Cisco Prime Central 2.1 Quick Start Guide

Preface

Related Documentation

See the . Cisco Prime Central 2.1 Documentation Overview

See also the documentation for the following suite components:

- Cisco Prime Network
- Cisco Prime Optical
- Cisco Prime Performance Manager
- Cisco Prime Provisioning

Note We sometimes update the documentation after original publication. Therefore, you should review the documentation on Cisco.com for any updates.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Installation Requirements

prime

This section explains what is required to install Prime Central 2.1.

Prime Central Server Requirements

The following table lists the Prime Central server system requirements.

Note The below mentioned requirements are for Small Scale deployments. For more information on the required network size for installation, see Prime Carrier Management Sizing guide.

Table 1: Database, OS, and Hardware Requirements

Minimum Requirement	Notes
Database	

Minimum Requirement	Notes
One of the following: prime • External Oracle 12C database • Embedded Oracle 12cR1 database	• If you are upgrading to Prime Central 2.1, it will continue to use Oracle 12cR1 database version 12.1.0.2. • Fresh installation of Prime Central 2.1with External; database, Local Embedded, or Remote Embedded database configuration supports only oracle 12C on RHEL 6.5 or 6.7 (database version 12.1.0.2). • Upgrade to Prime Central 2.1with External database configuration supports both Oracle 11g and Oracle 12c on RHEL 6.5, 6.7 , 6.8 or 6.9. • When configuring an external Oracle database for a large-scale environment (for example, a network with 65,000 devices), we recommend that you set the following values for these parameters to optimize performance: • Processes—1000 • Sessions—1536 • optimizer_index_caching—50 • optimizer_index_cost_adj—10 **Note** External Oracle Database configuration is supported only in standalone configuration and this configuration is not supported with Prime Central DR and HA configuration.
Memory	
• 24 GB of RAM • 10 GB of swap space	—
Disk Space	
Prime Central: • 20 GB of free space in the Prime Central installation folder • 6 GB of free space in the /tmp directory	—
External database: 22 GB for the data files	A *data file* is a physical file on disk that contains data structures such as tables and indexes. The optimal location is an external disk array (preferably RAID 10). The data files are created under the directory that you specify during installation.

Minimum Requirement	Notes
Embedded database: • 1 GB of space in the /tmp directory • 5 GB of space for software files in the home directory of the database's OS user (by default, /export/home/oracle) • 22 GB for the data files • 6 GB for the redo logs • 110 GB for the archive logs • 1.5 times the size of the database for the backup files	*Redo logs* are files that contain records of changes made to data. Redo logs should not reside on the same disk as the data files. An *archive log* is a member of a redo log that has been archived by the Oracle database. Archive logs should not reside on the same disk as the data files. Archive logs can be applied to a database backup for media recovery. A *backup file* stores a copy of the database data, which can be used to reconstruct data. Backup files should not reside on the same disk as the data files. Data files, redo logs, archive logs, and backup files are created under the directories that you specify during installation. Your system administrator must: • Back up the archive logs to tape daily. • Back up the database backups to external storage, such as to tape.
Prime Central Fault Management: • 24 GB of RAM • 50 GB of free space in the Prime Central Fault Management installation folder • 15 GB of free space in the /tmp directory • 10 GB of SWAP space	—
The server must have at least (*size of the current installation directory* + 7 GB) of free space in the folder where Prime Central 2.0 is installed.	Example: If Prime Central 2.0 is installed in the /opt/primecentral folder and that folder is 10 GB, you must have at least 17 GB of free space in the /opt folder before upgrading.
Upgrade from Prime Central Fault Management : The server must have at least (*size of the current installation directory* + 5 GB) of free space in the folder where Prime Central Fault Management 2.1.0is installed.	Example: If Prime Central Fault Management 2.1.0is installed in the /opt/primecentral/faultmgmt folder and that folder is 15 GB, you must have at least 20 GB of free space in the /opt/primecentral folder before upgrading.
64-Bit Operating System Platform	

Minimum Requirement	Notes
Red Hat Enterprise Linux (RHEL) 6.5, 6.7, 6.8 or 6.9	• The upgrade from Prime Central 2.0 to 2.1 is supported on both RHEL 5.8 and RHEL 6.4, 6.5, or 6.7, 6.8, or 6.9. Fresh installation of Prime Central 2.1is supported on RHEL 6.5 or 6.7 or 6.9. • When installing RHEL for Prime Central Fault Management installation, choose the **Software Development** option to ensure that the correct libraries are installed. We recommend that you check periodically for RHEL 5.8, 6.4, 6.5, or 6.7 6.5, 6.7, 6.8 or 6.9 patches and install any available updates.
Hardware	
One of the following: • Cisco Unified Computing System (UCS) B-series blade or C-series rackmountable server, bare metal or with VMware ESXi 5.1, 5.5, 6.0, or KVM Hypervisor (version: qemu-kvm-0.12.1.2). • Equivalent third-party vendor hardware platform	Use the following minimum hardware resources for the individual Prime Central and Fault Management servers: • 24 GB of RAM • 2 CPUs • 100 GB hard disk space Before installing RHEL 6.5, or 6.7, or , 6.8 6.9with VMWARE ESXi 5.1, 5.5, 6.0, or KVM Hypervisor (version: qemu-kvm-0.12.1.2)for Prime Central, verify your hardware compatibility. See the Cisco UCS hardware compatibility list at http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html.
Network	
NTP	NTP must be configured and enabled on Prime Central and any machine that hosts a Domain Manager.
Red Hat RPM Packages	
To verify RHEL 6 RPM packages	Enter: `rpm -q cloog-ppl compat-libcap1 compat-libstdc++-33 cpp gcc gcc-c++ glibc glibc-common glibc-devel glibc-headers gmp kernel-headers ksh libX11 libX11-common libXau libXext libXi libXtst libaio-devel libgcc libgomp libstdc++ libstdc++-devel libxcb mpfr nscd nss-softokn-freebl ppl tzdata`
For RPM installation, use the command:	**yum install <rpm>**

Minimum Requirement	Notes
For Prime Central, ensure to install the required RPM packages that are listed here .	If any of the required RPM packages are missing or if there is a version mismatch, Prime Central installation will not proceed. **Note** It is not recommended to bypass rpm verification, though there is an option to bypass rpm verification .
For Prime Central Fault Management, ensure to install the required RPM packages that are listed here .	If any of the required RPM packages are missing or if there is a version mismatch, Prime Central Fault Management installation will not proceed. **Note** It is not recommended to bypass rpm verification, though there is an option to bypass rpm verification .
For Prime Central, the following packages must be present in the system path: • perl 5.8.6 or later • top • unzip	The RPM packages should be installed along with RHEL. Refer RHEL installation procedure for more information.
To verify RHEL 6 RPM packages	Enter: `rpm -q atk audit-libs cairo compat-db compat-glibc compat-libstdc++-296 compat-libstdc++-33 compat-libtermcap compat-readline5 cracklib db4 elfutils elfutils-libs expat fontconfig freetype gamin gdk-pixbuf2 glib2 glibc glibc-common glibc-devel glibc-headers gtk2 gtk2-engines jasper-libs kernel-headers ksh libICE libSM libX11 libXau libXcomposite libXcursor libXdamage libXext libXfixes libXft libXi libXinerama libXmu libXp libXpm libXrandr libXrender libXt libXtst libgcc libjpeg-turbo libpng libselinux libstdc++ libthai libtiff libuuid libxcb ncurses-libs nscd nss-softokn-freebl openmotif22 pam pango pixman rpm-build xulrunner zlib`
For RPM installation, use the command	**yum install <rpm>**
Red Hat Services and Components	

