin\lib\perl5\5.14`

You can use the switch.pm file from an older Perl installation or look online for it.

the following was copied from the admin guide work it into this section to have:

--- Installing Perl

--- Upgrading Perl

Perl

Perl

Before installing OpenManage Network Manager, install Perl to take advantage of OpenManage Network Manager's scripting capabilities. See Adaptive CLI Script Language Syntax on page 290 for some of those capabilities. Note that in versions 7.2.3 and later Perl comes installed (with Cygwin). See Upgrading Perl in this verion below for caveats.

You must install it on the path on the application server/mediation server host. Best practice is to restart the server so it recognizes the path, and to use Perl version 5.10 or later (however not 5.16). Some functions also require Perl as well as the Perl module `Net::Telnet`, so make sure that whatever Perl you install includes that module. If it is not installed, `Net::Telnet` and other modules are available at www.perl.com/CPAN.

NOTICE

Running `perldoc [package name]` (for example `perldoc Net::Telnet`) lets you know whether your system has the relevant package.

Since it is freely available on the internet, Perl is not included in OpenManage Network Manager's installation. You can find information about Perl at www.perl.com. Follow the downloads link to find the recommended distribution for your specific platform. One recommended Perl package is from ActiveState, accessible at: www.activestate.com/activeperl/

Upgrading Perl in this verion

Perl v. 5.14 deprecates the `switch` module. This version is installed with the Cygwin update for Windows in this version and later. After this update if you still have `switch` cases/ scripts using `switch` statements, then you must install `switch.pm` manually.

To install `switch.pm`, copy that file into the following directories under Cygwin:

```
[installation root]\oware3rd\cygwin\lib\perl5\vendor_perl\5.14
[installation root]\oware3rd\cygwin\lib\perl5\5.14
```

You can use the `switch.pm` file from an older Perl installation or look online for it.

If you see an error saying `Can't locate Net/Telnet.pm` in Linux environments, you can resolve this issue by installing Net::Telnet with the following steps:

1. Log in as root user
2. Execute `#perl -MCPAN -e'shell'`
3. `Cpan> install Net::Telnet`

Basic Network Considerations

The OpenManage Network Manager (OMNM) application communicates with devices over a network. In fact, you must be connected to a network for the Application Server to start successfully. Firewalls, or programs using the same ports on the same machine where this application is installed can interfere with its ability to communicate with devices. Refer to the User Guide.

Your network may have barriers to communication with this software that are outside the scope of these instructions. Consult with your network administrator to ensure this application has access to the devices you want to manage with the protocols described below.

NOTICE

One simple way to check connectivity with a device is to open a command shell with Start > Run `cmd`. Then, type `ping [device IP address]` at the command line. If the device responds, it is connected to the network. If not, consult your network administrator to correct this. No useful information comes from disconnected devices.

Consider	Description

Name Resolution	The OMNM application requires resolution of equipment names, whether by host files or domain name system (DNS). If your network does not have a DNS, you can also assign hostnames in the following file on a Windows system:
	`%windir%\system32\drivers\etc\hosts`
	You must assign a hostname in addition to an IP address in that file. Here are some example hosts file contents (including two commented lines where you would have to remove the # sign to make them effective):
	`# 102.54.94.97 rhino.acme.com # source server`
	`# 38.25.63.10 x.acme.com # x client host`
	`127.0.0.1 localhost`
	Caution: This software **only** supports installation to a local file system. **Do not** install to shared drives.

Consider	Description
Protocols	The OMNM application uses the following protocols: • TCP/IP • SNMP • HTTP • UDP Multicast You can bypass multicast, if it is disabled on your network. To allow a client to connect without multicast, add the following property to the client's owareapps/installprops/lib/installed.properties file. `oware.application.servers[Host1 IP address], [Host2 IP address]...`
Fixed IP Address	The OMNM application includes a Web server and must be installed on a host with a fixed IP address. For demonstration purposes, you can rely on dynamic IP address assignment (DHCP) with a long lease. However, this is not recommended for production installations. See Web Portal Installation on page 27.

Windows Prerequisites

This application requires a temp directory on the host where it is being installed. If the install launcher cannot extract a Java Virtual Machine (JVM), then it cannot run. The launcher extracts a JVM to a temp directory and then starts the installer main using this temp JVM.

Windows typically has a temp directory, `WINDOWS\temp`. Installation expects that TEMP or TMP environment variable exists and points to this temp directory (check in a command shell with `cd %TEMP%` or `cd %TMP%`).

You can also execute the `win_install.exe` installation from a command line to override temp directory locations with this command line:

```
win_install.exe -is:tempdir c:\mytemp
```

Although it is not always necessary, during installation or uninstallation a suggested option is to disable any virus protection software, and any other running applications. Some applications have additional services (like Norton Unerase) that prevent correct installation on some systems. Stop these in Services in Control Panel's Administrative Tools.

This application cannot co-exist with other installations of Cygwin on the same Windows computer. Do not install it where Cygwin is already installed, either separately or as part of another application. If Cygwin is already installed, remove it before installing this application.

If they are present, turn off Microsoft Windows SNMP Services and Traps.

LinuxPrerequisites

If you are installing on Linux, you must log in as a non-root user. The Linuxinstallation prompts you to run some additional scripts as root during the installation process.

△ CAUTION:

Do not log in as root and su to a non-root user. Make sure your login automation does not do this either. This causes problems, particularly with upgrades.

When installing to Linux, make sure that you are installing as a user with the correct permissions, and are in the correct group. You must configure the installation directory so this user and group have all permissions (770, at least). You may install without any universal ("world") permissions. However, you must create a home directory for the installing user.

NOTE:

All files created during installation respect a umask of 007. All files from the *operatingSystem*.jar file are 770. Files from ocpinstall -x are set for 660. Bin scripts from ocpinstall -x are 770.

Best practice is to install as the user designated as DBA. If necessary, create the appropriate user and login as this user for running the install program. The installing user must have create privileges for the target directory. By default, this directory is:

`/opt/dorado`

CAUTION:

Linux sometimes installs a MySQL database with the operating system. Before you install this application, remove any MySQL if it exists on your Linux machine. Make sure to remove or rename the my.cnf file for that previous installation. If it is on the path, it can interfere with the correct operation of OpenManage Network Manager. See MySQL Server Configuration File Examples on page 21 for more about configuring MySQL.

NOTE:

To set the environment correctly for command line functions, after installation, type `oware` (or `. /etc/.dsienv` in Linux—[dot][space]/etc/[dot]dsienv) before running the specified command. **Also:** This application can run on any Linuxdesktop environment (CDE, KDE, Gnome, and so on) but the installer will only install shortcuts for CDE.

System Capacity

System requirements for each element of your system vary depending how you use it. The numbers in this guide are suggestions only, not definitive recommendations.

You should base the minimum configuration of any system on expected peak load. Typically a configuration running all elements of the application on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that could run create, modify or delete rules on tens or hundreds of thousands of business objects, your system requirements may be much higher. See System Basics on page 14 for more specific hardware recommendations.

Paths

Paths in this document are often written as Linuxrepresents them, with foreslashes (/) rather than Windows/DOS backslashes (\). The shell command `oware` makes any shell subsequently emulate a bash shell. That means either foreslash or backslash can accurately represent path separators as they may appear, depending on whether the `oware` command has set the environment to bash

emulation. Most shell commands for this application are available in Windows/DOS equivalents structured to call the emulator, then a bash script. If you have difficulty using a command line script in Windows/DOS, then try it after you have run `oware` or `. ./etc/.dsienv`.

NOTICE

Run command line scripts with -? to see their parameters.

CAUTION:
Do not install to paths with spaces in their names.

The OpenManage Network Manager (OMNM) product supports the following installation and configuration types:

- Hardware Requirements on page 14, whether embedded (MySQL) or Oracle,Enterprise (Distributed) Edition
- Clustered Edition
- Db High Availability Edition

Hardware Requirements on page 14, whether embedded (MySQL) or Oracle,Enterprise (Distributed) Edition

Distributed installations are suitable for most larger network environments in service providers and Enterprises.

Distributed means web server, application server, mediation servers are installed in separate servers without the clustering capabilities provided by the cluster edition.

A sinlge db server may also be distributed. If more than 1 db is required for redundancy (ie., RAC,MHA or Replication), then the DbHA edition license is also required.

To make an installation distributed, install components with the *Custom* installation option, and point them to the same partition (by default named for the Application Server's hostname concatenated with the word "partition").

NOTE:

In distributed installations, by default, installing an Application server by itself means the Mediation server process it ordinarily includes in stand-alone installations is turned off. You can put the following property in \owareapps\installprops\lib\installed.properties to turn it back on:

```
oware.appserver.mediation.setup=true
```

Databases on Separate Servers

If you are installing an Oracle database, you must put it on a separate host. See Oracle Database Management for more about that.

You can also install MySQL to a separate host. If you do this, on the (primary) appliction server, you must run `loaddb` after installing it, and run `dbpostinstall` to seed the components. Run `loaddb -s` when the web server is on a different host.

If your system's web server and database server are on different machines, you must run `loaddb -s` on the web server host to create the Synergy/portal database.

Adding Mediation Servers

You can add more mediation servers later in such installations with the *Custom* installation. You must point them to the Application Server partition during installation, and designate whether they are clustered pairs that fail over.

Often, such distributed installations use multicast to discover components. The command line (`startappserver` or `startmedserver`) -m parameter specifies that mulitcast address, or you can specify it in the `owareapps\ installprops\lib\installed.properties` file with the `oware.application.servers=[Host IP address]` property for autostart installations.

Multicast is optional, however, and you can disabled it if, for example, a firewall blocks multicast between components. See Disabling Multicast on page 191 for the way to configure the alternative (a non-clustered mediation server setup example also appears in Performing Complex Installations on page 57).

NOTICE

You can elect to ping mediation servers before attempting to call a rule. This avoids the long timeout that can occur when the mediation server's network cable gets unplugged. To enable this, add a property (`com.dorado.ping.medserver=true`) to `installed.properties` for each application server. Ping incurs some additional overhead incurred, so by default, the property is not set and no ping occurs before rules.

Enabling Mediation Server in the Web Portal

To enable mediation server portal modify and rename the following properties file: `oware/synergy/conf/server-overrides.properties.sample`

Uncomment the property `medserver.support=true`, and rename this file to omit the .sample extension.

Clustered Edition

If you cluster components (in addition to distributing them), OpenManage Network Manager lets you use the following features:

- Application Server clustering
- Mediation server load balancing (with the Application Server round robin process)

NOTE:

This does not support database replication (you must upgrade to Db HA edition)

Clustered servers can process using a round-robin method so that systems are protected from server failure. Also, with distributed mediation servers (also called mediation agents), the system can handle a larger number and volume of traps and events. This is usually used with even larger systems, or when the server will be processing a lot of traps (for example, 1-20 traps per second, bursting to 100 tps).

When you are installing a high availability system, installation includes a setup screen for the Config Server (the primary server in a cluster). The cluster's multicast address is configured automatically. Fill in these values if you are installing a clustered or high availability system.

The following are some clustering considerations. For additional details consult Clustering.

- Clustering does not require DNS entries for all servers.

- Servers (Application or Mediation) in a cluster need to share the following two pieces of information:

  Partition Name - Some unique string for this cluster, beginning with a letter. You can configure this name one of several ways for clustering:

  – Command line: - typical for testing

  – installed.properties - the command line overrides this property file.

  – pmstartup.dat - settings used by automatic server startup (i.e., Windows Service)

NOTE:

See Performing Complex Installations on page 57 for a real-world example of such an installation.

Mediation Listeners as Redundant Peers—For mediation server clusters, you can also elect to either send redundant messages to each server, or to have each server process messages independently. Select the former for a high availability mediation pair.

Db High Availability Edition

The optional Db High Availability (Db HA) capability installs automatically and makes the Application Server clustered and load balanced. Normally used in carrier-class or very large deployments.You can also configure Oracle or Mysql database installations for failover (see Oracle Failover on page 87).

NOTICE

You can test failover by stopping a server process.

In this edition, primary and secondary paired mediation servers use configurable heartbeats to monitor each others status. If the secondary mediation server detects that the primary is down, it will take over. The Application Server also monitors the mediation server and will generate an event/alarm if the primary mediation server goes down. Configurable trap buffers reduce trap loss during failover.

Primary and secondary clustered Application Servers also use configurable heartbeats to monitor each others status. If the primary fails, the secondary will take over and will also generate an event/alarm. Clients and mediation servers identify applications servers by partition name. This is the same for the primary and secondary Application Server, so the failover is transparent to the clients and mediation servers.

If you want to extend this to the database, Oracle Real Application Clusters (RAC) handle database replication, synchronization and failover. Application Servers identify Oracle by Service Name which is the same for all Oracle hosts, so failover between Oracle hosts is transparent to this application.

You can also have a form of Db HA at the application level with transaction management. For example:

Db HA installations support the following:

- Application Server clustering
- Mediation server load balancing (with the Application Server round robin process)
- Mediation server failover
- Supports Database redundancy (must have Oracle Parallel Server, Oracle's Real Application Cluster [RAC], Mysql replication or MHA or equivalent database).

Clustered Mediation Servers

For reliability, paired Mediation servers can fail over when they transmit SNMP traps and/or Network Element-initiated Syslog Messaging to Application Server(s). For failover to work, you must enable multicast between the cluster's mediation servers.

Each server in the cluster has a primary and a secondary role, and uses keep-alives heartbeats to verify the other Mediation server's operational state. Based on the operational state, only one Mediation server (the primary) forwards messages to the Application Server(s) for processing.

NOTE:

You must configure Network Elements to send SNMP traps and/or Syslog messages to all servers.

See Mediation Clustering on page 209 for more specifics.

Web Portal Installation

By selecting one of the custom installation options during the installation process, you can install OpenManage Network Manager's web server on a separate machine. This is particularly desirable if you plan to support a larger number of web clients (see System Basics on page 14 for sizing information).

When you install a separate web server, installation assumes you have already installed the application server, and can supply its IP Address / Hostname, a port where web server communicates with application server, and a heap size for this server. The default heap is 1G, but you can configure a larger heap to support more clients. The default port is 8089. Make sure no firewall restricts communication between application server and web server on this port. See the User Guide for information about installing with SSL.

Since the web portal needs a database, installing the Web portal also means you must select the database type (MySQL or Oracle) and location host and port number. The port default: 3306.

As in the Complete installation, the Web server starts automatically once installation is complete. In Windows, right-click the Apache Web server icon to Configure it (heap size, for example), Start and Stop this service. See Starting Application Server on page 50 for complete instructions, including Linux.

You can change the appserver IP reference in the `portal-ext.properties` (location: `\oware\synergy\tomcat-x.x.xx\webapps\ROOT\WEB-INF\classes`).

The URL for the portal itself on port 8080 on any IP address where it is installed, including 127.0.0.1 if you access it from the host where the web server itself is installed.

Application Server Installation

To install only the application server, select that option in the *Choose Install Set* screen that appears in the installer. As in most installations, and as is essential for distributed installations, you must select a partition name, whether the server starts automatically on host startup, the heap size, database type and location (host and port).