Minimum Requirement	Notes
The following Red Hat services and components (usually present as part of the Red Hat installation) are required: • /usr/bin/scp—Secure copy tool. • /usr/sbin/sshd—SSH daemon. • /usr/bin/ssh—SSH. • /usr/bin/ssh-keygen—Tool to generate, manage, and convert authentication keys.	The RPM packages should be installed along with RHEL. Refer RHEL installation procedure for more information.

Additional Requirements

- If you are using any of the OpenSSL versions known to have the CVE-2014-0160 vulnerability (better-known as Heartbleed), please review and take the steps outlined in the OpenSSL Security Advisory [07 Apr 2014].
- All systems must have access to the Prime Central server hostname.
- Clocks must be synchronized on Prime Central and all attached Prime application servers.
- When you install Prime Central, Prime Central Fault Management, or any suite components, Domain Name System (DNS) must be enabled on the hosts. Otherwise, Prime Central components cannot communicate, and clients cannot launch Prime Central.

  If the hosts do not have DNS access, or if their hostnames are not registered in the DNS, you must add those hostnames (with the correct IP addresses) to your local hosts file (/etc/hosts on Linux; ${Windows}\System32\drivers\etc\hosts on Windows).
- If DNS is not available, the Prime Central server and the Prime Central integration layer must include in their /etc/hosts file the following entries for Prime Network, Prime Optical, Prime Performance Manager, Prime Provisioning, :

  application-IP-address fully-qualified-application-hostname application-hostname

  For example, if Prime Optical is installed on the "my-server" workstation with IP address 209.165.200.225, the following entry must exist in the /etc/hosts file on the Prime Central portal and the Prime Central integration layer:

  ```
  209.165.200.225 my-server.cisco.com my-server
  ```

Installed Red Hat RPM Packages

Following are the Red Hat RPM packages required by both Prime Central and Prime Central Fault Management installer:

Note All packages mentioned in Table 2: RHEL 6.7 and 6.8 RPM Packages below are required for both RHEL 6.7 and 6.8. You must install every package whether you choose to use RHEL 6.7 or 6.8.

Table 2: RHEL 6.7 and 6.8 RPM Packages for Prime Central and Prime Central Fault Management Installer

atk-1.30.0-1.el6.i686	libXdamage-1.1.3-4.el6.x86_64
atk-1.30.0-1.el6.x86_64	libXext-1.3.3-1.el6.x86_64
audit-libs-2.4.5-6.el6.i686	libXext-1.3.3-1.el6.x86_64
audit-libs-2.4.5-6.el6.x86_64	libXfixes-5.0.3-1.el6.i686
cairo-1.8.8-6.el6_6.i686	libXfixes-5.0.3-1.el6.x86_64
cairo-1.8.8-6.el6_6.x86_64	libXft-2.3.2-1.el6.i686
compat-db-4.6.21-17.el6.i686	libXft-2.3.2-1.el6.x86_64
compat-db-4.6.21-17.el6.x86_64	libXi-1.7.8-1.el6.i686
compat-glibc-2.5-46.2.x86_64	libXi-1.7.8-1.el6.x86_64
compat-libstdc++-296-2.96-144.el6.i686	libXinerama-1.1.3-2.1.el6.i686
compat-libstdc++-33-3.2.3-69.el6.x86_64	libXmu-1.1.1-2.el6.i686
compat-libtermcap-2.0.8-49.el6.i686	libXmu-1.1.1-2.el6.x86_64
compat-libtermcap-2.0.8-49.el6.x86_64	libXp-1.0.2-2.1.el6.i686
compat-readline5-5.2-17.1.el6.i686	libXp-1.0.2-2.1.el6.x86_64
compat-readline5-5.2-17.1.el6.x86_64	libXpm-3.5.10-2.el6.i686
cracklib-2.8.16-4.el6.i686	libXpm-3.5.10-2.el6.x86_64
cracklib-2.8.16-4.el6.x86_64	llibXrandr-1.5.1-1.el6.i686
db4-4.7.25-22.el6.i686	libXrandr-1.5.1-1.el6.x86_64
db4-4.7.25-22.el6.x86_64	libXrender-0.9.10-1.el6.i686
elfutils-0.164-2.el6.x86_64	libXrender-0.9.10-1.el6.x86_64
elfutils-libs-0.164-2.el6.x86_64	libXt-1.1.4-6.1.el6.i686
expat-2.0.1-13.el6_8.i686	libXt-1.1.4-6.1.el6.x86_64
expat-2.0.1-13.el6_8.x86_64	libXtst-1.2.3-1.el6.i686
expect-5.44.1.15-5.el6_4.x86_64	libXtst-1.2.3-1.el6.x86_64
fontconfig-2.8.0-5.el6.i686	libgcc-4.4.7-18.el6.i686
fontconfig-2.8.0-5.el6.x86_64	libgcc-4.4.7-18.el6.x86_64
freetype-2.3.11-17.el6.i686	libjpeg-turbo-1.2.1-3.el6_5.i686
freetype-2.3.11-17.el6.x86_64	libjpeg-turbo-1.2.1-3.el6_5.x86_64

gamin-0.1.10-9.el6.i686	libpng-1.2.49-2.el6_7.i686
gamin-0.1.10-9.el6.x86_64	libpng-1.2.49-2.el6_7.x86_64
gdk-pixbuf2-2.24.1-6.el6_7.i686	libselinux-2.0.94-7.el6.i686
gdk-pixbuf2-2.24.1-6.el6_7.x86_64	libselinux-2.0.94-7.el6.x86_64
glib2-2.28.8-9.el6.i686	libstdc++-4.4.7-18.el6.i686
glib2-2.28.8-9.el6.x86_64	libstdc++-4.4.7-18.el6.x86_64
glibc-2.12-1.209.el6_9.1.i686	libthai-0.1.12-3.el6.i686
glibc-2.12-1.209.el6_9.1.x86_64	libthai-0.1.12-3.el6.x86_64
glibc-common-2.12-1.209.el6_9.1.x86_64	libtiff-3.9.4-21.el6_8.i686
glibc-devel-2.12-1.209.el6_9.1.i686	libtiff-3.9.4-21.el6_8.x86_64
glibc-devel-2.12-1.209.el6_9.1.x86_64	libuuid-2.17.2-12.28.el6.i686
glibc-headers-2.12-1.209.el6_9.1.x86_64	libuuid-2.17.2-12.28.el6.x86_64
gtk2-2.24.23-9.el6.i686	libxcb-1.12-4.el6.i686
gtk2-2.24.23-9.el6.x86_64	libxcb-1.12-4.el6.x86_64
gtk2-engines-2.18.4-5.el6.i686	ncurses-libs-5.7-4.20090207.el6.i686
gtk2-engines-2.18.4-5.el6.x86_64	ncurses-libs-5.7-4.20090207.el6.x86_64
jasper-libs-1.900.1-21.el6_9.i686	nss-softokn-freebl-3.14.3-23.3.el6_8.i686
jasper-libs-1.900.1-21.el6_9.x86_64	nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64
kernel-headers-2.6.32-696.3.1.el6.x86_64	openmotif22-2.2.3-19.el6.i686
ksh-20120801-34.el6_9.x86_64	openmotif22-2.2.3-19.el6.x86_64
libICE-1.0.6-1.el6.i686	pam-1.1.1-24.el6.i686
libICE-1.0.6-1.el6.x86_64	pam-1.1.1-24.el6.x86_64
libSM-1.2.1-2.el6.i686	pango-1.28.1-11.el6.i686
libSM-1.2.1-2.el6.x86_64	pango-1.28.1-11.el6.x86_64
libX11-1.6.4-3.el6.i686	pixman-0.32.8-1.el6.i686
libX11-1.6.4-3.el6.x86_64	pixman-0.32.8-1.el6.x86_64
libXau-1.0.6-4.el6.i686	rpm-build-4.8.0-55.el6.x86_64
libXau-1.0.6-4.el6.x86_64	sshpass-1.05-1.el6.rf.x86_64
libXcomposite-0.4.3-4.el6.i686	tcl-8.5.7-6.el6.x86_64

libXcomposite-0.4.3-4.el6.x86_64	xulrunner-17.0.10-1.el6_4.i686
libXcursor-1.1.14-2.1.el6.i686	xulrunner-17.0.10-1.el6_4.x86_64
libXcursor-1.1.14-2.1.el6.x86_64	zlib-1.2.3-29.el6.i686
libXdamage-1.1.3-4.el6.i686	zlib-1.2.3-29.el6.x86_64

Note Before proceeding with the installation, ensure that the above RPMs or a higher version is installed.

Use of **rpm –ivh <rpm>** is not recommended because dependencies are not installed when this command is used. Instead, use **yum install <rpm>**.

Table 3: RHEL 6.5 RPM Packages for Prime Central and Prime Central Fault Management Installer

atk-1.30.0-1.el6.i686	libXdamage-1.1.3-4.el6.x86_64
atk-1.30.0-1.el6.x86_64	libXext-1.3.1-2.el6.i686 (same version required)
audit-libs-2.4.5-6.el6.i686	libXext-1.3.1-2.el6.x86_64 (same version required)
audit-libs-2.4.5-6.el6.x86_64	libXfixes-5.0.3-1.el6.i686
cairo-1.8.8-6.el6_6.i686	libXfixes-5.0.3-1.el6.x86_64
cairo-1.8.8-6.el6_6.x86_64	libXft-2.3.2-1.el6.i686
compat-db-4.6.21-17.el6.i686	libXft-2.3.2-1.el6.x86_64
compat-db-4.6.21-17.el6.x86_64	libXi-1.6.1-3.el6.i686 (same version required)
compat-glibc-2.5-46.2.x86_64	libXi-1.6.1-3.el6.x86_64 (same version required)
compat-libstdc++-296-2.96-144.el6.i686	libXinerama-1.1.3-2.1.el6.i686
compat-libstdc++-33-3.2.3-69.el6.x86_64	libXmu-1.1.1-2.el6.i686
compat-libtermcap-2.0.8-49.el6.i686	libXmu-1.1.1-2.el6.x86_64
compat-libtermcap-2.0.8-49.el6.x86_64	libXp-1.0.2-2.1.el6.i686
compat-readline5-5.2-17.1.el6.i686	libXp-1.0.2-2.1.el6.x86_64
compat-readline5-5.2-17.1.el6.x86_64	libXpm-3.5.10-2.el6.i686
cracklib-2.8.16-4.el6.i686	libXpm-3.5.10-2.el6.x86_64
cracklib-2.8.16-4.el6.x86_64	llibXrandr-1.5.1-1.el6.i686
db4-4.7.25-22.el6.i686	libXrandr-1.5.1-1.el6.x86_64
db4-4.7.25-22.el6.x86_64	libXrender-0.9.10-1.el6.i686

elfutils-0.164-2.el6.x86_64	libXrender-0.9.10-1.el6.x86_64
elfutils-libs-0.164-2.el6.x86_64	libXt-1.1.4-6.1.el6.i686
expat-2.0.1-13.el6_8.i686	libXt-1.1.4-6.1.el6.x86_64
expat-2.0.1-13.el6_8.x86_64	libXtst-1.2.1-2.el6.i686 (same version required)
expect-5.44.1.15-5.el6_4.x86_64	libXtst-1.2.1-2.el6.x86_64 (same version required)
fontconfig-2.8.0-5.el6.i686	libgcc-4.4.7-18.el6.i686
fontconfig-2.8.0-5.el6.x86_64	libgcc-4.4.7-18.el6.x86_64
freetype-2.3.11-17.el6.i686	libjpeg-turbo-1.2.1-3.el6_5.i686
freetype-2.3.11-17.el6.x86_64	libjpeg-turbo-1.2.1-3.el6_5.x86_64
gamin-0.1.10-9.el6.i686	libpng-1.2.49-2.el6_7.i686
gamin-0.1.10-9.el6.x86_64	libpng-1.2.49-2.el6_7.x86_64
gdk-pixbuf2-2.24.1-6.el6_7.i686	libselinux-2.0.94-7.el6.i686
gdk-pixbuf2-2.24.1-6.el6_7.x86_64	libselinux-2.0.94-7.el6.x86_64
glib2-2.28.8-9.el6.i686	libstdc++-4.4.7-18.el6.i686
glib2-2.28.8-9.el6.x86_64	libstdc++-4.4.7-18.el6.x86_64
glibc-2.12-1.209.el6_9.1.i686	libthai-0.1.12-3.el6.i686
glibc-2.12-1.209.el6_9.1.x86_64	libthai-0.1.12-3.el6.x86_64
glibc-common-2.12-1.209.el6_9.1.x86_64	libtiff-3.9.4-21.el6_8.i686
glibc-devel-2.12-1.209.el6_9.1.i686	libtiff-3.9.4-21.el6_8.x86_64
glibc-devel-2.12-1.209.el6_9.1.x86_64	libuuid-2.17.2-12.28.el6.i686
glibc-headers-2.12-1.209.el6_9.1.x86_64	libuuid-2.17.2-12.28.el6.x86_64
gtk2-2.24.23-9.el6.i686	libxcb-1.8.1-1.el6.i686 (same version required)
gtk2-2.24.23-9.el6.x86_64	libxcb-1.8.1-1.el6.x86_64 (same version required)
gtk2-engines-2.18.4-5.el6.i686	ncurses-libs-5.7-4.20090207.el6.i686
gtk2-engines-2.18.4-5.el6.x86_64	ncurses-libs-5.7-4.20090207.el6.x86_64
jasper-libs-1.900.1-21.el6_9.i686	nss-softokn-freebl-3.14.3-23.3.el6_8.i686
jasper-libs-1.900.1-21.el6_9.x86_64	nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64
kernel-headers-2.6.32-696.3.1.el6.x86_64	openmotif22-2.2.3-19.el6.i686
ksh-20120801-34.el6_9.x86_64	openmotif22-2.2.3-19.el6.x86_64