Compatibility with Previous Versions

The impact of the above behavior on previous mediation versions occurs only where no preferred mediation server is available. Before such behavior was available, the application made an arbitrary selection from any available mediation servers, possibly using the same server every time. Now, only the local application server can handle the request. If you have configured the application server to

perform mediation (true by default), then the system should continue to execute these requests as it had in the past. If the application server is not configured to perform mediation, then requests may fail with `no mediation` errors instead of being routed to the wrong mediation server possibly resulting false `device not available` errors.

Configuration Options

By default, each mediation server has a single network mask established during installation. Each mediation server in a cluster or HA Pair should yield the same network address when the default mask is applied to the mediation server's IP address. Here is an example of a default mask setting on a mediation server:

```
oware.mediation.subnet.mask=255.255.255.0
```

In addition to the default mask, you can define additional routing configurations as application server properties. Each application server in a cluster should have the same settings. You can add more IP Addresses and/or masks to the default configuration made locally on the mediation server for each mediation server partition. The property name is `com.dorado.mediation.routing` with a mediation partition name appended. Here is an example of routing requests for any device IP address starting with 10.10 to a mediation server named `foo-medPartition`:

```
com.dorado.mediation.routing.foo-medPartition=10.10.0.0;255.255.0.0
This appends Partition to the partition name. For example
  com.dorado.mediation.routing.rcellmedPartition=172.16.0.0;255.255.0.0
```

The syntax for routing configuration values is as follows:

```
ipAddress;mask[,ipAddress;mask]
```

Basically, you can add more IP and mask pairs as comma delimited values. If you omit the mask, then assumes it is 255.255.255.255. If you omit the IP address, then assumes the address is the mediation server's IP address. If an IP address or mask is not valid, a warning appears once in the application server log when the properties load. If one of several values for a single property is not valid, still applies the other setting.

The application server itself performs mediation when no agents are available. This is required unless your deployment includes at least one mediation server. All application servers in a cluster must have the same configuration. To disable mediation services on an application server after you have configured a distributed mediation server elsewhere, add the following property on the application server (preferably in `installed.properties`):

oware.appserver.mediation.setup=false

Setting Up User Accounts??

Setting Up Your RDBMS

Collecting License Information

Once OMNM is downloaded, unzip the files to your system. Open the “license.xml” file located in the “install” subdirectory with WordPad and verify the license has not expired. Using an expired “license.xml” file prevents OMNM from operating properly. Contact your Dell Representative for a purchased or an extended trail license.

Obtaining Info

Table 2-5.

Understanding Best Practices

Table 2-6. Installation Best Practices

System/Component	Best Practice	
Single Server Hardware	• Review and understand the different deployment options and requirements • Choose expandable hardware for future expansion • Use a single server for ease of management and deployment	
High Availability (HA) Hardware	• Use as few as two servers for ease of management	
IP Address	• Have a permanent IP address for your system • Refer to the "Fixed IP Address" instructions in the User Guide if your system uses DHCP and the IP address changes after a completed installation	
Firewalls	• Disable system firewalls before application installation • Enable the firewalls after installation	

Ports Used

This application uses the following ports. Ensure your firewalls or other network security measures do not block these ports.

Port Number	Used by...
1098	Naming service (JNDI)
1099	Naming service (JNDI)
3100	HA Naming Service (JNDI)
3200	HA Naming Service (JNDI RMI)
4444	JRMP invocation (RMI)
4445	Pooled JRMP invocation (RMI)
6500 to 6510	Mediation cut-through
80	HTTP
443	HTTPS
8093	JMS

The client HTTP cut-through goes directly to the device from the client. So, you must get to devices via port 8080 to cut-through to the embedded web server. Telnet cut-through goes directly to the application server as a proxy on ports 6500-6510.

The following ports are seldom required, but are listed here in case present or future functionality requires them:

Port	Used by...
23	Telnet
1103	JNP Discovery
1123	JNP REPLY

Linux Disk Partition Information

Suggested partitioning includes separation into several partitions including /, swap, /usr, /opt, and /export/home.

/ (root)—The root partition contains everything that is not specifically placed on a slice/partition. The rule of thumb here is: Do not put data on this partition that is likely to grow significantly (logs, applications, data, and so on). This partition can be as little as 200MB, however best practice indicates as much as 2GB if space is available.

swap—swap is the space allocated for the operating system to use as part of its virtual memory to augment physical memory. If something in memory has not been used for a while, the operating system will move it to disk temporarily. Recommendations for this are typically for two to three times the physical memory, however we usually determine the amount available based on physical memory. If you have 512MB, specify 1.5-2.0GB. As physical memory increases, still specify 1-2 times the physical memory so you have enough disk space for the operating system. The following are instructions about setting swap:

a. Check your current swap space setting with `swap -l`

b. su to root (if not already).

c. Issue `mkfile (size required) (filename)`

d. Execute `swap -a (pathname)`. this adds the swap file. You *must* use an absolute path name

e. Check with `swap -l` to confirm the new swap addition.

/usr—Typically holds operating system commands and utilities related to the operating system. `/usr` can also contain the documentation associated with these commands. This partition should be a minimum of 1.5GB for a full installation. Best practice is to specify 2GB and potentially more if you know you will be adding operating system utilities.

/etc—We recommend this be located on the root partition, not on its own partition. The data here may change from time to time, but the typically does not grow significantly.

/var—Best practice is to create a partition for `/var`. This contains the syslog data, print spool, mail, and so on. This partition could grow significantly from the required amount of disk space depending on the applications running on the system. We recommend you allow at least 2GB.

/opt—The `/opt` partition holds application software that is added to the system. Redcell would be an application that should be installed here. The size of this partition should depend on the required disk space for applications including Redcell. Both the application's software and data reside in the same directory structure, however, so you can add more volumes to another partition.

/export/home— `/export/home` is typically for user data. Most systems have user home drives specified in this space (for example: `/export/home/auser`). This should have enough space for all user data.

/<some_partition_name>—With a RAID configuration, you can specify a large amount of disk space for data purposes.

3

Installing OMNM

Installing OMNM

Before installing the product, make sure that you have performed all the pre-installation tasks discussed in Preparing for Installation on page 9.

For a description of the installation wizard and the different fields and options, see Installation User Interface on page 77.

Installing the Application – 38
Uninstalling the Application – 63

Installing the Application

The steps required to do an installation depend on the operating system on which you plan to install and whether you plan to do a single- or multi-server installation. This section provides the following instructions for some of the different installation situations:

- Installing on Linux
- Completing Post-Installation Tasks
- Verifying Your Installation
- Installing on Windows
- Installing OMNM Silently
- Installing Licenses
  - Starting Application Server
  - Application Password
  - Starting Application Server
- Installing on Linux from the Command Line
- Performing Complex Installations
  - Startup Sequence for Initial Testing
  - Stopping Servers

Installing on Linux

Install the OpenManage Network Manager (OMNM) application on a Linux/Solaris system as follows.

1.Log in as a non-root user credentials.

The non-root user must have permission to create directories in the selected installation path. Installing to a directory that requires root level access fails.

2.Start the installer using one of the following methods:

- Insert the media into its drive and start the installer for the appropriate operating system.

  You cannot install from a directory whose name begins with @. You must also extract any compressed (zipped) installation source before executing the installer.

- Enter the following commands on Linux:

  ```
  cd /MyInstallDir/
  ./linux_install.sh
  ```

  If you want to run the installer from the command line, see Installing on Linux from the Command Line on page 56.

- Enter the following commands on Solaris:

  ```
  cd /MyInstallDir/
  ./
  ```

  The installation starts and reminds you to shut down other running software (this may include anti-virus software). Click Next.

3.Follow the installer instructions and provide input as needed, such as:

- Accepting the license agreement
- Selecting the install location
- Selecting a setup type
- Providing the location to store product icons, partition name, heap size, and so on
- Selecting a default IP address for use by the software on a multi-homed machine (multiple NICs)
- Selecting they type of database (MySQL/Oracle)

During the install process, the installer performs a series of system checks to verify that the target system supports the OpenManage Network Manager application and the required ports are available.

If you are installing the software on a machine with multiple network interface cards (NICs), the installer prompts you to select one IP address for the system on which you are installing.

Click *Next.*

Enter the partition name if your desired name differs from the supplied default, and insure it starts with a letter, and select whether to autostart. Click *Next.*

Click *Next.*

4. If installing to a multi-homed machine (multiple NICs), choose a default IP address for use by the software. Installation automatically records this address. C lick *Next.*

   You can add the following properties to `owareapps\installprops\installed.properties` to override portions of the IP selection's impacts:

```
#
# specific interface used for all NMS initiated
# communications to the network
com.dorado.mediation.outbound.address=localhost
#
# specific interface used for binding mediation
# listeners such as SNMP trap listener
com.dorado.mediation.listener.address=localhost
#
# specific interface used for all northbound
# communications to external management system(s)
com.dorado.mediation.northbound.address=localhost
```

   For any property, replace the *localhost* text with the correct IP. Refer to the *OpenManage Network Manager User Guide* for more on overriding properties.

   During a fresh install or upgrade, the installer checks for a running third-party MySQL instance. If there is an existing service named MySQL, a conflicting software found warning is displayed. Here are your options:

   - Continue with the installation and the OMNM installer stops the running MySQL service and then creates and starts its own service named MySQL.

     Note that the preexisting third-party MySQL instance and any of its related databases are not deleted. Only the service is deleted and recreated.

- Return to previous windows and select an installation option that does not include the database.

5. If you are installing on Linux, you must run a setup script in a separate shell, logged in as root user. Installation prompts you to run a generated script after the install phase finishes. This script records information in case you need technical assistance and installs some files as root. Open a new shell, log in as root, and run the listed script (`$OWARE_USER_ROOT/install/root/setup.sh`).

   This step installs some essential environment files. It does not check for patches (the installation does that). The contents of `patch_check.log.timestamp` now appear embedded in `setup.log`.

6. **MySQL:** The installer either builds the database for first time use or prompts you to rebuild it if a database already exists. Building the database for the first time may take several minutes to complete.

   If you installed MySQL on a separate server, you must run `dbpostinstall` on the (primary) appliction server too whenever you upgrade our change your system.

CAUTION:

Ensure your Linux package has not already installed a version of the MySQL database. If it has, uninstall that database before proceeding. **Also:** Do not configure and/or install a database larger than the available disk space.

NOTICE

Regardless of the initial database size, post-installation configuration of Database Aging Policies (DAP) can have a significantly impact on how fast it reaches its capacity. The default DAP for alarms, for example, never cleans open alarms from the database. Similarly, defaults for archiving event history may not suit your environment. Consult the *User Guide* for details about tuning these policies.

7. **Oracle:** For Oracle databases run the following command lines:

```
loaddb -u system -w manager
loaddb -u system -w manager -s.
```

   If `loaddb -u system -w manager` does not work the first time, add -d. You must run the command line both with and without the -s. Then run:

```
dbpostinstall
```

   Oracle Database Management addresses fine-tuning these installation steps.

8. When you install the Application Server service, the installer prompts you to start the service without rebooting again. If you elect to start the Application Server service, a yellow monitor icon appears in the Windows system tray and it turns green when the service is up and running.

   To confirm an automated-starting Application Server is running, you can run `pmgetstatus` in a shell. Both Application Server and Web Server (status indicated by the Apache icon in Windows) must be completely started before you can open the client.

9. Finally, the application prompts you to click *Done*.

10. After you complete the installation, you may want to install Adobe Acrobat Reader. You can download a free copy from www.adobe.com. This application requires Acrobat to successfully print reports.

Additional post-OpenManage Network Manager installations can also include Perl and FTP/TFTP servers. See Installing Perl on page 16 and Setting Up FTP / TFTP on page 30.

See Starting Application Server on page 50 for instructions about running what you have just installed.

Completing Post-Installation Tasks

Verifying Your Installation

Installing on Linux

To run OpenManage Network Manager (OMNM) on a Linux system, follow the Best Practices: Linux.

Best Practices: Linux

- OMNM runs on any Linux desktop environment (CDE, KDE, Gnome, and so on).
- Most Linux intstallations include lib-apr for Tomcat. This application requires it, so if you have customized your Linux hosts to omit it, put it back.
- Make sure any third-party firewall or the Linux IP Tables firewall is off or allows traffic on the ports needed for your installation. See the *Ports Used* section of the *User Guide* for specifics.
- Install your Linux distribution (example: CentOS) on the server, choosing *Basic Server* when prompted to select software. *CentOS* should be the only repository selected. Choose *Customize Later* to decline further customizing the installation.
- The Xvfb process must be running to have a Web client work correctly. This is automated when the application server starts automatically. You can manually start the Xvfb process with root access using the following:

  ```
  [root@test X11]Xvfb :623 -screen 0 1152x900x8 2>/dev/null &
  ```

  Verify that the Xvfb process is running as follows:

  ```
  >ps -ef | grep Xvfb
  root 25991 21329 0 16:28 tty2 00:00:00 Xvfb :623 -screen 0 1152x900x8
  qa 26398 26053 0 16:31 pts/3 00:00:00 grep Xvfb
  ```

  (The path may differ from this example.)
- If you are installing with an Oracle database, do not set the Oracle in OMNM to user `redcell`.

Post Installation

The following commands work only if you elected to autostart your system during installation. When running these commands ($service oware start/stop/status) with the installing user, Redcell prompts for the user's password

1.To start the application server:

```
root > /etc/init.d/oware start
```

2.To check the status of the application server:

```
root > /etc/init.d/oware status
```

3.To start the web server:

```
root > /etc/init.d/synergy start
```

4.To check the status of the web server:

```
root > /etc/init.d/synergy status
```

5.When application server and web server have completed their startup, open a browser to this URL: *appServerIP or hostname*:8080

Install OpenManage Network Manager:

6.You cannot install as root user, so, if necessary, log out as root and login as the user (here, `test`) created in the previous steps and run the installation script:

```
cd /home/test/MyInstallation
./linux_install.sh
```

...or if you prefer a text-only installation:

```
./linux_install.sh -i console
```

7.Now follow the instructions in the installation wizard or text, making sure to specify the configured target directory (in this example `/test/`*`installPath`*) as its installation root.

Application files are installed in the *installLocation*/OpenManage/Network Manager directory.

8.As part of the installation, you must run a specified installation script as root. When you run the setup script, among other things, it automatically re-routes event/alarm traffic from port 162 to port 8162.

NOTE:

You may see benign errors during the root portion of the Linux installation. Installation always attempts to find the CWD (current working directory). If another process deleted it, an error appears before the script runs. The error is benign and the script still runs, using a temp location controlled by the operating system.

9.If you did not elect to autostart them, start the web server and/or application server. The command line for application server:

```
startappserver
```

For web server.

```
/etc/init.d/synergy start
```

10.When application server and web server have completed their startup, open a browser to this URL: `[application server IP or hostname]:8080`

NOTE:

When you log in, if you see the message "Credentials are needed to access this application." Add `oware.appserver.ip=[application server IP address]` *to* `/oware/synergy/tomcat-XXX/webapps/ROOT/WEB-INF/class/portal-ext.properties`.

Installing on Windows

The instructions are the same for Linux and Solaris installations except where noted. Install the OpenManage Network Manager (OMNM) application on a Linux/Solaris system as follows.

1.Navigate to the win_install.exe file

2.Start the win_install.exe installation wizard.

The introduction window displays a welcome message and product description. Click Next to advance through the information and instructions throughout the installation process.

3.Accept the license agreement terms to install OMNM.