libICE-1.0.6-1.el6.i686	pam-1.1.1-24.el6.i686
libICE-1.0.6-1.el6.x86_64	pam-1.1.1-24.el6.x86_64
libSM-1.2.1-2.el6.i686	pango-1.28.1-11.el6.i686
libSM-1.2.1-2.el6.x86_64	pango-1.28.1-11.el6.x86_64
libX11-1.5.0-4.el6.i686 (same version required)	pixman-0.32.8-1.el6.i686
libX11-1.5.0-4.el6.x86_64 (same version required)	pixman-0.32.8-1.el6.x86_64
libXau-1.0.6-4.el6.i686	rpm-build-4.8.0-55.el6.x86_64
libXau-1.0.6-4.el6.x86_64	sshpass-1.05-1.el6.rf.x86_64
libXcomposite-0.4.3-4.el6.i686	tcl-8.5.7-6.el6.x86_64
libXcomposite-0.4.3-4.el6.x86_64	xulrunner-17.0.10-1.el6_4.i686
libXcursor-1.1.14-2.1.el6.i686	xulrunner-17.0.10-1.el6_4.x86_64
libXcursor-1.1.14-2.1.el6.x86_64	zlib-1.2.3-29.el6.i686
libXdamage-1.1.3-4.el6.i686	zlib-1.2.3-29.el6.x86_64

Note It is recommended that you use the same rpm for some of the packages in RHEL 6.5 as specified in the table above. Do not install a higher version as it is not supported.

Following are the Red Hat RPM packages required by the Prime Central installer:

Table 4: RHEL 6.5 RPM Packages for Prime Central Installer

cloog-ppl-0.15.7-1.2.el6.x86_64.rpm	libX11-1.5.0-4.el6.x86_64.rpm (same version required)
compat-libcap1-1.10-1.x86_64.rpm	libX11-common-1.5.0-4.el6.noarch.rpm (same version required)
compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm	libXau-1.0.6-4.el6.i686.rpm
cpp-4.4.7-18.el6.x86_64.rpm	libXau-1.0.6-4.el6.x86_64.rpm
expect-5.44.1.15-5.el6_4.x86_64.rpm	libXext-1.3.1-2.el6.i686.rpm (same version required)
gcc-4.4.7-18.el6.x86_64.rpm	libXext-1.3.1-2.el6.x86_64.rpm (same version required)
gcc-c++-4.4.7-18.el6.x86_64.rpm	libXi-1.6.1-3.el6.i686.rpm (same version required)
glibc-2.12-1.209.el6_9.1.i686.rpm	libXi-1.6.1-3.el6.x86_64.rpm (same version required)
glibc-2.12-1.209.el6_9.1.x86_64.rpm	libXtst-1.2.1-2.el6.i686.rpm (same version required)

glibc-common-2.12-1.209.el6_9.1.x86_64.rpm	libXtst-1.2.1-2.el6.x86_64.rpm (same version required)
glibc-devel-2.12-1.209.el6_9.1.i686.rpm	libaio-devel-0.3.107-10.el6.x86_64.rpm
glibc-devel-2.12-1.209.el6_9.1.x86_64.rpm	libgcc-4.4.7-18.el6.i686.rpm
glibc-headers-2.12-1.209.el6_9.1.x86_64.rpm	libgcc-4.4.7-18.el6.x86_64.rpm
gmp-4.3.1-12.el6.i686.rpm	libgomp-4.4.7-18.el6.i686.rpm
kernel-headers-2.6.32-696.3.1.el6.x86_64.rpm	libgomp-4.4.7-18.el6.x86_64.rpm
ksh-20120801-34.el6_9.x86_64.rpm	libstdc++-4.4.7-18.el6.i686.rpm
libX11-1.5.0-4.el6.i686.rpm (same version required)	libstdc++-4.4.7-18.el6.x86_64.rpm
libstdc++-devel-4.4.7-18.el6.x86_64.rpm	libxcb-1.8.1-1.el6.x86_64.rpm (same version required)
libxcb-1.8.1-1.el6.i686.rpm(same version required)	mpfr-2.4.1-6.el6.x86_64.rpm
nscd-2.12-1.209.el6_9.1.x86_64.rpm	nss-softokn-freebl-3.14.3-23.3.el6_8.i686.rpm
nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64.rpm	ppl-0.10.2-11.el6.x86_64.rpm
sshpass-1.05-1.el6.rf.x86_64.rpm	tcl-8.5.7-6.el6.x86_64.rpm
tzdata-2017b-1.el6.noarch.rpm	

Note It is recommended that you use the same rpm for some of the packages in RHEL 6.5 as specified in the table above. Do not install a higher version as it is not supported.

Table 5: RHEL 6.7 RPM Packages for Prime Central Installer

cloog-ppl-0.15.7-1.2.el6.x86_64.rpm	libXau-1.0.6-4.el6.i686.rpm
compat-libcap1-1.10-1.x86_64.rpm	libXau-1.0.6-4.el6.x86_64.rpm
compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm	libXext-1.3.3-1.el6.i686.rpm
cpp-4.4.7-18.el6.x86_64.rpm	libXext-1.3.3-1.el6.x86_64.rpm
expect-5.44.1.15-5.el6_4.x86_64.rpm	libXi-1.7.8-1.el6.i686.rpm
gcc-4.4.7-18.el6.x86_64.rpm	libXi-1.7.8-1.el6.x86_64.rpm
gcc-c++-4.4.7-18.el6.x86_64.rpm	libXtst-1.2.3-1.el6.i686.rpm
glibc-2.12-1.209.el6_9.1.i686.rpm	libXtst-1.2.3-1.el6.x86_64.rpm
glibc-2.12-1.209.el6_9.1.x86_64.rpm	libaio-devel-0.3.107-10.el6.x86_64.rpm
glibc-common-2.12-1.209.el6_9.1.x86_64.rpm	libgcc-4.4.7-18.el6.i686.rpm

glibc-devel-2.12-1.209.el6_9.1.i686.rpm	libgcc-4.4.7-18.el6.x86_64.rpm
glibc-devel-2.12-1.209.el6_9.1.x86_64.rpm	libgomp-4.4.7-18.el6.i686.rpm
glibc-headers-2.12-1.209.el6_9.1.x86_64.rpm	libgomp-4.4.7-18.el6.x86_64.rpm
gmp-4.3.1-12.el6.i686.rpm	libstdc++-4.4.7-18.el6.i686.rpm
kernel-headers-2.6.32-696.3.1.el6.x86_64.rpm	libstdc++-4.4.7-18.el6.x86_64.rpm
libstdc++-devel-4.4.7-18.el6.x86_64	ksh-20120801-34.el6_9.x86_64.rpm
libxcb-1.12-4.el6.i686.rpm	libX11-1.6.4-3.el6.i686.rpm
libxcb-1.12-4.el6.x86_64.rpm	libX11-1.6.4-3.el6.x86_64.rpm
libX11-common-1.6.4-3.el6.noarch.rpm	mpfr-2.4.1-6.el6.x86_64.rpm
nss-softokn-freebl-3.14.3-23.3.el6_8.i686.rpm	nscd-2.12-1.209.el6_9.1.x86_64.rpm
ppl-0.10.2-11.el6.x86_64.rpm	nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64.rpm
tcl-8.5.7-6.el6.x86_64.rpm	sshpass-1.05-1.el6.rf.x86_64.rpm
tzdata-2017b-1.el6.noarch.rpm	

Note Before proceeding with the installation, ensure that the above RPMs or a higher version is installed.

Use of **rpm –ivh <rpm>** is not recommended because dependencies are not installed when this command is used. Instead, use **yum install <rpm>**.

Protocols and Ports of Prime Central Components

The following table lists the protocols and ports that Prime Central component uses.

Table 6: Protocols and Ports of Prime Central Components

Port No.	Exposure	Protocol	Used by...	The system administrator should...
Prime Central Portal				
1107	Public	SSH	Internal services for SSH communication	Apply a rate-limiting policy.
1108	Public	TCP	Embedded Oracle database	Apply a rate-limiting policy.
1199	Private	TCP	RMI service	Only allow access to this port from localhost.
1521	Public	TCP	Oracle database server listener	Apply a rate-limiting policy.

Port No.	Exposure	Protocol	Used by...	The system administrator should...
8005	Private	TCP	Tomcat shutdown	Only allow access to this port (or its equivalent) from the Prime Central portal, unless remote shutdown is required.
8009	Private	TCP	Apache JServ Protocol (AJP)	Disable this port if it is not in use.
8090	Private	TCP	Discovery service	Only allow access to this port from localhost.
8443	Public	TCP	Default HTTPS port; subject to change during installation	Apply a rate-limiting policy and make this port available to all users who need to access the Prime Central portal.
Prime Central Integration Layer				
1099–1103	Private	TCP	Karaf JMX RMI registry (Prime Central integration layer management)	Allow a dynamic range from 1099 to the number of integration layer registrations; for example, 1103. Set aside a range of 10 ports.
8101–8105	Private (localhost)	TCP	Karaf SSH shell	Allow a dynamic range from 8101 to the number of integration layer registrations; for example 8105. Set aside a range of 10 ports.
9020	Private/Public	TCP	Alarm management northbound interface (NBI)	Only allow access to this port from localhost, unless alarm management NBI access is required. If so, enable access from the alarm management client machines and apply a rate-limiting policy.
9110	Private/Public	TCP	Multi-Technology Operations System Interface (MTOSI) WS-SOAP NBI	Only allow access to this port from localhost, unless MTOSI NBI access is required. If so, enable access from the MTOSI client machines and apply a rate-limiting policy.
9220	Private/Public	TCP	3GPP NBI	Only allow access to this port from localhost, unless 3GPP NBI access is required. If so, enable access from the 3GPP client machines and apply a rate-limiting policy.
32768–61000	Private/Public	TCP	Ephemeral ports	Only allow access to this port from localhost, unless Prime Central uses a dual-server (distributed) installation. If so, enable access from the Prime Central portal and apply a rate-limiting policy.

Port No.	Exposure	Protocol	Used by...	The system administrator should...
44444–44448	Private	TCP	Karaf JMX RMI server (Prime Central integration layer management)	Allow a dynamic range from 44444 to the number of integration layer registrations; for example 44448. Set aside a range of 10 ports.
61614	Private/Public	TCP	JMS NIO Failover transport	Only allow access to this port from localhost, unless Prime Central uses a dual-server (distributed) installation with JMS NIO Failover transport. If so, enable access from the Prime Central portal and apply a rate-limiting policy.
61615	Private/Public	TCP	Java Message Service (JMS) Secure Sockets Layer (SSL) transport	Only allow access to this port from localhost, unless Prime Central uses a dual-server (distributed) installation with JMS SSL transport. If so, enable access from the Prime Central portal and apply a rate-limiting policy.
61616	Private/Public	TCP	JMS NIO transport	Only allow access to this port from localhost, unless Prime Central uses a dual-server (distributed) installation with JMS NIO transport. If so, enable access from the Prime Central portal and apply a rate-limiting policy.
Fault Management Component				
1162	Public	TCP, UDP	Fault Management	Allow applications to use this port to send SNMP traps to the Prime Central Fault Management component.
2000	Private	TCP	Fault Management	Only allow access to this port from localhost.
4100	Private	TCP	Fault Management	Only allow access to this port from localhost.
4200	Private	TCP	Fault Management	Only allow access to this port from localhost.
4300	Private	TCP	Fault Management	Only allow access to this port from localhost.
4400	Private	TCP	Fault Management	Only allow access to this port from localhost.
5435	Private	TCP	Fault Management	Only allow access to this port from localhost.
9043	Private	TCP	Fault Management	Only allow access to this port from localhost.

Port No.	Exposure	Protocol	Used by...	The system administrator should...
9060	Private	TCP	Fault Management	Only allow access to this port from localhost.
9080	Private	TCP	Fault Management	Only allow access to this port from localhost.
16310	Private	TCP	Fault Management	Only allow access to this port from localhost.
16311	Public	TCP	Fault Management	Allow Prime Central to use this port to display the Alarm Browser and Alarm Report portlets.
16312	Private	TCP	Fault Management	Only allow access to this port from localhost.
16313	Public	TCP	Fault Management	Allow the Prime Central integration layer to use this port to send user management and suite monitoring requests to the Prime Central Fault Management component.
16314	Private	TCP	Fault Management	Only allow access to this port from localhost.
16315	Private	TCP	Fault Management	Only allow access to this port from localhost.
16316	Private	TCP	Fault Management	Only allow access to this port from localhost.
16318	Private	TCP	Fault Management	Only allow access to this port from localhost.
16320	Private	TCP	Fault Management	Only allow access to this port from localhost.
16321	Private	TCP	Fault Management	Only allow access to this port from localhost.
16322	Private	TCP	Fault Management	Only allow access to this port from localhost.
16323	Private	TCP	Fault Management	Only allow access to this port from localhost.
16324	Private	TCP	Fault Management	Only allow access to this port from localhost.