4.

1.Log in as a user with administrator's permissions on the Windows machine where you want to install the software or as any non-root account on Linux.

do ***not*** use a name containing spaces.

2.If you are installing from CD, insert it into its drive.In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run the `win_install.exe` shortcut from a file manager.

3.You cannot install from a directory whose name begins with @. *Also:* You must extract any compressed (zipped) installation source before executing the installation.

4.A dialog appears as the Setup program initializes the installation wizard, then it reminds you to shut down other running software (this may include anti-virus software). Click *Next.*

5.Installation performs a series of system checks to verify that the target system supports the OpenManage Network Manager application and the required ports are available. If all checks pass, the license agreement appears. You must accept the license to proceed. Click *Next.*

If you are installing the software on a machine with multiple network interface cards, installation prompts you to select one IP address for the system you are installing. *Also:* Windows 2008 may not support the installer finding the host's IP Address. In such cases, a screen appears where you can enter the IP address and Partition Name for your installation.

6.A Component Summary Screen appears, listing the package you are about to install. Click *Next.*

7.Another screen reminds you to shut down other applications, Click *Next.*

8.If you are upgrading from a previous version, the next screen detects it. The next two screens suggest best practice is to backup the database, and ask whether to re-build the existing installation's database. See Upgrading/Patching from Previous Versions for more about what to expect in upgrade installations.

9.The next screen lets you select the directory where the application installs. If you want to install to a different directory, type the path or click *Choose* to select another in a directory browser.[1] After confirming the installation location, click *Next.*

10.Select the setup type from the available options.

Complete—Installs the application server, database server, mediation server, and client on the host.

If you selected *Oracle* as your database (on a separate machine) a subsequent screen prompts you for the Oracle connection details when installing an Application Server with Oracle as the chosen DBMS. Fill in initial values for Logon User and Password along with the Host, Port and SID.

Application Server—This leads to screens where you confirm the hostname (by default the existing machine's name), heap size, and database location. Refer to *OpenManage Network Manager User Guide* for more about setting heap size for this and web server.

In a subsequent screen you must confirm whether to install the Application Server as a service (or daemon); you can also elect to start it manually. See Starting Application Server on page 50 for more information on autostart. [1]

Web Portal—This series of screens prompts you for the location of the web server (IP / Hostname and port), and its memory heap. Application server must already have been installed for this selection. Separate web servers are recommended when more web clients access your system. See System Basics on page 14 for more sizing advice.

Custom—This leads to screens where you can select from among the available features to install. These include Application Server, Web Server, Mediation Server, or Database.

If you install a mediation server, you must enter the Redcell partition it addresses, accept or alter the subnet mask for it. By default the subnet mask is 255.255.255.0. This mask represents the portion of the network serviced by this agent.

If you install to a stand-alone database, you can select from either the included MySQL or Oracle.

MySQL installation asks you to specify the data path, a minimum and maximum size. If you specify no maximum, then the database will grow until the disk is full. Best practice is to configure Database Archiving Policies (DAPs) to prevent a full disk. See Database Management.

Oracle does not install an Oracle database, but points the application server to an Oracle instance that must already be installed. You must specify its User, Password, Host, Port and SID in subsequent screens.

In the screens for these alternatives, you can also check *Autostart* to have the installed.[2]

Click *Next*.

1. In Linux, if you try to install to a location where you do not have write permissions, the installer fails to create the target directory structure. You must have permission to create the directory as the user running the installation. If not, log in as root and either create the target directory and configure permissions or grant permissions on the parent directory so user can create a subdirectory later (during installation).
1. You must also include a medserver configuration for the application server to perform mediation tasks. If you do not, then the application server's mediation capabilities are disabled. If some time later you want to disable mediation capabilities configured here, you can add oware.appserver.mediation.setup=false to the installprops/lib/installed.properties file.

Click *Next.*

Enter the partition name if your desired name differs from the supplied default, and insure it starts with a letter, and select whether to autostart. Click *Next.*

Click *Next.*

11. If installing to a multi-homed machine (multiple NICs), choose a default IP address for use by the software. Installation automatically records this address.Click *Next.*

    You can add the following properties to `owareapps\installprops\installed.properties` to override portions of the IP selection's impacts:

    ```
    #
    # specific interface used for all NMS initiated
    # communications to the network
    com.dorado.mediation.outbound.address=localhost
    #
    # specific interface used for binding mediation
    # listeners such as SNMP trap listener
    com.dorado.mediation.listener.address=localhost
    #
    # specific interface used for all northbound
    # communications to external management system(s)
    com.dorado.mediation.northbound.address=localhost
    ```

    For any property, replace the *localhost* text with the correct IP. Refer to the *OpenManage Network Manager User Guide* for more on overriding properties.

    During a fresh install or upgrade, the installer checks for a running third-party MySQL instance. If there is an existing service named MySQL, a conflicting software found warning is displayed. Here are your options:

    - Continue with the installation and the OMNM installer stops the running MySQL service and then creates and starts its own service named MySQL.

      Note that the preexisting third-party MySQL instance and any of its related databases are not deleted. Only the service is deleted and recreated.
    - Return to previous windows and select an installation option that does not include the database.

12. An installation summary appears. Click *Install,* and the installer installs all of the required software for your hardware configuration.

2. If you want your server to autostart, but want to tune it before it autostarts, elect to install as a service/daemon, but run it manually first until tuning is done, then resume using autostart. For Windows: go to Services in Control Panel, stop the service and make it start manually instead of automatically. You can set it to automatically start when you are ready to resume using autostart. For Linux: after rebooting (if that occurs), use the pmstopall command to stop appserver. Start and stop manually using startappserver/stopappserver. Then run pmstartall or reboot to resume using autostart. See startappserver / stopappserver Command Lines on page 66. As always, run oware in Windows, or . /etc/.dsienv in Linux before running command lines.

13. If you are installing on Linux, you must run a setup script in a separate shell, logged in as root user. Installation prompts you to run a generated script after the install phase finishes. This script records information in case you need technical assistance and installs some files as root. Open a new shell, log in as root, and run the listed script (`$OWARE_USER_ROOT/install/root/setup.sh`).

    This step installs some essential environment files. It does not check for patches (the installation does that). The contents of `patch_check.log.timestamp` now appear embedded in `setup.log`.

14. **MySQL:** The installer either builds the database for first time use or prompts you to rebuild it if a database already exists. Building the database for the first time may take several minutes to complete.

    If you installed MySQL on a separate server, you must run `dbpostinstall` on the (primary) appliction server too whenever you upgrade our change your system.

CAUTION:

Ensure your Linux package has not already installed a version of the MySQL database. If it has, uninstall that database before proceeding. **Also:** Do not configure and/or install a database larger than the available disk space.

NOTICE

Regardless of the initial database size, post-installation configuration of Database Aging Policies (DAP) can have a significantly impact on how fast it reaches its capacity. The default DAP for alarms, for example, never cleans open alarms from the database. Similarly, defaults for archiving event history may not suit your environment. Consult the *User Guide* for details about tuning these policies.

15. **Oracle:** For Oracle databases run the following command lines:

```
loaddb -u system -w manager
loaddb -u system -w manager -s. [1]
```

    Then run:

```
dbpostinstall
```

    Oracle Database Management addresses fine-tuning these installation steps.

16. When you install Application Server a service, the installer prompts to let you start the service without rebooting again. If you elect to start the Application Server service, a monitor icon appears in the Windows tray that is yellow as Application Server starts up, and green when it is completely up and running.

    To confirm an automated-starting Application Server is running, you can run `pmgetstatus` in a shell. Both Application Server and Web Server (status indicated by the Apache icon in Windows) must be completely started before you can open the client.

17. Finally, the application prompts you to click *Done*.

18. After you complete the installation, you may want to install Adobe Acrobat Reader. You can download a free copy from www.adobe.com. This application requires Acrobat to successfully print reports.

1. If loaddb -u system -w password does not work the first time then add -d. You must run the command line both with and without the -s.

Additional post-OpenManage Network Manager installations can also include Perl and FTP/TFTP servers. See Installing Perl on page 16 and Setting Up FTP / TFTP on page 30.

See Starting Application Server on page 50 for instructions about running what you have just installed.

Installing OMNM Silently

You can execute the installation in console mode. Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type `back`. You may cancel this installation at any time by typing `quit`. Run one of the following in a shell to initiate console installation:

```
win_install.exe -i console
linux_install.sh -i console
```

These installations provide text alternatives for various features. For example:

```
===============================================================================
Choose Product Features
-----------------------
ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
   LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:
1- [X] Application Server
2- [X] Web Portal
3- [ ] Mediation Server
4- [X] Database
Please choose the Features to be installed by this installer.: 3
```

In such lists, the `[X]` indicates a selected feature. If you enter numbers on the `Please choose` line, this toggles the selection on or off. In the above example, the number 3 has toggled `3` so no `[X]` appears in that line, indicating this installation skips Mediation Server.

Silent Installation

Linux supports silent installation in which installer runs without any user interaction. A near-silent mode is also possible on Windows. Set installer and user-defined variables through a properties/response file, as described below. You can collect the properties from a installation you wish to recreate.

To run a silent installation, follow these steps:

1. Create a response file—The installer automatically creates a sample properties file during a normal installation. Run installation and look for the file called `sample_installer.properties` in your install location root directory.
2. Execute the silent install—Copy the `sample_installer.properties` to the installer's directory. For example:

```
D:\installer\RCES\7.2\0.111\install\Disk1\InstData.
```

3. Rename `sample_installer.properties` file to just `installer.properties`.
4. To trigger a silent installer from the command line, type the following command:

```
installername -i silent
```

5.The `-i` argument means the installer automatically checks the directory in which it resides in for a file called `installer.properties` or `[installername].properties`.

Alternatively, you may also call a properties file from the command line:

```
installername -f properties file
```

You may use the direct or the relative path to the properties file. If you specify the properties file you must include the following property to trigger silent mode.

```
INSTALLER_UI=silent
```

MySQL Database

After installing a MySQL database to a separate host in console mode, you must run `loaddb`, `loaddb -s`, and then run `ocpinstall -s`, all from the application server installation console.

Installing Licenses

The Application Server, and other optional software, requires licenses. These should be installed by default, but if the license has expired, or if for any other reason your license is not available at startup the Application Server (or other application) shuts down and will not start.

You can install licenses for basic Application Server functionality, and for extended functionality for drivers and applications at any time. You can install these from the *License Management* in the Quick Navigation Portlet in the client. Select the license file in that screen (click the *Select File* button) on any client, and the Application Server stores the permissions to use that functionality in the database.

The license (`license.xml`) is typically in a directory below the installation shortcuts / links. To install the license without the benefit of a client (which does not start without a running Application Server), run the following commands in a shell before starting the server:

Windows

```
>oware
>licenseimporter c:\path\license.xml
```

Linux

```
>. /etc/.dsienv
>licenseimporter c:\path\license.xml
```

NOTE:

Most of the time, you must log out and re-log in for an imported license to take effect. On rare occasions, you must restart application server.

When the `licenseimporter` concludes its work, you should see:

```
importing.....done
```

The `c:\path` portion of this command line is an example. Correct it to wherever you have your license file (by default this is below installation directory on the CD or in `$OWARE_USER_ROOT`).

Start Linux applications after logging out, and logging back in either from the installed icon on the desktop, or from a command line. The following command lines all assume you run `oware` or `. /etc/.dsienv` before running them, to set the environment correctly. The commands:

```
startappserver
startmedserver
```

Both `stopappserver` and `startappserver` scripts may require username / passwords as parameters, if you have an installation that requires a password. To see the syntax of either of these scripts, append -? to them on a command line. Here is the help output from `stopappserver`:

```
~/:stopappserver -?
Usage(1):  stopappserver server_url [-u username] [-p password]
Usage(2):  stopappserver server_url password
example -  stopappserver localhost:1099 -u OWAdmin -p secret
example -  stopappserver localhost:1099 secret
If omitted, username will be assumed to be OWAdmin.
If omitted, password will be assumed to be blank.
If no arguments are provided, server_url will be assumed to be
   localhost:1099.
```

By default, these scripts assume the *OWAdmin* user and a blank password, so if you have changed the default password for OWAdmin, you must pass it to stopappserver.

Starting Linux Installations

The operating system prompts user `redcell` for the root password for the following command lines (no such prompt appears for root user):

Application Server

```
$service oware start
```

Portal Server

```
$service synergy start
```

In `/etc/init.d`, you can run the following:

```
#./oware start
#./synergy start
```

When you have autostart enabled, to start appserver and process monitor:

```
$startpm &
```

To stop appserver and process monitor

```
$stoppm
```

When process monitor is running, you can check the appserver status

```
$pmgetstatus
```

To stop the application server process only

```
$pmstopall
```

To start the appserver again when process monitor is already running:

```
$pmstartall
```

To open a web client, go to this URL: [host IP address]:8080.

NOTE:

You cannot run a separate mediation server and an Application Server on the same host. If no separate mediation servers are detected, the Application Server will act as a mediation server.

NOTICE

If a mediation server fails to start up with an ENetworkFailure, delete all files in the `oware\temp` directory manually to successfully start the mediation server.

If either application server or mediation server fails to start, particularly after an interruption in service, like a power failure, delete this directory's contents: `oware\jboss*\server\oware\data`

Web Services

Newer web services are disabled by default. Enable them by adding this line to $OWARE_USER_ROOT/owareapps/installprops/lib/installed.properties:

```
com.dorado.core.ws.disable=false
```

These are automatically available when `dnc.ocp` is installed. From version 7.0.0 forward, older non-Axis2 web services are disabled by default too. You can enable them by adding the following to the $OWARE_USER_ROOT/owareapps/installprops/lib/installed.properties file:

```
com.dorado.legacy.ws.enable=true
```

Disabling older web services enhances performance.

Application Password

The default user (admin) initially has the password admin. The database stores all passwords in encrypted form.

Starting Application Server

If you are installing mediation or Application Servers, an option appears during installation to configure the server to autostart when the server boots. The final installation screen asks whether you want to start the application server, so you do not need to start the server immediately after installing it.

The startup sequence: Database server starts first, then Application server. Mediation server can start any time before or after this sequence, and waits for application server. See Stopping Servers on page 64 for instructions about stopping Application Server.

You can stop, start and monitor the autostarted Application Server service, with command lines (`pmstopall`, `pmstartall`, and `pmgetstatus`), or use a system tray tool for controlling the Application Server in Windows. As always, run `oware` in Windows, or `. /etc/.dsienv` in Linux before running the command lines.

For security reasons, `pmstopall` has security requirements similar to `stopappserver`. Here is a sample command line:

```
pmstopall <hostname>:1099 -u <username> -p <password>
```

Both `-u` and `-p` are optional parameters. If you omit `username`, the application assumes `OWAdmin` is the user. If you omit a password, the application assumes a blank password.

While you can always run the command-line script `startappserver`, a second Application Server on same ports fails. Also, the Windows *Start Application Server* shortcut does not appear in the *Start* menu when you elect autostart, assuming your installation offers that as an option.

If you select no autostart, then no autostart service installs, and you must manually start the Application Server either from the *Start* menu (in Windows), or from a command line with `startappserver`. (See Starting Application Server on page 50)

If you want to install the service (daemon) after you have already installed the rest of the application, you must run the `installprocman` script from a command line. See Installing Server Manager on page 51 for details.