Port Exposure Categories

The ports listed in Table 6: Protocols and Ports of Prime Central Components belong to the following exposure categories:

- Private—These ports should not be accessible from outside workstations. Administrators should restrict access to localhost (127.0.0.1). Administrators can use firewall software such as Linux iptables to implement access restrictions.
- Public—These ports might need to be accessible from outside workstations. To protect against external security threats, administrators should restrict access to these ports to only those workstations that need explicit access. As additional precaution against denial of service (DoS) attacks, administrators should apply rate-limiting policies. Administrators can use firewall software such as Linux iptables to implement access restrictions and rate-limiting policies. Whenever possible, if the set of source addresses is known, restrict all other access.
  - In some cases, the packet source is not known ahead of time; for example, the HTTPS port that clients use to communicate with the Prime Central portal.
  - In some cases, the packet source is known ahead of time; for example, a distributed Prime Central installation, where the Prime Central portal must communicate with the Prime Central integration layer.
- Ephemeral—These ports are similar to public ports, except that their port numbers are not fixed. Depending on the Prime Central deployment scenario, ephemeral ports might require public exposure. If so, administrators should restrict access to these ports to only those workstations that need explicit access. As additional precaution against denial of service (DoS) attacks, administrators should apply rate-limiting policies. Administrators can use firewall software such as Linux iptables to implement access restrictions and rate-limiting policies.
  - In some cases, the packet source is not known ahead of time; for example, the HTTPS port that clients use to communicate with the Prime Central portal.
  - In some cases, the packet source is known ahead of time; for example, a distributed Prime Central installation, where the Prime Central portal must communicate with the Prime Central integration layer.
- Restricted—We recommend that administrators restrict access to all other ports. Administrators can use firewall software such as Linux iptables to implement access restrictions.

Sample Remediation Policy Script

The following sample script shows how a system administrator can implement a remediation policy by using the built-in Linux iptables firewall feature.

```
#!/bin/bash

FWCONF=/etc/init.d/iptables
FW=/sbin/iptables

#Start firewall
$FWCONF save
$FWCONF start

#Remove any previous rules:
$FW -F
$FW -X
$FW -P INPUT ACCEPT
$FW -P FORWARD ACCEPT
$FW -P OUTPUT ACCEPT

#Drop invalid packets
```

```
$FW -A INPUT -m state --state INVALID -j LOG --log-prefix "DROP INVALID "   --log-ip-options
 --log-tcp-options
$FW -A INPUT -m state --state INVALID -j DROP

#Permit rules

#Allow local packets (category 1 packets)
$FW -A INPUT -i lo -j ACCEPT

#Allow icmp/esp/ah packets
$FW -A INPUT -p icmp --icmp-type any -j ACCEPT
$FW -A INPUT -p esp -j ACCEPT
$FW -A INPUT -p ah -j ACCEPT

#Allow any tcp traffic to port <allowed-port> with rate-limiting to <rate> packets/second
(category 2a packets)
$FW -A INPUT -s 0/0 -d 0/0 -j ACCEPT --protocol tcp --dport <allowed-port> -m hashlimit
--hashlimit
<rate>/second

#Allow tcp traffic from source address <source-IP> to a port <allowed-port> with rate-limiting
 to <rate>
packets/second (category 2b packets)
$FW -A INPUT -s <source-IP>/32 -d 0/0 -j ACCEPT --protocol tcp --dport <allowed-port> -m
hashlimit --hashlimit
 <rate>/second

#Allow any tcp traffic to ephemeral ports with rate-limiting to <rate> packets/second
(category 3a packets)
$FW -A INPUT -p tcp --dport 32768:6100 -m hashlimit --hashlimit <rate>/second

#Allow tcp traffic from source address <source-IP> to ephemeral ports with rate-limiting
to <rate>
packets/second (category 3b packets)
$FW -A INPUT -s <source-IP>/32 -p tcp --dport 32768:6100 -m hashlimit --hashlimit
<rate>/second

#Allow established connections
$FW -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$FW -A INPUT -p tcp --dport ssh   -j ACCEPT

#Drop everything else (category 4 packets)
$FW -A INPUT -j DROP

#Save firewall rules.
$FWCONF save
```

Embedded Database Requirements

An embedded database for use with Prime Central has the following requirements. These requirements are in addition to those in Prime Central Server Requirements .

You can install the embedded database on Red Hat Enterprise Linux (RHEL) 6.5, 6.7, 6.8 or 6.9 .

Table 7: RHEL 6.4 RPM Packages

cloog-ppl-0.15.7-1.2.el6.x86_64.rpm	libgcc-4.4.7-3.el6.i686.rpm
compat-libcap1-1.10-1.x86_64.rpm	libstdc++-devel-4.4.7-3.el6.x86_64.rpm
compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm	libX11-1.5.0-4.el6.i686.rpm

cpp-4.4.7-3.el6.x86_64.rpm	libXau-1.0.6-4.el6.i686.rpm
gcc-4.4.7-3.el6.x86_64.rpm	libxcb-1.8.1-1.el6.i686.rpm
gcc-c++-4.4.7-3.el6.x86_64.rpm	libXext-1.3.1-2.el6.i686.rpm
glibc-2.12-1.107.el6.i686.rpm	libXi-1.6.1-3.el6.i686.rpm
glibc-devel-2.12-1.107.el6.x86_64.rpm	libXtst-1.2.1-2.el6.i686.rpm
glibc-headers-2.12-1.107.el6.x86_64.rpm	mpfr-2.4.1-6.el6.x86_64.rpm
kernel-headers-2.6.32-358.el6.x86_64.rpm	nss-softokn-freebl-3.12.9-11.el6.i686.rpm
ksh-20100621-19.el6.x86_64.rpm	ppl-0.10.2-11.el6.x86_64.rpm
libaio-devel-0.3.107-10.el6.x86_64.rpm	

Note To verify that all of the required RHEL 6.4 RPM packages are installed, enter the following command as the root user:

 # rpm -q cloog-ppl compat-libcap1 compat-libstdc++-33 cpp gcc gcc-c++ glibc glibc-devel glibc-headers kernel-headers ksh libaio-devel libgcc libstdc++-devel libX11 libXau libxcb libXext libXi libXtst mpfr nss-softokn-freebl ppl --qf '%{name}.%{arch}\n'|sort

The following components (usually installed as part of Red Hat) must be present in the system path:

- /bin/sh
- /bin/tcsh
- gunzip
- perl 5.8.6 or later
- tar

Table 8: RHEL 6.5 RPM Packages

cpp-4.4.7-17.el6.x86_64.rpm	libgcc-4.4.7-17.el6.i686.rpm
gcc-4.4.7-17.el6.x86_64.rpm	libgomp-4.4.7-17.el6.i686.rpm
gcc-c++-4.4.7-17.el6.x86_64.rpm	libgomp-4.4.7-17.el6.x86_64.rpm
glibc-2.12-1.192.el6.i686.rpm	libstdc++-4.4.7-17.el6.i686.rpm
glibc-2.12-1.192.el6.x86_64.rpm	nss-softokn-freebl-3.14.3-23.3.el6_8.i686.rpm
glibc-common-2.12-1.192.el6.x86_64.rpm	tzdata-2016j-1.el6.noarch.rpm
glibc-devel-2.12-1.192.el6.i686.rpm	
glibc-devel-2.12-1.192.el6.x86_64.rpm	

glibc-headers-2.12-1.192.el6.x86_64.rpm	
gmp-4.3.1-10.el6.i686.rpm	
kernel-headers-2.6.32-642.11.1.el6.x86_64.rpm	
ksh-20120801-33.el6_8.sjis.1.x86_64.rpm	