Autorun is useful for production server installations. However, if you do not elect this option, then you must manually start the Application Server and mediation server yourself (using the `startappserver` and `startmedagent` command lines or the item in the Windows *Start* button menu).

For Oracle/Windows installations with autostart selected for a server, the last step in the installation may prompt you about whether to start process monitor immediately. This potentially lets you defer appserver startup until the next reboot for the sake of Oracle.

NOTE:

Autostart takes some time for the initial load. You cannot see progress for the process unless you tail the server.log file.

Installing Server Manager

The `installprocman` script is in `$OWARE_USER_ROOT/oware/bin`. The script takes several parameters.

Usage:

```
-i       install service"
-r       remove service"
-d       set dependency on MySql service (-i only)"
-n Name  assign a custom display name (-i only)"
```

If you are installing the service on a host which houses both the MySQL database and application server you should execute the script with the -i and -d flags (`installprocman -i -d`).

If you are installing the service on a host which has only application server (MySQL is distributed to another host) the script should be executed with on the -i flag (`installprocman -i`).

Installation of Process Monitor System Tray Icon

To ensure the Process Monitor System Tray icon appears each time the system is restarted simply add the `$OWARE_USER_ROOT/oware/bin/pmtray.exe` binary to the *all users* startup folder (`C:\Documents and Settings\All Users\Start Menu\Programs\Startup`).

Update pmstartup.dat

Finally, modify the `application.server.active=` property in `$OWARE_USER_ROOT/oware/lib/pmstartup.dat` and change the default value from `false` to `true`. Once complete, reboot the system and the application server automatically starts and the system tray icon automatically appears in the user's startup folder.

pmgetstatus

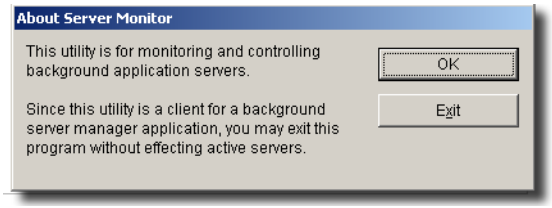
If you elect to autostart your Application Server, you can run the `pmgetstatus` script from a command line to see the status of Application Servers. If you run `oware` first in the shell where you run `pmgetstatus`, this script will automatically be on the path. Here is its usage (produced by typing the script name followed by `-?`):

```
Usage: pmgetstatus [-h <Server IP>] [-p <Server Port>] [-i <Iterations>
[-r <Refresh Rate>]]
Oware utility for reporting status on managed server processes. By default,
   the local host is queried for 1 iteration.
Options:
   -h <Server IP>      -- Server host IP. Defaults to local host
(127.0.0.1).
    -p <Server Port>    -- Process monitor command port.
                           Default loaded from
c:/work/oware/lib/pmstartup.dat
    -i <Iterations>     -- Number of times to repeat command, -1 is
infinite (requires Ctl-C).
    -r <Refresh Rate>   -- Refresh rate of iterative command in seconds.
Default is 5.
                           Requires -i option.
    -?                  -- Show this help.
```

Windows Server Monitor

When you install your application as a service on Windows, you also install a server monitor. This monitor is a client to the server manager which controls starting and stopping of an application or mediation server.

Figure 3-1 Server Manager Client



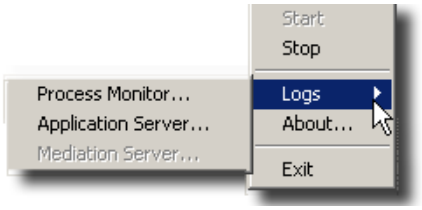
Double click the tray icon to display the about panel. *OK* closes this dialog, but maintains the icon in the tray, while *Exit* ends the Server Manager (client and tray icon).

The tray icons themselves indicate the current service condition.

Icon	Status
	Offline (no status available, or not controlled by server manager)
	Running (initializing, or shutting down)
	Ready
	Stopped

You can also right-click the icon to see the client menu.

Figure 3-2 Process Monitor Client Menu



The logs item let you view logged items for Server Manager, Application Server. You can *Start* or *Stop* the service(s) running on your host.

NOTICE

System changes can make the server monitor system tray icon disappear while the process is still running. If you cannot make your icon reappear, try running `pmtray -r` from a command line.

Web Server Parameters

When you install OpenManage Network Manager, installation also includes an Apache Web server. Its monitor appears in the Windows tray, but you can also configure memory parameters for the web server in the `setenv.*` files under `oware/synergy/tomcat*/bin`.

For example:

Linux

```
-Xmx1024m -XX:MaxPermSize=256m
```

Windows

```
set "PORTAL_MAX_MEM=1024"
set "PORTAL_32BIT_MAX_MEM=768"
set "PORTAL_INIT_MEM=128"
```

Set only MAX_MEM and the INIT_MEM. Higher values permit better performance and more users, especially on 64bit machines. Do not change the other settings.

Best practice on a 64bit system: 2048 for the MAX_MEM and 256 for the INIT_MEM. If you have a lot of extra ram then specify more.

Any database parameters for Web server installation refer to the system's existing database.

NOTICE

The web server starts automatically with installation. If it does not, you can right-click the Synergy Network Management icon in Windows and select Start Service, or in Linux type the following in a shell: `/etc/init.d/synergy start` (or `stop`). In Linux systems, `startportal.sh` and `startportal.sh stop` accomplish the same thing, with additional checks.

Startup Properties

The values in `installed.properties` now set most properties for the process monitor to pass when starting a server. All command-line options for the `startappserver` script are now in `installed.properties` (see refer to the *OpenManage Network Manager User Guide* for more on overriding properties). These are active for each execution of the server (even a mediation server) on the machine where the override exists. Command line arguments override these properties.

The following are properties you can set in `owareapps\installprops\lib\installed.properties` to configure servers:

- Default server partition name also used by client and mediation to locate a server

  `oware.client.partition.name=demo1`
- Default interface used by servers and direct access cut-thru sessions.

  `oware.local.ip.address=192.168.0.10 [for example]`

  The IP address also appears in database connection properties:

  `com.dorado.meta_database.name=//192.168.0.10:3306/owmetadb`
  `com.dorado.jdbc.database_name.mysql=//192.168.0.10:3306/owbusdb`

  To change the IP address, stop the server, set these properties to the new IP address and delete the content of the `oware/temp` directory. Then restart the server.

Web Portal Properties

If you do not use the ipaddresschange script, you will also have to change the IP address for the sake of the web portal. Change this in `portal-ext.properties` in `\oware\synergy\tomcat-7.0.40\webapps\ROOT\WEB-INF\classes`

Change property: `jdbc.default.url=jdbc:mysql://[IP address]/lportal?useUnicode\=true&characterEncoding\=UTF-8&useFastDateParsing\=false`

and

`oware.appserver.ip=[IP address]`

So these reflect the correct IP address, then restart the web service.

ipaddresschange

A simpler alternative to changing properties is to use the `ipaddresschange` script. If you were to install this application on a machine on one network, then move your machine to another network, the IP address from your original network remains hard-coded. You must change the application's IP address to reflect the new network for the software to function correctly. Here is how to do it, once you have connected the application server machine to the new network:

a. First, shut down the Oware Server Manager. Open a command shell (*Start* > *Run* `cmd`, in Windows) then type: `net stop "Oware Server Manager"` (including the quote marks)

b. Next, find out what your new IP address is. To do this type `ipconfig` in the command shell you just opened, and make note of the IP Address that appears. You will need that number in a subsequent step.

c. Type `oware` at the command line. This sets the environment.

d. In the same shell, type `ipaddresschange -n [the IP address discovered in b]`

e. Restart Oware Server Manager by typing: `net start "Oware Server Manager"` (including the quote marks). Also restart the web service.

Your machine should then be able to connect to other devices on this network and function correctly.

NOTE:

After the utility is done, if you are using Server Monitor, its Icon in the program tray has an x through it. You must either reboot or use Windows' Administrative facility stop the oware server manager service and restart it. ***Also:*** *In certain packages, you may have to alter the properties mentioned in the Web Portal Properties mentioned above.*

- Use only https for web services

  `oware.appserver.web.enable.https=false`
- Set to true when there is no graphics adaptor available for server

  `java.awt.headless=false`
- To change the default HTTP/HTTPS port numbers for web services, add the following properties to `owareapps/installprops/lib/installed.properties`:

  ```
  oware.appserver.web.http.port=[default port number:80]
  oware.appserver.web.https.port=8443
  ```

  You may then change the port values for these property entries and restart the Application Server. Special setup (outside the scope of this document) is necessary to run a web server on port numbers lower than 1024 on many operating systems.

CAUTION:

Do not change the system time while the Application Server is running. If you must change the system time, shut down the server before the change, and restart it afterwards.

Proactive Runtime Management

To insure Redcell continues to run smoothly long after you have installed it, best practice is to take the following precautions. For more about this, see Troubleshooting Your Application.

- Make sure you configure database archiving policies (DAPs) to suit your system, particularly if you have device messaging (typically alarms and syslog) that threaten to fill your database.
- Occasionally check the Audit Trails to ensure DAPs are running properly.
- Configure your syslog and alarm events to only catch significant ones.

- Configure devices to suppress their own messages if these messages are unimportant.

Using Two Interfaces

While installation accommodates selecting between two interfaces, some rare occasions require communicating with both. When that occurs you must add the additional IP address, not selected during installation, to the application server's `tomcat-server.xml` listener so it can communicate with the webserver on the other IP. The following changes make this work:

Add to `/dorado/oware/synergy/conf/server-overrides.properties` on fresh installation:

```
oware.appserver.ip=192.197.95.2
```

(The address above is an example of IP address not selected during installation.)

Add to `/dorado/oware/jboss-5.1/owareconf/tomcat-server.xml` on fresh or update installation:

```
<Connector     scheme="http"
               address="192.197.95.2"
               port="@http.port.num@"
               maxThreads="150"
               minSpareThreads="5"
               maxSpareThreads="75"
               enableLookups="false"
               redirectPort="@https.port.num@"
               acceptCount="100"
               connectionTimeout="20000"
               disableUploadTimeout="true"
            debug="0"/>
```

Installing on Linux from the Command Line

Use the following command to run the Linux installation from a command line:

```
linux_install.sh -i console
```

The text prompts are equivalent to the graphic interface prompts.

The following system files may be modified during root installation:

```
/etc/.dsienv - installed
/etc/my.cnf - installed
/etc/rc2.d/S75owaredb — installed
/etc/rc2.d/S76oware — installed
```

The installation process installs program files, does setup functions, and performs the initial database loadIf you need detailed information on the different installer options, see Installation User Interface on page 77.

Install on a Linux System from the command line as follows.

1.Create the install directory as root and set the permissions.

For example, enter the following command if installing to the /dellemc/openmanage/networkmanager default directory:

```
mkdir -p /dellemc/openmanage/networkmanager
chown :synergy /dellemc/openmanage/networkmanager
```

```
chmod 770 /dellemc/openmanage/networkmanager
```

Note that if you do not do this before starting the installer, you will get an error during the installation. At that point, open another shell tool, execute these commands as root, and then return to the installer to continue.

2. Navigate to the installer executable.
3. Enter `./linux_install.sh -i console`.

   Informational content shows, such as minimum system requirements.
4. Press Enter through the informational content.
5. Enter whether you want an Express Install (1) or Custom Install (2).
6. Follow the remaining prompts for you selected installation.

   When the installation is complete, a successful/unsuccessful message is displayed. If successful, press Enter to exit. Otherwise, follow the instructions provided for an unsuccessfule installation. Also see, Troubleshooting Installation Issues on page 75.

Performing Complex Installations

The following describes an installation to a cluster. In a production environment, such installations must take account of the network security settings and firewalls.

Here are a few things to check before your installation:

- Ensure any time (NTP) server processes are running.
- From a command line ping all hosts from each other to ensure connectivity exists. Ping with fully-qualified domain name and with the hostname alone.
- Ensure that the installing user has admin privileges on any Oracle database. See Oracle Database Management for more about setting up Oracle.
- Refer to the ports used in the *OpenManage Network Manager User Guide* for a list of ports that must be open on the firewall for components to communicate with each other. Open the appropriate ports (bidirectionally).

NOTICE

It is often easiest to disable firewalls completely while initially installing and testing distributed installations with firewalls between components.

Best practice includes adding this line to the application user's Linux `.profile`

```
. /etc/.dsienv
```

This means the user sources the environment on login. On Windows, running the `oware` command on clients creates a bash emulation with the same environment.

Follow these steps for your installation:

1. Make the appropriate Custom installations to all affected machines (Application Servers, mediation servers, clients). You must know the following that you configure:
   - Cluster name—For example: `my_redcell_cluster` is our Application Server cluster.

NOTE:

Some steps below are unnecessary if you plan to simply distribute processing rather than clustering servers.

- Database information—`@[Server_name]:[port]:[database name]`. For example: `@my_server:1521:MYDB`.
- If you are clustering servers, you must select which will be the config server. For example: `my_server`.

You may want these to autostart in a production system. If so, select that option when installing.

2. Install to Oracle as the installing user, first with `loaddb`, then with `dbpostinstall`. Run `loaddb -u [dba user] -w [dba password] -s -g` on the (primary) application server. See also Oracle Database Management for more Oracle information.

NOTE:

If you have a MySQL database on a separate host, you must also run `dbpostinstall` *on the primary application server for the sake of that database too.*

If you are planning to change the database name, you must change it in `owareapps/installprops/lib/installed.properties` on the Application Server.

For `loaddb` to work, you must have `$ORACLE_HOME/network/admin/tnsnames.ora` file configured on your Application Server. Here is an example configuration:

```
-------------------------------------------------------------------
MYDB =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = [Server_name])(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = MYDB)
    )
  )
-------------------------------------------------------------------
```

To test DATABASE connectivity from appserver try:

```
pingdb -u <username> -p <password>
```

See Oracle RAC Property on page 60 for more information about installing with Oracle's failover.

3. Add `oware.config.server=[fully qualified primary appserver name]` to `owareapps/installprops/lib/installed.properties` on the Application Servers. Here are the relevant portions of these `installed.properties` files:

Appserver:

```
#*********************************************************
```

```
#  The following properties override those found in         *
#  oware/lib/*.properties in order to establish valid       *
#  properties for this installation.                        *
#***********************************************************

oware.config.server=my_server
oware.installed.package.name=RedCell
...
oware.client.partition.name=my_redcell_cluster
oware.local.ip.address=193.35.184.175
oware.mediation.subnet.mask=255.255.255.0
com.dorado.bom_dbms.name=oracle
com.dorado.jdbc.user=redcell
com.dorado.jdbc.password=mypwd
com.dorado.jdbc.database_name.oracle=@my_server:1521:MYDB
...
```

NOTE:

If you plan to change the database name, you must change the relevant portion of your Application Servers' `installed.properties` *files. Similarly, if you use a database tool to change the default user's password, you must change that password in the* `com.dorado.jdbc.password` *property.*

The config server distributes tasks to members of a cluster. If you are not clustering, then this step is superfluous.

4. If you are clustering mediation servers, you must add the mediation server cluster config server in `installprops/medserver/lib/installed.properties` on all such servers. This example installation does *not* cluster mediation servers. We do, however, want to bypass multicast communication with Application Servers, so this file is configured with the `oware.application.servers` property. Multicast may be restricted by a firewall,

Medserver:

```
/installprops/medserver/lib/installed.propertes

#***********************************************************
#  The following properties override those found in         *
#  oware/lib/*.properties and                               *
#  oware/medserver/lib/*.properties in order to establish   *
#  valid mediation properties for this installation.        *
#***********************************************************

## This property defines whether mediation listeners should make use of
## of high availablity or not.
## Possible values  true  - Listener come up in high availability
   mode(Forwarding/Standby)
## false - Listener come up independently.
com.dorado.mediation.listener.use.high.availability=false
##
##multicast message communication between agents for working in a peer
   environment.
com.dorado.mediation.listener.multicast.intercomm.address=226.0.0.26
oware.application.servers=193.35.184.175,193.35.184.170
```

This modification is typical for secure environments where multicast is restricted by a firewall.

NOTE:

If you use the oware.application.servers property, you must (comma-separated) list all available servers wherever you use it to bypass multicast. See Disabling Multicast on page 191

An HA "cluster" consists of only two mediation servers. You can have more than two, but that just means more than one standby server exists. If you set the HAproperty to false, all clustered mediation servers are active at the same time, and any number of mediation servers can be in the same cluster.

5. Disable Mediation server on appserver machines by not configuring it during installation. Alternatively, you can put this property in `\owareapps\installprops\lib\installed.properties`:

```
oware.appserver.mediation.setup=false
```

6. If you installed autostarting, configure it in `owareapps/installprops/installed.properties`. See Startup Properties on page 54 for a list of potentially configurable properties.

7. During testing you can start application or mediation servers two different ways:

   - To test autostart: run `/etc/rc2.d/S76oware start` as root
   - For manual startup (common during testing) run the following as the application's user:

```
startappserver -c <config server> -p <cluster> -m <multicast address>
```

and

```
startmedserver -a <appserver cluster>
```

See also Starting Application Server on page 50.

Oracle RAC Property

Add the following property to enable Oracle RAC on all Application Servers

```
/owareapps/installprops/lib/installed.properties
Add com.dorado.oracle.rac.connect.url=@(DESCRIPTION=(ADDRESS_LIST=\
   (ADDRESS=(PROTOCOL=TCP)(HOST=[hostname1])(PORT=1521))\
   (ADDRESS=(PROTOCOL=TCP)(HOST=[hostname2])(PORT=1521)))\
   (FAILOVER=on)(LOAD_BALANCE=on)(CONNECT_DATA=(SERVER=DEDICATED)\
   (SERVICE_NAME=[Oracle service name])))
```

Startup Sequence for Initial Testing

When starting complex installations, the following is the recommended sequence:

1. Start the database.
2. Start the config server (the primary Application Server for a cluster).
3. Start the remaining Application Servers.
4. Start the mediation servers, one at a time.
5. Start the web server(s).
6. Start the web client.

Once you have successfully completed the above with single servers, start the rest of the cluster of Application Servers. To test that each mediation server works, start and stop them one at time. Running discovery is a good test of connectivity.

E-Mail

The application can trigger e-mails. To configure your system correctly to send these in your e-mail environment, consult *User Guide*.

Verifying Your Installation

Starting OpenManage Network Manager (After installation)

Database Running, Connected—Make sure your database is running. MySQL installs automatically as a service (daemon), Oracle must be started separately. Make sure your database connects to the application server if it is on a separate host. Do not install on Linux with MySQL already installed (uninstall any included MySQL first).

Start Application Server—If you installed this software as a service and application server is down, in Windows right-click the server manager icon in the tray, and start application server. Sometimes, this icon may prematurely indicate application server has started. Wait a little, and the application server will catch up to the icon.

When initiated from the tray icon, startup changes its color from red to yellow to green, when complete. Once the icon has turned green, the web client may display the message "The server is currently starting up. This page will refresh when the server has fully started." This message indicates the application server requires extra time to start. When the message does occur connect the web browser again after a few minutes.

Login—Default OpenManage Network Manager login is *admin*, password *admin*.

NOTE:

The first time you start the application after you install it, you may have to wait some additional minutes for Application to completely start. One indication you have started viewing your web client too soon is that it does not display the Quick Navigation portlet correctly. **Workaround**: Force OpenManage Network Manager to re-initialize the admin user. To do that: Login as Admin. Go To > Control Panel > Users and Organizations. Select and edit the Admin user. Edit any field (Middle Name for example). Save. Sign out. Log back in with admin.

For Successful Discovery (After startup) Have the Following:

Connectivity—Ensure application server has connectivity to devices to discover. One easy way to do this is to ping the discovery target from the application server host. Right-clicking a discovered device and selecting *Direct Access* also lets you ping the device to validate your connection.

Backup / Restore / Deploy (After device discovery)

FTP/TFTP Server—Make sure an external FTP/TFTP server / process is running and has network access to the target device(s). Typically FTP/TFTP must be on the

same side of firewalls as managed devices. OpenManage Network Manager's internal FTP/TFTP server is for testing only. If FTP and TFTP are separate processes, configure them so they write to the same directory.

Alarms / Monitoring

Minimize Network Traffic—Configure "chatty" devices to quiet down. Use *Suppress Alarms* to keep performance at acceptable levels, and configure database archiving so the database does not fill up.



CAUTION:

Some OpenManage Network Manager features do not work without internet access. In particular: Maps, because the maps OpenManage Network Manager uses need internet access to retrieve maps and plot locations. But if you do not need functioning map portlet(s), then running OpenManage Network Manager without internet access works well as long as the network is properly configured and resolves the *localhost* name to application server's IP address.

Uninstalling the Application

Use Control Panel to uninstall in Windows. Uninstall by running the following on Linux:

```
$OWARE_USER_ROOT/_uninst/uninstall.sh
```

You must uninstall from Linux as root. No graphic wizard appears, and you must respond to the command-line prompts as they appear.

You can uninstall the software by using Windows' control panel's *Add/Remove programs* feature (or with `Uninstall Redcell\Uninstall Redcell.exe`), or by running the following on Linux:

```
$OWARE_USER_ROOT/_uninst/linux_uninstall
```

or for console mode, run...

OWARE_USER_ROOT/_uninst/linux_uninstall -i console

NOTE:

If you uninstall in a shell rather than using the graphic uninstaller, uninstaller cannot uninstall its own directory. This produces some errors you can safely ignore in a console uninstallation. Use `cd /opt` *and then* `rm -rf [installation target directory]` *to do final cleanup.*

In graphic uninstallation, as in installation, click *Next* to continue through the screens as they appear. One such screen appears listing what you want to uninstall. Confirm that you want to remove all the listed installed components. You can optionally delete all the applications' files and directories (complete removal).

CAUTION:

Uninstallation on MySql servers may delete the database and any application directories. The applications' directories also contains any installed application components and device drivers.

The option to delete directories is primarily to support application developers having to uninstall and re-install the basic application platform without losing component files (like device drivers) on disk that were not part of the installation.

NOTICE

Deletion is recommended, but not required. It removes files created after installation; temp files, database files, cache files, and files extracted from OCP/DDP files. Overall, it is the best way to get a clean uninstallation. You can back up your `oware/lib/*.properties` files or overrides before uninstalling if you want to preserve them. An alternative is overriding properties. Refer to the *OpenManage Network Manager User Guide* for more on overriding properties.

When the software has been completely uninstalled on Windows, if prompted, you must reboot your computer to complete deletion of any locked files. Best practice is to reboot right away.

Uninstalling removes all installed files and files created by using the installed system (that it has permission to delete). It does *not* remove directories that were not created by this application's installation or runtime. User-created directories in the product's directory path remain after product removal.

NOTE:

Uninstaller may freeze on hosts with inadequate resources. ***Also:*** *The uninstaller deletes uninstall.exe, if you press the cancel button. After the canceling uninstallation, several directories and files remaining on disk that require manually deletion to completely uninstall.*

Stopping Servers

To stop the Application Server, you can either use the Application Server tray icon in Windows (see Starting Application Server on page 50), or stop the server from a command line. The command line to stop a server is `pmstopall`.

If you have not automated server startup, then you can use the `stopappserver` and `stopmedserver` scripts to stop these servers, even remotely. Here is the syntax:

```
stopappserver <hostname>:1099 -u <username> -p <password>
stopmedserver <hostname>:1099 -u <username> -p <password>
```

Both `-u` and `-p` are optional parameters. If you omit `username`, the application assumes `OWAdmin` is the user. If you omit a password, the application assumes a blank password.

CAUTION:

Using Ctrl+C in the application server shell may stop the application server, but processes can linger which you must stop manually before you can successfully restart application server. One example occurs when the application server shell displays "…. FAILED TO LISTEN ON TRAP PORT 162 …. "during startup. If this occurs, use task manager to stop WMIBeam and WMINotification processes. If such processes do not exist in task manager, reboot before starting application server.

If you have not logged in and changed the password for OWAdmin with the application's login screen the login to stop the server fails. By default, `OWAdmin` and the installing user have the role `OWServerAdmin`. Any user assigned this role can stop the appserver. Blank passwords are valid if they are defined for the user.

If you used `startappserver` in a shell to start the Application Server, you can stop the server by either interrupting that shell with Ctrl+C or by closing the shell. Ultimately, you can kill the Java processes on your machine to halt a server.

See Upgrading from a Previous Version on page 66 for additional notes about shutting down processes and services. If you uninstall when a server is active, the uninstallation will attempt to shut it down and failing that will prompt you to shut it down manually.

4

Updating an Existing Installation

Updating an Existing Installation

Before updating the product, make sure that you performe all pre-installation tasks discussed.

For a description of the installation user interface and the different fields and options, see Installation User Interface on page 77.

Upgrading from a Previous Version
Backing Up the Database – 68
Restoring Databases – 68
Upgrading on Linux – 70
Upgrading on Windows – 71
Importing the OMNM MySQL Database – 72

Upgrading from a Previous Version

When you upgrade your OpenManage Network Manager installation from a previous version, keep the following topics in mind, as they apply:

- User Validation
- Upgrading Your Operating System
- General Upgrade Advice/Information
- Handling Missing Users

User Validation

The installer in recent versions prevents installation as users `root` (Linux) or `administrator` (Windows). This may halt an upgrade installation on Windows if you installed the previous version as user `administrator`.

To avoid this issue, create a new user (in the administrator group). Then navigate to the target installation directory and change ownership of all directories, subdirectories and files to that new user. Right-click the directory and select *Properties* > *Security* > *Advanced* > *Owner* tab. Then add the new user as an owner. Make sure that you select "Replace owner for sub-containers and objects." After applying the changes, login as the new administrator user and proceed with the upgrade.

Upgrading Your Operating System

If the OpenManage Network Manager version you plan to install does not support your operating system version, upgrade to a supported operating system before the OpenManage Network Manager upgrade. Upgrade your operating system as follows.

1. Back up the database.

   For instructions about backing up all databases, see Backing Up the Database on page 68.

2. Upgrade the operating system.
3. Install the original OpenManage Network Manager version on the new operating system.
4. Restore the database.
5. Proceed with the OpenManage Network Manager upgrade.

See Restoring Databases on page 68 for instructions about restoring databases.

General Upgrade Advice/Information

- Make sure that you log out of the operating system between installations.
- Make sure that you have a new license, which is required to activate new features.
- Close and re-open browsers when upgrading.
- The following require manual migration (export, then import) from previous versions: SMTP settings, some Scheduler items, Custom Adaptive CLIs. Some schedules may require deletion/re-making. If you open them and they are blank, use this method.
- You must re-create topologies as Visualizations.
- User Names/Passwords, and User Groups (Roles) are not automatically reassigned and must be created again manually.
- The default password policy has no restrictions on password length.

- Adaptive CLI with Perl scripts must contain valid Perl under the “strict” pragma (`use strict;`). If you import or migrate from a previous version a Perl script that does not pass this “strict” criterion, you must rewrite it for “strict” compliance before you can successfully edit or copy it.
- Any configured color changes to the portal may not persist and must be re-made manually. Similarly, customized page layouts or page order may not persist and you must typically re-arrange them manually.
- After upgrade or installing new features or module you may need to reset newly available permissions. New permissions permit no access by default. To see them, any administrator user can look in the Permissions in Control panel. If you select the administrator role and see an enabled *Add* button, then upgrading added new permissions. View and change any permissions not assigned after clicking *Add*.
- If you upgrade, some device information may not appear. If this occurs, delete and rediscover the device after upgrading. This is true of the population of Groups. When upgrading, to get the correct population of device groups some times, you must delete the Group (for example: Dell PowerConnect) before doing the upgrade.
- If upgrade, or any installation, has difficulties, troubleshoot by searching for “error” in `[installation root]\install.log`.
- Upgrading to a different path than the default may cause path/shortcut errors.
- Upgrade may require resetting Config File portlet permissions.
- Expect first application server restart after upgrade to be slower than usual.
- When vendors re-brand their devices, previously supported devices may appear with 6027 as vendor. Essentially, you must delete the 6027 vendor, re-seed the relevant driver, re-start application server and re-discover the devices to remedy this.
- Note that some OpenManage Network Manager components may trigger virus detection. You can either ignore such warnings or turn off your virus checker before installing.
- Make sure that you know how the old dashboard is setup before upgrading. Some upgrades require you to re-create performance dashboards.
- Note that any time you cancel an installation in progress, remnants of installation may remain. Uninstall can leave remnants too.

NOTICE

Whenever you upgrade your system and your database is on a separate server, you must run the `oraclepostinstall` script on the (primary) application server too.

Finally, you must also to log out and log back in to OpenManage Network Manager for any permission change to take effect.

Handling Missing Users

If you upgraded your OpenManage Network Manager installation, users and/or their role associations may not appear. You can fix this by going to one of the following Control Panel screens:

Roles > Administrator > Actions > Assign members.

Roles > Power users > Actions > Assign members.

Roles > [ROLENAME] > Actions > Assign members.

Then click *Update associations*. Alternatively, you can go to the Server Administration portion of the Control Panel and click *Execute* to *Reindex all search indexes*.

Backing Up the Database

To back up your database, open a command shell (*Start* > *Run* `cmd`, in Windows), and then type the following at the prompt replacing USERNAME and owbusdb. By default, the database is `owbusdb`, user name is `root` and password is `dorado`.

```
mysqldump -a -u USERNAME --password=[name] owbusdb > FILENAME.mysql
```

For example:

```
mysqldump -a -u oware --password=dorado owmetadb > owmetadb.mysql
```

If you have Performance monitors or Traffic Flow Analyzer, you must also back up your stored procedures otherwise they do not get restored when you restore the database. The command line here adds `--routines`. For example:

```
mysqldump -a -u oware --password=dorado --routines owbusdb > owbusdb.mysql
```

This writes the owbusdb to a plain-text file called `FILENAME.mysql` (`owbusdb.mysql` in our examples). This file is a full backup with which you can fully restore your database in case of problems.

Defaults for the database are `oware` (login) and `dorado` (password). These are typically different from the login/password for the application.

NOTICE

To get a rough estimate of a database's size, looking at the size of the directory `\oware3rd\mysql\data`.