Note To verify that all of the required RHEL 6.5 RPM packages are installed, enter the following command as the root user:

rpm -q cloog-ppl compat-libcap1 compat-libstdc++-33 cpp gcc gcc-c++ glibc glibc-devel glibc-headers kernel-headers ksh libaio-devel libgcc libstdc++-devel libX11 libXau libxcb libXext libXi libXtst mpfr nss-softokn-freebl ppl --qf '%{name}.%{arch}\n'|sort

Table 9: RHEL 6.7, 6.8, 6.9RPM Packages

cpp-4.4.7-17.el6.x86_64.rpm	libgcc-4.4.7-17.el6.i686.rpm
gcc-4.4.7-17.el6.x86_64.rpm	libgcc-4.4.7-17.el6.x86_64.rpm
gcc-c++-4.4.7-17.el6.x86_64.rpm	libgomp-4.4.7-17.el6.i686.rpm
glibc-2.12-1.192.el6.i686.rpm	libgomp-4.4.7-17.el6.x86_64.rpm
glibc-2.12-1.192.el6.x86_64.rpm	libstdc++-4.4.7-17.el6.i686.rpm
glibc-common-2.12-1.192.el6.x86_64.rpm	libstdc++-4.4.7-17.el6.x86_64.rpm
glibc-devel-2.12-1.192.el6.i686.rpm	libXtst-1.2.2-2.1.el6.x86_64.rpm
glibc-devel-2.12-1.192.el6.x86_64.rpm	libstdc++-devel-4.4.7-17.el6.x86_64.rpm
glibc-headers-2.12-1.192.el6.x86_64.rpm	libX11-1.6.3-2.el6.i686.rpm
gmp-4.3.1-10.el6.i686.rpm	libX11-1.6.3-2.el6.x86_64.rpm
kernel-headers-2.6.32-642.11.1.el6.x86_64.rpm	libX11-common-1.6.3-2.el6.noarch.rpm
Note If upgrade fails on RHEL 6.7 ensure to upgrade to RHEL 6.9.	
libX11-1.6.4-3.el6.x86_64	libXft-2.3.2-1.el6.x86_64
libXtst-1.2.3-1.el6.x86_64	pixman-0.32.8-1.el6.x86_64
audit-libs-2.4.5-6.el6.i686	pixman-0.32.8-1.el6.i686
libXi-1.7.8-1.el6.i686	libxcb-1.12-4.el6.x86_64
libXext-1.3.3-1.el6.x86_64	libXrandr-1.5.1-1.el6.i686
libXi-1.7.8-1.el6.x86_64	libXrender-0.9.10-1.el6.x86_64

libXfixes-5.0.3-1.el6.x86_64	audit-libs-2.4.5-6.el6.x86_64
elfutils-libs-0.164-2.el6.x86_64	libXrender-0.9.10-1.el6.i686
libXfixes-5.0.3-1.el6.i686	libX11-1.6.4-3.el6.i686
libXext-1.3.3-1.el6.i686	libxcb-1.12-4.el6.i686
libXtst-1.2.3-1.el6.i686	libXft-2.3.2-1.el6.i686
elfutils-0.164-2.el6.x86_64	libXrandr-1.5.1-1.el6.x86_64

Database Memory

Installation Phase

For the installation phase, the database memory requirements are:

- Swap space: 150 MB
- RAM: At least 4 GB

Runtime Phase

For the runtime phase, the database swap space requirement is two times the size of RAM, up to 32 GB.

Ports and Files

The following ports and files are required:

- Port 1108 must be available for SSH communication between the Prime Central owner and the database owner. The port must also be open on the embedded database server, if it is installed separately.
- The `/etc/hosts` file must include the workstation's local hostname and IP address.

  Example of a correct entry in the `/etc/hosts` file:

  ```
  127.0.0.1 localhost.localdomain localhost
  ::1    localhost6.localdomain6 localhost6
  IP-address myserver.domain.com myserver
  ```

  Example of an incorrect entry in the `/etc/hosts` file (without the server IP address information):

  ```
  127.0.0.1 localhost.localdomain localhost
  ::1    localhost6.localdomain6 localhost6
  ```

- The **hostname --fqdn** command must return the hostname with the fully qualified domain name. For example:

  ```
  sh-nv210-266.cisco.com
  ```

- The **hostname** command should return the non-fqdn hostname. For example:

  ```
  sh-nv210-266
  ```

If the output is not displayed as above, hostname can be configured either through `/etc/sysconfig/network` or through a CLI command:

- Edit file `/etc/sysconfig/network` to add hostname details and then reboot the VM to make the changes permanent.
- Use the command **hostname <name>** to make temporary changes.

- The `/etc/nsswitch.conf` file must not have NIS or NIS+ for password, group, shadow, or services. For example:

```
passwd: files
shadow: files
group: files
services: files
```

Dual-Server Installation

If you are installing the embedded database and Prime Central on separate servers, note the following additional prerequisites for the remote server:

- Perl 5.8.6 or later must be installed on the root user.
- The following ports must be available:
  - 22 (the default SSH port)
  - 1108 (for SSH communication between the Prime Central owner and the database owner)
  - 1521

The installation script copies the Oracle installation files to the remote server under the home directory of the user connecting to the workstation via SSH. The home directory must have at least 4 GB of space available for the installation files. This is especially important if the home directory is root (/), because overconsumption might cause the server to crash.

Security

Prime Central connects to the database using an Oracle encryption feature. By default, connections between Prime Central and the embedded database are encrypted.

Prime Central image bundled with JRE does not support Address Space Layout Randomization (ASLR) or stack protection and hence the system is vulnerable to buffer overflow attacks.

The REST/HTTP Interface is designed to be only accessed inside a controlled environment without any reachability from untrusted end points or over untrusted networks. If it must be accessed across unsecured networks, then customers need to put in additional security mechanisms.

As Prime Central uses Oracle database, it is recommended to periodically check Oracle website (https://support.oracle.com) for any critical patch update that needs be installed to address any security alerts.

If you are using any of the OpenSSL versions, it is recommended to periodically check for the latest patches or upgraded versions using the advisories in order to fix security vulnerabilities.

Prime Central Client Browser Requirements

The following table lists the client browsers and the Citrix XenApp deployment that Prime Central 2.1supports. You must enable cookies and caching in your browser. Mozilla Firefox is the recommended browser.