Here are the backup commands for all the databases:

```
mysqldump -a -u root --password=dorado owbusdb > owbusdb.mysql
mysqldump -a -u root --password=dorado owmetadb > owmetadb.mysql
mysqldump -a -u root --password=dorado lportal > lportal.mysql
mysqldump -a -u root --password=dorado synergy > synergy.mysql
```

To backup stored procedures too:

```
mysqldump -a -u oware --password=dorado --routines owbusdb > owbusdb.mysql
```

Restoring Databases

Restoring from `FILENAME.mysql` is a three step process. This occurs, again, in a command shell:

1. Drop the database:

   ```
   mysqladmin -u USERNAME -p drop owbusdb
   ```

   or

   ```
   mysqladmin -u USERNAME --password=[password] drop owbusdb
   ```

2. Recreate the database

   ```
   mysqladmin -u USERNAME -p create owbusdb
   ```

   or

   ```
   mysqladmin -u USERNAME --password=[password] create owbusdb
   ```

3. Import the backup data

   ```
   mysql -u USERNAME -p owbusdb < FILENAME.mysql
   ```

   or

   ```
   mysql  -u USERNAME --password=[password] owbusdb < FILENAME.mysql
   ```

Here are restoration commands for all the databases:

```
mysql -u root --password=dorado owmetadb < owmetadb.mysql
mysql -u root --password=dorado owbusdb  < owbusdb.mysql
mysql -u root --password=dorado lportal  < lportal.mysql
mysql -u root --password=dorado synergy  < synergy.mysql
```

NOTE:

If you receive the error "Access Denied. Invalid Role for this device" or if the application(s) fails with error indicating that it cannot connect to the device after a network change, There may be a DNS resolution issue. You may still be able to ping or connect to a device by IP address but testing server connectivity by using hostname will confirm or rule out a DNS problem. This would only be a problem if the device(s) were discovered or set to "Manage by Hostname". If the system was migrated to a system that is not using DNS, then name resolution could fail and there would be no connectivity to devices. The solution from the Resource Manager is to Right Click -> edit and un-check "Manage by Hostname". This will then default to Manage by IP address. Alternatively, you can fix name resolution in your environment.

NOTICE

Whenever you upgrade your system and your database is on a separate server, you must run the `oraclepostinstall` script on the (primary) application server too.

Upgrading on Linux

Upgrading on Linux

This section provides the steps for preparing your Linux system for an upgrade and then running the installer.

Preparing to Upgrade on Linux

Preparing to Upgrade on Linux

This section summarizes the steps to take to prepare for an OpenManage Network Manager (OMNM) application upgrade on a Linux system.

Prepare to upgrade your OMNM version on a Linux system as follows.

1. Back up the database to another machine and any other resources that need manual installation. The backup is stored in the *isntallDir*/backup.sql directory. See Upgrading from a Previous Version on page 66 for more specifics.

   For example, backup your OMNM MySQL database to another machine or network drive with the following commands:

   ```
   mysqldump -a -u root --password=dorado --routines owbusdb >
   owbusdb.mysql
   mysqldump -a -u root --password=dorado  owmetadb > owmetadb.mysql
   mysqldump -a -u root --password=dorado lportal > lportal.mysql
   ```

   The password may be different than the default (`dorado`).

2. Upgrade your operating system if needed before upgrading the OMNM application.

   Make sure that the Linux upgrade does not include the MySQL database. If it does, remove it after the upgrade and the import the OMNM MysQL database (see Importing the OMNM MySQL Database on page 72 for instructions).

3. Make sure that you export the system settings if you modified the default settings.
4. Verify that the current installation's Application server starts without exceptions.
5. Make sure that you remove or rename the my.cnf file for your current OMNM installation.

   The several my.cnf configuration files on a Linux install are in the following locations:

   ```
   installPath/oware3rd/mysql/my.cnf
   installPath/oware3rd/mysql/5.7.16-linux-x86-64/my.cnf
   installPath/oware3rd/mysql/5.7.16-linux-x86-64/config/my.cnf
   ```

6. Disable any firewalls.

Now you are ready to get started Running the Installer.

Running the Installer

These instructions assume that you have already backed up your database and other necessary configurations requiring a manual backup. If you have not already done the backups or prepared your system for an upgrade, see Preparing to Upgrade on Linux on page 70 before continuing.

Run the installer as follows.

NOTE:

The installer automatically stops the Application and Web servers during an upgrade.

1. Login as a non-root user, such as synergy.
2. Upload the OMNM package to your home directory, such as /home/synergy.
3. Confirm that no running java process exists.

   ```
   ps -ef | grep java
   ```
4. Kill any existing java processes.
5. Modify the linux_install.sh and linux_install.bin permissions to allow their execution.

   ```
   cd version/install
   chmod +x linux_install.sh
   cd Disk1/InstData
   chmod +x linux_install.bin
   ```
6. Start the installer:

   ```
   ./linux_install.bin
   ```
7. Accept the license agreement to start the upgrade proces1s.

   A message that an existing installation was detected and this will be an upgrade. Also noted are the installed features. Click Enter to continue. Otherwise, enter quit to cancel the upgrade.
8. Answer each prompt appropriately.

   If you did not backup your database before starting the update, you are given one more chance to do so. The database backup is stored in the *installDir*/backup.sql file by default.

   If you elect not to rebuild the database, the update still re-seeds the system settings.

   If you encounter port conflicts, resolve them before continuing.

   The servers automatically start when the update finishes. You may need to reboot the server if your performance monitor information does not appear.

   If you are running either MySQL or Oracle as your database on a separate server, you must also run `dbpostinstall` on the (primary) application server before starting your system.

   If your upgrade fails, see the install.log, db_setup.log or app_setup.log file in the destination directory for messages that may help fix the failure.

Upgrading on Windows

As with a standard install, make sure that you can communicate with the network.

Disable Windows Firewal. If you do not disable the firewall, the installer provides an option to allow/not allow firewall access. If you choose to allow firewall access, rules are added to the Windows Firewall Inbound Rules list for the OMNM product.

If you have an SNMP service running, end it from the Task Manager. This service causes a port 161 conflict druing installation, which must be resolved before continuing.

If the Application server automatically starts during installation, the Web and Application servers start as a service. Programs that run as a service **do not** trigger a Windows Firewall notification that allows you to grant firewall access to the program. Additionally, MySQL always runs as a service.

If you are running a domain profile that implements firewall setting with a Group Policy, the rules added by the OMNM installer may be overridden.

NOTE:

The installer automatically stops the Application and Web servers during an upgrade.

1 Download the OMNM package to your local host in a tempory location.

2 Start the installer:

```
win_install.exe
```

The install files are automaticall extracted and the installation wizard begins.

3 Accept the license agreement to start the upgrade process.

4 Answer each prompt appropriately.

If you did not backup your database before starting the update, you are given one more chance to do so. The database backup is stored in the *installDir*\backup.sql file. For example:

installDir\OpenManage\Network Manager\backup.sql

If you elect not to rebuild the database, the update still re-seeds the system settings.

If you encounter port conflicts, resolve them before continuing.

The servers automatically start when the update finishes. You may need to reboot the server if your performance monitor information does not appear.

If you are running either MySQL or Oracle as your database on a separate server, you must also run `dbpostinstall` on the (primary) application server before starting your system.

If your upgrade fails, see the db_setup.log, install.log, or app_setup.log file in the destination directory for messages that may help fix the failure.

Importing the OMNM MySQL Database

Upgrades sometimes fail, operating system upgrades could cause database issues, and you may need to revert back to the database before the upgrade. Make sure that you back up your database before doing any kind of an upgrade.

Import the OMNM MySQL database as follows.

1 Shutdown the Application server and Web server.

2 Confirm no running java process exists.

```
ps-ef | grep java
```

3 Kill any existing java processes.

4 Drop the database with the following command lines:

```
mysqladmin -u root --password=dorado drop owmetadb
mysqladmin -u root --password=dorado drop owbusdb
mysqladmin -u root --password=dorado drop lportal
```

5 Create a new database with the following command lines:

```
mysqladmin -u root --password=dorado create owmetadb
mysqladmin -u root --password=dorado create owbusdb
mysqladmin -u root --password=dorado create lportal
```

6 Import the backed up database:

```
mysql -u root --password=dorado owmetadb < owmetadb.mysql
mysql -u root --password=dorado owbusdb < owbusdb.mysql
mysql -u root --password=dorado lportal < lportal.mysql
```

7 Start the Application server by entering the `#service oware start` command.

8 Enter `oware status` to verify that the Application server is ready.

9 Start the Web server by entering the `#service synergy start` command.

10 Enter `synergy status` to verify that the Web server is ready.

11 Login to the Web client and confirm that the data imported correctly.

5

Troubleshooting Installation Issues

Troubleshooting Installation Issues

This section provides a list of actions that created issues during OpenManage Network Manager (OMNM) installation and the steps to resolve the issue.

Action	Error	Resolution
Login	Credentials are needed to access this application.	Modify the portalext.properties file in the /oware/synergy/tomcat-xxx/webapps/ROOT/WEB-INF/class directory to include: `oware.appserver.ip=[appServerIPaddress]`
Run SOAP the **first time**	SOAP Service Manager: Unable to read 'DeployedServices.ds: assuming fresh start'	This is just an informational warning, not an error. The file referenced does not exist but is created for you.
	HeapDumpOnOutOfMemoryError	This is not an error, and is not logged at ERROR level. This is a Java VM option that enables creating a heap dump when the VM encounters and OutOfMemoryError. This dump is useful when diagnosing memory issues.

A

Installation User Interface

Installation User Interface

While running the OpenManage Network Manager (OMNM) installation wizard (installer) or the command line installer, the options that are displayed vary depending on the choices you make and the options you purchased. This section describes the windows and command line prompts where you input or change setting.

Window/Prompt	Field/Option	Description
Software Requirements		Displays some minimum system requirements and provides: • A link to access the OMNM User Guide from the user interface • The OMNM User Guide location from the command line
License Agreement		Allows you to install the product when selected. If this is a new installation, the next step is to choose the installation types. If this is an upgrade, the next step is to choose the database backup options,
Installation Types	Express Install	Installs the most common program features to their default locations. This option is recommended for most users. When selected, the next option is to select Managed Devices. The express install asks for the target RTM and completes the install based on current sizing guidelines.
	Custom	Installs the program features you select to the location you specify, and allows you to specify how they are configured. When selected, the next option is to Choose Install Folder followed by: • Network Interfaces/Network Address • Heap Settings • MySQL Setup
Managed Devices	Number of Managed Devices	Provides a list of managed device ranges from which to select. The default is less than 50. • less than 50 (8GB RAM) • 50 to 200 (12 GB RAM) • 200 to 500 (16 GB RAM) • 500 to 100 (24 GB RAM) • 1000 to 5000 (64 GB RAM) **Note:** Selecting a higher range increases system memory requirements. If you selected Express installation, the next option is Network Interfaces/Network Address.
Choose Install Folder	Directory Name	Provides the default directory. Optionally specify a diffterent directory. This option shows only if you selected a Custom Install installation type.
Network Interfaces/ Network Address didn't get this on custom install 0.104 installer	Address	Lists the network interfaces detected on the local machine. Select or enter which address to use for the OMNM application. If you selected Express installation, your system is scanned for port conflicts. If conflicts are found, the Warning! Possible port conflicts window is displayed. Otherwise, the installation starts. If you did not create the install folder before starting the installer, you will get an Invalid Install Folder error. If you selected Custom installation, the next option is Heap Settings.

Window/Prompt	Field/Option	Description
Heap Settings	Max	Allows you to customize the number of devices monitored by the OMNM application and the number of concurrent OMNM users by setting the maximum values for: • Application Server Heap Settings (Gigabytes) • Synergy Web Services Heap Settings (Gigabytes) The default values are 3 for the application server and 2 for the Web service. By default, these settings support 100 devices or less and 25 concurrent users. Refer to the Quick Start Guide and the User Guide for additional Heap settings supported.
MySQL Setup	Data Path	Specifies the database location. The default location is: *installPath*/OpenManager/Network Manager/oware3rd/mysql
	Initial Size	Is the database capacity allocated during database creation.
	Max Size	Controls the database growth. If left blank, the growth is unlimited as needed until the disk is full. If a maximum is specified, the capacity grows as needed up to the maximum size specified. Best practice is to configure Database Archiving Policies (DAPs) to prevent a full disk. See Database Management If a firewall was not detected, there were no port conflicts, or both, the installation starts.
	During a fresh install or upgrade, the installer checks for a running third-party MySQL instance. If there is an existing service named MySQL, a conflicting software found warning is displayed. Here are your options: • Continue with the installation and the OMNM installer stops the running MySQL service and then creates and starts its own service named MySQL. Note that the preexisting third-party MySQL instance and any of its related databases are not deleted. Only the service is deleted and recreated. • Return to previous windows and select an installation option that does not include the database.	
Windows Firewall Detected - Allow Access?	Allow/Do not allow firewall access	Specifies whether to allow firewall access when a firewall is detected. If you allow firewall access, rules are automatically added to the Windows Firewall Inbound Rules list. If you do not allow the firewall, the OMNM application does not perform as intended. A list of programs requiring firewall access is displayed after installation so that you can manually configure the firewall. The default is to allow firewall access.
Monitor Server Startup Now?	Yes/No	Specifies whether to run the Server Status Console now (Yes) or not (No). The default is Yes. The console monitors the startup progress of you servers and allows you to start the application. If you selected Yes, the console is displayed after the installation completes and you click Done. **Note:** This option is not available when you run the installer from the command line.

Window/Prompt	Field/Option	Description
Warning! Possible port conflicts		Indicates that the installer detected port conflicts and shows which ports are used by other applications. Resolve these conflicts before continuing with the OMNM installation. If not resolved, the OMNM application may not function.

Invalid Install Folder		Displays a message when installing on a Linux system and the the targed install directory does exist or have write permissions.
		`/installPath/openmanage/networkmanager`
		Create this directory as root:
		`mkdir -p /dellemc/openmanage/networkmanager`
		`chown :synergy /dellemc/openmanage/networkmanager`
		`chmod 770 /dellemc/openmanage/networkmanager`

Root privileges required		Requires you to run a configuration script as root before before the installation can continue. This is only for a Linux installation. Run the `$OWARE_USER_ROOT/install/root/setup.sh` setup script in a separate shell, as root. This step installs some essential environment files. It does not check for patches (the installation does that). The contents of `patch_check.log.timestamp` now appear embedded in `setup.log`.
Database Backup Options	Yes/No	Performs a full backup of date before proceeding when you select Yes (1).
Database Backup Path		Displays the default backup directory. Press Enter to accept. Otherwise, enter the full path for the backup and then press Enter. **Note:** You must have write permissions to the backup directory location. The database backup is stored in the backup.sql file in the specified directory.
Database Migration	Yes/No	Specifies whether to apply any required schema changes and automate possible data migration tasks (No) or rebuild database content (Yes). The default is No (2).

Index

A

Access Control 785
Access Profile
  General 638
  Template Editor 637
  Templates 636
  Templates Portlet 626
Acrobat 29
Action Group Editor 583
Action Groups 582
Action Job Screen Results panel 554
Actions 210
Actions in Visualizations 377
Active Directory 108
Active Performance Monitor
  Create ACLI 447
  Show Command 446
  SNMP Performance Monitoring 443
  SNMP Performance Monitoring Example 443
  Support 577
Adaptive CLI
  Actions 529
  Attribute Appearance and Validation 547
  Attribute Presentation 541
  Attributes 536
  Conditional Blocks 558
  Config File Generation 547
  Continue Pattern 544
  Editor 534
  Error Condition 543
  Example extracting Upload / Download Speeds 568
  General 534
  Juniper E-Series 534
  Juniper M/T 534
  Login limitations 527
  Monitor Attributes 578
  Non Configuration attributes 543
  Perl requirement 59
  Perl Scripts 558
  Prerequisite Validation 545
  Script Language Syntax 557
  Scripts 541
  Setting devices to configuration mode 534
  Troubleshooting 585
  Troubleshooting Timeouts 585
  With Reboot 565
Adaptive CLI FAQs 697
Add > Applications menu 116
Add a Windows Firewall Exception for Remote WMI Connections 678
Adding or Updating Extensions 701
Additional Products 18
Additional WMI Troubleshooting 678
Advanced External Script Monitor 579
Advanced Troubleshooting 656
Aging Policies
  Editor 100
  Options 102
Alarm 785
Alarm / Performance / Database 661
Alarm / Performance / Retention 661
Alarm archiving 99
Alarm Life Cycle 256
Alarm Processing Flow 256
Alarm Propagation, enhanced 251
Alarm Suppression in Topology Views 389
Alarms 185
  Alarm State 189, 726
  Assigned User 188, 726
  Correlation, Parent/Child 191, 730
  Date Assigned 189, 727
  Date Closed 189, 726
  Date Opened 187, 724, 754
  Editor 194, 732
  Email 193, 731
  Entity Type 187, 194, 724, 732
  In Topology 388
  Notification Instance 189, 726
  Service Effecting 187, 725
  service effecting 755, 776
  Snap Panels 191, 729
  Visualizations / Topologies 388
Alarms / Monitors / Performance 655
Alarms Portlet
  disable context 358
Amigopod 45
AP Editor / AP Template Editor 637
API 785

Application Server
Statistics 425
Application Server Does Not Start 649
Application Server Memory (Linux) 681
Application Server Memory Low 681
Application Server Status Monitor 442
Application Settings 96
Archiving data 99
Aruba
Backup and Restore 692
Backup and Restore limitations 692
Devices 691
SNMP limitations 692
Aruba Devices 691
Attribute Presentation 541
Attributes
Alternative ways of Grouping in Reports 278
Attributes Extraction 546
Audible Alerts 195
Audit Trail 179
Screen 176
Snap Panels 180
Audit Trail portlet 179
Authentication 38, 785
Authoritative User 636
Authorization 785
Authorizations 363, 736
Avaya
Cut-Through 692
Device Prerequisites 692
RTCP 692
Setting Up RTCP 692
Avaya Device Prerequisites 692
Avoiding restore for trivial differences 590

B

Back button 152
Background Settings 386
Backup / Restore / Deploy 654
Backup and Restore 692
Backup/Restore/Deploy 660
Backups
Configurations 398
Latest Configurations 480
Bandwidth Calculation 475
banners, characters in 141
Base Driver 41
Basic Network Considerations 35
Best Practices
Configuring Memory on Installation 61
FTP Servers 393
How to Install on Linux 65, 683
MySQL configuration 63
Overriding Properties 36
Performance and Monitors 415
Pre-Installation Checklist 29, 645
Refresh Proscan Targets 593, 770
Report size limitations 284
Single Server Hardware 31
System Repair / Maintenance 39
Web portal / Multitasking 29
BIG-IP F5 694
Brocade Devices 694
Browser Cache 29

C

Cache solutions 29
Calculating bandwidth 475
Calculations within Top N Portlets 479, 741
CAS 110
Central Authentication Server 110
Central Authentication Server (CAS) 110
Change Determination Process 616
Change Management / ProScan 589
Change Manager
Compliance Policy Violation report 594
Use paradigms 589
Change the site logo 86
Changing Dashboard Time / Date Format 483
Chat / Conferencing 158
Child Pages 162
Cisco
Copying to the Device Rather than the Application 696
Devices 695
Event Processing Rules 613
IOS upgrade caveat 695
IPSLA Monitoring 455
Proscan Policy Groups 611
Saving Running-Config to Startup Config 695
Setup Prerequisites 695
Cisco Compliance
Actions 612
Policies 610
Cisco Devices 695
Cisco Metro Ethernet SLA Monitors 458
Clustering 701
Common Device Prerequisites 691
Common Menu Items 173
Common Problems 657

Common Setup Tasks 145
Communication Problems 657
Comparison reports 274
Compliance Policy Summary 594
Conferences 159
Config File Templates
Entering encrypted passwords 547
Configuration Files 401
Editor 403
Expanded 402
Configuration Files portlet not visible 91
Configure Alarm E-mail 191, 729
Configure Distributed Component Object Model (DCOM) and User Account Control (UAC) 675
Configuring
Multitenancy 626
Configuring Audit Trails 178
Configuring Chat for Multitenancy 625
Configuring Job Viewer 178
Configuring Monitors 415
Configuring Pages and User Access 113
Configuring Resync 143
Configuring Views 375
Constraining Data Access 640
Contacts
Editor 262
Portlet 261, 708
Container
Authorizations 363, 736
Editor 360
General 361, 735
Membership 362, 736
Multitenancy 359, 734
Portlets filtered 365, 738
With Maps 369
Container Editor 360
General 361, 735
Container Manager 358
Expanded 359, 734
Container View 364
Multitenant Sites 366, 739
Context 357, 358
Context Display Rules 357
Context, disabling Alarms Portlet response 358
Continue Pattern 544
Control Center
Administrator options 76
Control Panel 75
Server Administration > Mail 79, 149
Cookies and Sessions 29
Copying to the Device Rather than the application 696
CoS 785
Create the Monitor 449
Creating a new label 399
CRON Events 699
Custom Action 212
Custom Attributes 92
Custom Debug 153
Custom Report Images 289
Customizing Report Logos 289
Cut-Through 692

D

DAP 99
SubPolicies 102
viewer 105
Dashboard
Editor 484
Time / Date Format 483
View Selection 484
Views 481
Dashboard Performance 418
Dashboard Templates for Interface and Port Equipment 493
Data Configuration 91
Data rollup 431, 481
Data summary 431
Database 785
Database Aging
Policies 99
Sub-Policies 103
Database Backup 105
database sizing 62
Date format 139
Debug 667
Default Server Status Monitor 442
Default User Roles 78
Deploy OS 410
Deploying firmware fails 660
Deployment 785
Device O/S Overrides 659
Device Prerequisites 689
Digital Certificate 785
Direct Access
Tool 121
Direct Access Fails Because of Java Security Settings 651
Disabling Remote User Account Control for Workgroups 677
Discovery
exclude IP addresses 141
Discovery / Resync 654
Discovery Issues 658
Discovery Profile
Inspection 142
Network 140
Results 142
Display Strategies 384
Displaying Tenant Domains in Top N Portlets 480
DNS 35
DNS Does Not Resolve Public Addresses 700
Dock 155
Domain 785

Domain Access 641
Domain, Name Servers 35
Domains 77
drvrpt 153

E

Edit Custom Attributes 175
Email Action 213
  Variables 219
e-mail reply 147
e-mail sender 147
E-mail variables 219
Enable Remote Procedure Call (RPC) 675
Enabling Account Privileges in WMI 676
Enabling DCOM 675
Enabling Estimated Flows 498
Encryption 785
Enhanced Alarm Propagation 251
Environment / Operating System Issues 698
Equipment 785
  Name 189, 726
Equipment Discovery - HTTP Authentication 659
Error Condition 543
Ethernet Access Point 786
Ethernet Access Service 786
Ethernet Service 786
Ethernet Trunk 785
Ethernet Trunk Port 786
Event 786
  Child 243
  Messages 238
Event Definition 786
Event Definitions 233
  Correlations 238
  Editor 235
  Extensions 240
  General 235
  Message Template 236
Event History
  Portlet 196
  Snap Panels 198
Event Instance 786
Event Life Cycle 253
Event Processing
  Filters 204
  Rules 198
Event Processing Flow 253
Event Template 786
Event Threshold 786
Expanded
  Actions Portlet 530
  Alarm Portlet 188, 726
  Audit Trail Portlet 180
  Event History Portlet 197
  Location Portlet 266
  OS Images portlet. 406
  Portlets 167
  Reports Portlet 285
  Resource Monitor 428
  Vendor Portlet 270
Export / Import 173
  Page Configurations 173
Exporter Registration 506
Exporting 786
Extended Event Definitions (EED) 243, 244
Extending Visualize Label Length 386
External Script Monitor
  Advanced 579
Extract an Adaptive CLI Attributes from a Syslog Alarm 224

F

Fail to Connect Application Server / Client 653
FAQ
  Adaptive CLI 697
  Backup and Restore 692
  Debug fine tuning 668
  Discovery Problems 657
  Log Generation Fails with "Build Failed" Error (Linux) 671
  Monitoring Mediation Servers 679
  Prevent discovery problems 657
  Radius Authentication Alternatives 110
  Resolve port conflicts 669
  Service Integrity Check 696
  Service Troubleshooting 696
  Services Discovery 696
  Troubleshooting 643
  Unix issues 681
  WMI Troubleshooting 671, 672
FAQs
  LDAP 109
Feature permissions 26
Feedback 158
File
  Backup, Restore 397
  Management 395
File Issues 647
File Servers
  Editor 394
  Port conflict 148
  Portlet 393
Filter 19, 787
  Management 95
  Visualize portlet 375
Filter / Settings (Rule Editor) 203
Finding Port Conflicts 51, 669
Fine Tuning Event Messages 238
Fine-Tuning Debug 668
Firefox difficulties 29
Firewall 57
  Issues 43

Requirements 64
Firewall Configuration 57
Fixed IP Address 36
Flash 29
For 64-bit browsers 29
Flipdebug 667
Formatting reports 273
Forward Northbound 215
Forwarding Configuration Change Commands 622
FTP
Protocol Selection 148
Servers 395
FTP server 393
Functional permissions 91

G

General (Rule Editor) 202
Generic Trap 217
getlogs 669
Getting Started 59
Google maps alternative 373
Graphs 162
Group File Management Failure 661
Group Reports 289
GUI 787

H

Handling Missing Users 26
Hardware 31, 656
Hardware Errors 699
Hardware sizing
Cloud Server 418
Heap 61
Tuning Advice 38
Heartbleed SSL vulnerability 75
Help / Tooltips 152
How to
Add / Remove Columns 169
Add User Roles 82
Add Users 79
Advanced Script Monitor Example 579
Backup Configurations 398
Configure an Action Group 584
Configure ProScan Groups 590
Configure Resource Level Permissions 117
Configure User Site Access 640
Create a Container for each Customer 118
Create a Custom Dashboard View 485
Create a Key Metrics Monitor 445
Create a Monitor for an External Script 450, 578
Create a Multitenancy Environment 627
Create a new Page Tab (My Resources) 115
Create A Performance Template 491
Create a Report Template 272
Create a Server Status Monitor Dashboard 443
Create a Simple Dashboard View 483
Create a topology view 375
Create a Visualization 375
Create an Adaptive CLI Monitor 446
Create an ICMP Monitor 445
Create an SNMP Interface Monitor 443
Create Event Processing Rules 200
Create new users 115
Create Source Group Criteria 600
DAP Workflow 99
Deploy an OS Image 411
Discover Your Network 140
Do Change Management (Example) 591
Filter Expanded Portlet Displays 172
Make an Adaptive CLI Run an External Script 556
Make an LDAP Admin User 87
Monitor Network Availability 430
Open an archived file in dapviewer. 100
Report on Change Determination 621
Restore a single configuration to many target devices 413
Restore Configurations 400
Restrict Pages for a User 116
Run Change Determination Process 616
Share a Resource 174
Use “How To” 20
Use Containers 360
Use Extended Event Definitions 243
Use Traffic Flow Analyzer 505
View Historical Dashboard Data 490
HTTP Authentication 659
HTTPS 73
https
//console.developers.google.com 373

I

ICMP (Ping) 657
ICMP Monitor 465
Import / Export 173
Incomplete Discovery 143
Increasing Startup Logging 670
Initial Logon after installation fails 651
Install on Linux 65, 683
Installation
  And Startup 60
  Windows 2012 27
Installation Issues 645
Installation Language default. 60
Installer Failure 649
Installer Logs 649
Install-From Directory 649
Installing Perl 59
Interface Portlet 356, 745
Internal FTP server limitations 393
Internet access impacts 31, 647
IP Address changes 36
IP v4 / v6 136
IPSLA OIDS 455
ISATAP 787

J

Java 29, 57
Jstack Debugging in Windows 7 679
Juniper COS 466
Juniper RPM 467
Juniper XE Devices 497

K

Key 787
Key Features 17
Key Management 787
Key Metric
  Editor 494
  Monitor 468

L

Labels 396
LDAP 86, 107
LDAP FAQs 109
Legend Tab 387
License 19
  Viewer 124
license expiration warning 125, 130
License Expiration Warning Alarms 129, 133
License Installation 702
Licenses
  Traffic flow 497, 662
Linked View 382
Links
  Visualization 389
Linux Firewall
  Turn off 654
Linux Issues 681
LLDP Warnings in Discovery 143
Localization 80
Location
  Editor 265
  Manager
    Address 265
    Parent location 265
  Portlets 263
  Snap Panels 267
  Updates 268, 366, 739
Log
  Categories 667
  Retention 670
Log Generation Fails with "Build Failed" Error (Linux) 671
Login
  Failures 653
  Restrictions 631
Logon Fails with Invalid Logon Message 652
Logs 669
logs.jar 670

M

Mail hosts 86
Maintenance
  CLI Trace Debug logs 41
  Database Aging Policies (DAP) 40, 645
  Database Backup 40
  Scheduled Items 40
Manage > Domain Access 641
Managed Object 787
Managed Resources 145
Managing Windows systems 27
Mandatory Fields 167
Map Context 366
  Portlets filtered 365, 738
  With Containers 369
  Without Containers 369
Maps and Containers Together 369
Mass deployments 409
Match Regex for each line 598
Mediation 93, 787
  Server Status Monitor 442
Mediation Agent 787
Mediation Server on separate machine fails 652
MEG 787
Memory
  Advice 38
  Footprint 61
  Tuning 37
Memory Issues 682
Memory issues
  Windows heap 682
Menu 190, 728

Bar 160
MEP 787
MIB 787
MIB Browser
Tool 120
Undiscovered devices 470
MIB File locations 121
Migrating
Heartbeats 435
Versions 24
Minimum Hardware 24, 31
Missing Performance Data / Monitor Stops Polling 662
Missing Users 26
Monitor
Discovery Relationship 415
Graph Background 440
Options Type-Specific Panels 453
Reports in Multitenant Environments 446
Strings 571
Text Values 571
Top N 478
Monitor Editor 433
Calculated Metrics 436
Conditions 441
Inventory Mappings 440
Monitor Options 436
Thresholds 438
Monitor Life Cycle 420
monitorAttributeTrend 254
Monitoring from a Cloud Server 418
Monitoring Life Cycle 420
monitorTargetDown 418
More Failures on Startup 652
MSP 77
Multiple indexes in the SNMP Interface 472
Multiple Performance Templates 493
Multitenancy 77
Access Profile Editor General 638
Access Profile Template Editor 637
Access Profile Templates 636
Access Profile Templates Portlet 626
Assigning Devices in Discovery 629
Authoritative User 636
Batch Imports 625
Chat 625
Components 626
Configuring page access 630
Constraining Data Access 640
Containers 359, 734
Control Panel 626
Creating a Site Template 627
Creating an Access Profile Template 628
Creating Sites 631
Discovery Profiles Portlet 626
Displaying Tenant Domains in Top N Portlets 480
Domain Access 641
Event Processing Rules (EPRs) 200
General 638
Importing Discovery Profiles 139
Login Restrictions 631
Manage > Domain Access 641
Managed Resources Portlet 626
Multitenant Batch Imports 625
Organization Settings 635
Page Templates 634
Portal > Page Templates 634
Portal > Site Templates 632
Portal > Sites 632
Provisioning Site-Creating User Permissions 627
Resource Access 641
Resource Assignments 638
Roles 78
Roles and permissions 78
Serving Multiple Customer Accounts 625
Site Id Filtering 641
Site Management 630
Site Management and Access Profiles 626
Site Management Editor 634
Site Management Portlet 626
Site Templates 632
Sites 632
Sites / Site Templates in Control Panel 631
Supported Portlets 629
Template Association 638
User Site Access 639
User Site Access Policy 639
User Site Access Portlet 626
View and Further Configure Devices for the Site 628
Multitenancy and LDAP 109
Multitenant Users 85
my.cnf 62
MySQL
Changing InnoDB Log Files 65
Optimizing 62
MySQL Database Issues 665
MySQL Database Sizing 62

N

Name Resolution 35
Navigation 151
Netrestore File Servers 147
Network
    Basics 35
    Considerations 35
    Monitoring 662
    Requirements 35
    Topology 374
Network Assessor Reports 292
Network Tools 120
    Direct Access 121
    MIB Browser 121
    Ping 120
New permissions 26, 91
Nokia Maps 373
Non Configuration attributes 543
Northbound Generic trap 217
NTLM 110

O

OAM 787
OID 787
Open SSO 110
OpenID 110
Oracle Database Issues 667
Organization Settings 635
OS Image
    Editor 406
    Portlet 405
OSPF 787
Portal > 88
Other Failures on Startup 652
Other Installation Issues 648
Overall Compliance 592

P

Page Level Permissions 114
Page Locations 161
page navigation bar 160
Partial Matching with Wildcard Characters in EDDs 244
Partition Name Limitations 64
Password Policies 86
Password reminder disable 73
Password Reset 148
Patch Installation 701
Patches 667
PDF 175
Performance and Monitors 415
Performance Dashboard 484
    Portlet 484
Performance Monitor Flow 420
Performance Note 20
Performance Tuning Traffic Flow Analysis 498
Perl 59
    Perl Script Example 559
Perl / Java (Groovy) Language Policies 605
Permissions 26
    Manager 89
Personal pages 114
Ping Tool 120
pmtray 64
Policy 787
Policy Enforcement Points (PEP) 787
Policy routing 788
Policy Rules 788
Portal
    Memory Settings 37, 700
    Portal Settings 86
    Roles 82
    Settings 86
Portal > Password Policies 86
Portal > Sites / Site Templates in Control Panel 631
Portal Updates (netview.war) 701
Portlet 163
    Instances 166
    Level Permissions 117
portlets
    Audit Trail 179
Ports
    Assignments 47
    Required 64
    Used 46
Post Upgrade Web Portal Problems 700
Post-processing rules 207
Potential Problem Processes 699
PPTP (Point-to-Point Tunneling Protocol) 788
Pre-Flight Checklist 645
Preventing Discovery Problems 657
Printing a portlet's contents 173
Private Key 788
Profile 788
Promote 409
Propagation
    Ports v. Devices 236
ProScan 589, 749
    Case Sensitive 600
    Compliance Reporting 619
    count number of occurrences 599
    Criteria Properties 600
    Editor 595
    Editor - Compliance 597
    Editor - General 595
    Java (Groovy) 607
    Manager 592, 768
    Monitor 469
    Multi-Line Support 600
    Perl 606
    Policy, Group Editor 609
    Supported Regular Expressions 603
    Use Cases 589
    Use paradigms 589
ProScan Policy

Creating or Modifying 594
Creating or Modifying Groups 608
Protocol
Flows 51
Protocol Flows 51
Protocols Used 36
Public / Private Page Behavior 81
Public Key 788

Q

QoS 788
QoS C3pl Account Monitor 464
Qos Class Map Monitor 460
Qos Estimate Bandwidth Monitor 464
Qos IPHC Monitor 463
Qos Match Statement Monitor 461
Qos Packet Marking Monitor 463
QoS Police Monitor 464
Qos Police Monitor 461
Qos Queuing Monitor 462
Qos RED Monitor 462
Qos Traffic-Shaping Monitor 462
Quick Navigation 119
Quick Start 59

R

RADIUS 110, 788
Raise User Limits 700
Recommended Operating System Versions 26
Recommended Windows File Servers 395
Redcell > Application Settings 96
Redcell > Mediation 93
redcellUnknownTrap 234
Refresh 152
Refresh Monitor Targets 477
Regular Expression metacharacters 603
Regular Expressions 603
metacharacters 575
Special characters 575
re-index 76
Re-indexing Search Indexes 657
Remote Mediation Ports 51
Report Missing Data 663
Report Templates
Editors 273
Reports 663
Customizing Logos 289
formatting 273
Maximum size 282
Portlet 282
Snap Panels 286
Repositories 103
Reset the WMI Counters 673
Resize columns 152
Resolving Port Conflicts 669
Resource Assignments 638
Resource Monitors
Portlet 427
Snap Panels 429
Restore Configurations 400
Restoring Compliant Files 590
Restoring Database 105
Resync 143
Resync alarms 191, 729
Retention Policies 431, 661
return address 147
Return to previous 152
revision history (guide) 21
RIP 788
Roles 82
RTCP 692
Rule Editor 202
Actions 210

S

Saving page configurations 114
Saving Running-Config to Startup Config 695
Schedule Refresh Monitor Targets 477
Schedules 181
Portlet 183
Scheduling 181
Actions 181
Scheduling Monitor Target Refresh 477
Screen resolution 28
Screen width in pixels 28
Script Monitor Example 579
Search
In Portlets 166
Indexes 76
search 165
Search Indexes 657
Secure Connections 73
Secure connections, application and mediation servers 73
Secure WBEM Access 45
Self Management 442
Self Monitoring 442
Self-signed Certificate 788
SELINUX 699
Server 106, 669
Monitor 64
Statistics 425
Server Information 698
Server log Maintenance 40
Server Sizing 31
Service
Verification 455
Service Integrity Check 696
Service/Policy Troubleshooting FAQs 696
Services 656
Services Discovery 696

Serving Multiple Customer Accounts 625
Sharing 174
Shift+Click 152
Show Performance Templates 490
Show Versions 152, 153
showversions 657
Single Server Sizing 31
Site Id Filtering 641
Site Management 630
Access Profiles 626
Editor 634
Portlet 626
Site Map portlet 162
SIteminder 110
Sizing
Memory 61
Sizing, Standalone Installations 32
SMTP 789
SMTP Mail Sender 702
SMTP, configuring 146
Snap Panels 169
SNMP 658, 789
Interface Monitor 471
Interface Monitor Example 443
Monitor 469
Performance Monitoring Example 443
Table Monitor 473
Solaris
Processor recommendation 27
Sorting 167
Spanning Tree Protocol (STP) 789
SSH (Secure Shell) 789
SSL 73
SSL (Secure Sockets Layer) 789
SSL between application and mediation servers 73
Standalone Database Installation Problems 649
Standard Change Management Policies 609
Starting
Application server 24, 39, 644
Web Client 72
Web Server 24, 39, 64, 644
Starting and Stopping Servers 652
Startup Failures 657
Startup Issues 649
Startup issues for Windows installations 651
Status Bar Messaging 157
Stopping
Application Server 24, 39, 644
Web Server. 24, 39, 644
Stopping LDAP Authentication 88
Sub-Policies 103
Supported
Flow versions 497
Operating System Versions 26
PowerConnect Models 42
Web Browsers 28
Syslog Escalation Criteria 207
System Maintenance 39
System requirements 24

T

Telnet 658
Tenant Reports 446
Terms of Use 78
Testing Remote WMI Connectivity 674
TFTP Servers 395
Threads startup error 68, 685
Threshold
Display 440
Graph Background 440
Time Format Settings 151
Timeout 660
Tooltips 152
Top [Asset] Monitors Portlets 478
Top Configuration Backups Portlet 480
Top N Portlets
Calculations 479, 741
Topological correlation 477
Topology 374
Balloon 385
Circular 385
Layout 384
Orthogonal 385
OVERVIEW 384
Radial 386
Saving 382
Topology Icon Size 374
trace 668
Traffic Flow
Device Limitations 497
Device Setup Examples 503
Drill Down 515
Performance Tuning 498
Search 516
Snapshot 518
Traffic Flow Database Advice 500
Trap (SNMP Trap) 789
Trap Forwarding 789
Trap Forwarding process 216
Triggering Bandwidth Calculations 476
Troubleshooting 24, 643
Alarm 661
Alarm / Performance / Database 661

Backup/Restore 660
Common Problems 657
Create Process failed 648, 654
Database 661
Debug 667
Deploying firmware fails 660
Device O/S Overrides 659
Discovery 143, 658
Discovery Problems 657
Failures on Startup 652
File Problems 647
getlogs 669
Increasing Startup Logging 670
Installer Failure 647
Install-From Directory 649
JMX Console 698
Log Retention 670
Login Failures 653
Logs 669
logs.jar 670
My Alerts 158
MySQL Too Many Connections 666
Network Monitoring 662
Other Failures on Startup 652
Patches 667
Performance 661
Preventing Discovery Problems 657
Resolving Port Conflicts 669
showversions 657
Startup Failures 657
Timeout 660
Tips 24, 39, 643
Unsynchronized Clocks in Clustered Installations 652
Upgrade / Data Migration Fails 656
Users and Organizations 76, 657
version.txt 657
Windows 649
Troubleshooting Adaptive CLI 585
Troubleshooting Flow 654
Tuning Log Retention 670
Turning on debugging 667

U

Uninstall 648
Uninstalling 72, 689
Unknown Traps 234
Unsynchronized Clocks in Clustered Installations 652
Update Location 268, 366, 739
Updating Driver Patches 701
Updating Polling Subscriptions 477
Updating Your License 19
Upgrade / Data Migration Fails 656
Upgrade adds permissions 91
Upgrade installation halts 25
Upgrade Installations 701
Upgrading
From a Previous Version 24
Licenses from previous version 19
Upgrading Perl 60
User
Login Report 292
Missing 26
Role 78
Screen Name length 36
User Site Access 639
User Site Access Policy 639

V

Vendors
Portlet 269
Snap Panel 272
Verify Administrator Credentials 674
version.txt 657
Versions 657
View as PDF 175
Visualization 374
Visualize
Alarms 388
As filter 375
Balloon 385
Circular 385
Circular Layout 385
Configuring Views 375
Container display settings 364, 737
Design Tools 380
Global Settings 386
Hierarchical-Cyclic 384
Layout 384
Legend Tab 387
Links in Visualization 389
My Network 374
Node alarms 389
Organic 386
Orthogonal 385
Overview 384
Properties and Settings > Layouts Tab 384
Properties and Settings > Properties 386
Radial 386
Saving Views 382
Tools 378
Top-Level Nodes Tab 387
View 382
Views 383, 390
VLAN 789

VRF
Monitor 475

W

WBEM 44
Prerequisites 44
root login 44, 691
Web-Based Enterprise Management 44
Web client timeout override 98
Web Portal 664
Web Server 700
Web Server Property Overrides 36
Web Services ports 47, 64
Why share a schema? 536
Windows 649
2012 27
Server 2008 27
Terminal Server 27
WMI 42, 58, 658
ports 58
Windows Management Instrumentation 42, 58
WMI and Operating Systems 672
WMI Authentication 678
WMI Troubleshooting 672
WMI Troubleshooting Procedures 671

X

XML Event Definition 243

A

Acrobat Reader, 40, 46
Adaptive CLI
Perl requirement, 20
Application Password, 50
Appserver, 58
Automatically Starting Servers, 50
Avoiding long timeouts, 25

B

Basic Network Considerations, 21
Best Practices
How to Install on Linux, 41

C

Change the IP address, 54
Changing the system time, 55
command line installation, 56
Command Line, Startup parameters, 49
Configuring
e-mails, 61
Ctrl+C, 64
Cygwin, 22

D

Databases on Separate Servers, 24
Default database password, 59
DNS, 21
Domain Name Servers, 21

E

E-mail configuration, 61
Enterprise (Distributed) Edition, 24

F

Failover, 26
FAQ
Change IP Address, 54
High Availability, 26
Minimum hardware, 23
System Capacity, 23
Why not install Medserver and Appserver on the same machine?, 24
Feature permissions, 67
Figures
Server Manager Client, 52
Files modified during installation, 56
Fixed IP Address, 22

H

Handling Missing Users, 67
hardware requirements, 14
Hardware, System Requirements, 23
High Availability, 26

I

Install on Linux, 41

installation types, 24
Installing
Licensing, 48
MySQL Database from console, 48
Installing Perl, 20
Internet access impacts, 62

L

Licensing, 48
Linux prerequisites, 22

M

Mediation
disabling, 60
High availability, 27
Properties, 59
Server installation, 24
migrating versions, 66
Minimum Hardware, 13, 23
Missing Users, 67
Modified Files, 56
Multiple NICs, 39, 43
MySQL
On a separate host, 24

N

name resolution, 21
network
requirements, 21
Network Considerations, 21
New permissions, 67

O

OWAdmin, 64
oware.application.servers, 22, 25, 59
OWServerAdmin, 64

P

Paired Mediation Servers, 27
Partition Name Limitations, 24
Password, 50
Paths, 21
Perl, 20
Permissions, 67
ping mediation servers, 25
pmgetstatus, 52
pmstopall, 50
Prerequisites, 22
Protocols, 22

R

Restoring Database, 68

S

screen
resolution, 14
width in pixels, 14
Server manager, 52
Server startup sequence, 50
shared drive unsupported, 21
Silent Installation, 47
Start application server, 50
Start web server, 54
startappserver, 49
Startup Sequence for Initial Testing, 60
stopappserver, 49-50, 64
stopmedserver, 64
Stopping Application Servers, 64
Stopping Servers, 64
Stopping web server, 54
System Capacity, 23
System requirements, 13
system requirements, 13

T

Threads startup error, 19

U

Uninstalling, 63
Upgrade installation halts, 66
Upgrading Perl, 21
URL for the RC Synergy portal, 27
User

Missing, 67
Using Two Interfaces, 56

W

Web Server Parameters, 53
Web Services, 50
Windows Prerequisites, 22

READER COMMENT

Did you find a mistake? Is any information missing from this publication? If so, please let us know by contacting us through one of the methods listed below. Be sure to include the manual title and publication date.

e-mail: *tsc@doradosoftware.com*

fax: 916.673.1044

mail:Dorado Software

4805 Golden Foothill Parkway

El Dorado Hills, CA 95762

dorado SOFTWARE
4805 Golden Foothill Parkway
El Dorado Hills, CA 95762
(888) 939-9959