Table 10: Supported Client Browsers

Certified Citrix Setup	Operating System	Mozilla Firefox Version	Microsoft Internet Explorer Version
Citrix Presentation Server 4.5 XenApp 5.0, installed on a Windows 2003 (SP2) server	Windows 7, 10 (32 and 64 bit)	Firefox 48 and 49 standard edition	Internet Explorer 10 and 11
		Firefox 52 (32 bit) Extended Support Release (ESR)	Internet Explorer 10 and 11

Supported Client JRE Versions

The following table lists the client JRE Versions that Prime Central 2.1supports.

Table 11: Supported JRE Platforms

Platform	Prime Central
JRE 1.8 update 121 JRE 1.8 update 161	Yes

Note AGORA EMS supports JRE 1.6. So, for cross-launching from Prime Central , you need to install JRE 1.6 in the client windows machine.

Component Version Requirements

You can install a suite component in standalone mode or with Prime Central. If you want to install it with Prime Central, your suite component must be the version listed in the Cisco Prime Central 2.1 Release Notes

Prime Central 2.1 Image (Electronic Copy) Signature Verification

Before installing electronic copy of signed Cisco Prime Central image (not USB), you need to verify the signature of an image file. Follow the below procedure to verify the same:

SUMMARY STEPS

1. If you do not have openssl (supported version 0.9.8e or later) installed, download and install it. See http://www.openssl.org
2. If you do not have python (supported python version is 2.7.4 or later) installed, download and install it. See https://www.python.org/
3. Place the following files in a temporary directory after extracting from PrimeCentral21.zip:
4. In the temporary directory, run the following command:
5. If the result is:

DETAILED STEPS

Step 1 If you do not have openssl (supported version 0.9.8e or later) installed, download and install it. See http://www.openssl.org

Step 2 If you do not have python (supported python version is 2.7.4 or later) installed, download and install it. See https://www.python.org/

Step 3 Place the following files in a temporary directory after extracting from PrimeCentral21.zip:

- The product file - PrimeCentral21.zip
- The signature file - PrimeCentral21.img.signaturethat is packaged with the product file
- The certificate file - PRIMECENTRAL20.cer PRIMECENTRAL.21.cer
- The verification file - IS_verify_bulkhash.pyc

Step 4 In the temporary directory, run the following command:

python IS_verify_bulkhash.pyc -e PRIMECENTRAL20.cer -i PrimeCentral20.img –s PrimeCentral153.img.signature -v dgst -sha512

Step 5 If the result is:

Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...

Successfully downloaded and verified crcam2.cer.

Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...

Successfully downloaded and verified innerspace.cer.

Successfully verified root, subca and end-entity certificate chain.

Successfully verified the signature of PrimeCentral21.img using PRIMECENTRAL.21.cer

The image is successfully verified.

Note Do not proceed further if image verification fails. This indicates that the image is not signed/ the file is not from Cisco Systems, or it has been tampered. Kindly contact your Cisco representative for further assistance.

Extracting the Image Prime Central 2.1

Step 1 Insert Cisco Prime Central installation USB into your Linux machine.

If you have Cisco Prime Central installation .img image (instead of USB), enter the following commands to mount it:

mkdir /mnt

mount -o loop PrimeCentral21.img /mnt

Step 2 Go to ISO 2.1directory by entering the below command:

cd/mnt/ISO2.1

Step 3 Go to the required iso directory based on the installation requirement, according to the below table:

Directory	Contents
Base Application	Contains **.iso** for Prime Central Base Application and Oracle binaries
Disaster Recovery	Contains **.iso** for Disaster Recovery
Fault Management	Contains **.iso** for Fault Management
Gateways	Contains **.iso** for IBM tier1 and tier2 gateways
High Availability	Contains **.iso** images for High Availability

Step 4 Enter the following command to mount the required iso image:

mkdir <mounting directory>

mount -o loop <required .iso> <mounting directory>

Note It is recommended to copy the installation binaries from <mounting directory> to a new directory, and continue installation from this new directory, to avoid loss of file if unmounted.

Step 5 Continue to the relevant installation section:

- Installing Prime Central
- Installing Prime Central Fault Management
- Installing the Gateways Used with Prime Central

Installing Prime Central

- Database—Can be installed as an external or an embedded Oracle database version 12.1.0.2.

- Prime Central portal—Provides a single sign-on and a multi-tenant common administrative interface for all applications within the suite.
- Prime Central integration layer (IL)—Performs back-end mediation and enables information exchange between the various components
- Fault Management—Locates, diagnoses, and reports network problems.

Installing Prime Central in a Single-Server Setup

Installing the database, Prime Central portal, and Prime Central integration layer on the same server is a two-part process:

1. Prepare the server for installation.
2. Install Prime Central.

Note During the installation, the variables that you define must adhere to the constraints described in Pathname, Group Name, Username, and Password Constraints.

Preparing the Server for Installation

Before you install Prime Central, you must first connect to the server and, if using X server, verify the display settings.

To prepare the server for Prime Central installation:

Step 1 Use one of the following options to connect to the server where you want to install Prime Central:

- VNC (recommended)—See http://www.realvnc.com.
- X server—For this option, Reflection X is recommended. See http://www.attachmate.com/products/reflection/x/.

Step 2 As the root user, launch a terminal on the server where you want to install Prime Central. (If you logged in as a nonroot user, use su - to become the root user.) The C shell (csh) is recommended, but you can also use the Bash shell.

- To start the C shell, enter: **/bin/csh**
- To start the Bash shell, enter: **/bin/bash**

If you are using X server, continue to Step 3.

If you are using VNC, skip to Step 5.

Step 3 Set the DISPLAY variable:

setenv DISPLAY *hostname-or-IP-address***:0.0**

Step 4 Verify that the display is set correctly:

echo $DISPLAY

In the command output, you should see:

hostname-or-IP-address:0.0

Step 5 Set the ulimit value.

If using a C shell, enter: **limit descriptors 1048576**

In the command output, you should see:

```
# limit descriptors
descriptors  1048576
```

If using a Bash shell, enter: **ulimit -n 1048576**

In the command output, you should see:

```
# ulimit -n
1048576
```

Step 6 (For an external database only; not applicable to an embedded database) If you are using a local or remote external database,

download prePCInstallForExt12c.sh from the scripts folder in the Base Application folder (where images/primecentral_v.bin is located) 2.0.bin is located). Copy prePCInstallForExt12c.sh to ORACLE_HOME/network/admin and execute.

Step 7 Verify that the following Red Hat RPM packages are installed
To verify the RHEL 5 RPM packages, enter:

```
rpm -q compat-db compat-glibc compat-glibc-headers compat-libstdc++-296 compat-libstdc++-33 elfutils
 elfutils-libs gtk2 gtk2-engines kernel-headers ksh libgcc libXft libXmu libXp libXpm libXtst
openmotif22 pam --qf "%{name}/%{version}/%{release}/%{arch}\n"
```

To verify the RHEL 6 RPM packages, enter:

```
rpm -q cloog-ppl compat-db compat-glibc compat-libcap1 compat-libstdc++-296 compat-libstdc++-33 cpp
 elfutils elfutils-libs expect gcc gcc-c++ glibc glibc-common glibc-devel glibc-headers gmp gtk2
gtk2-engines kernel-headers ksh libaio-devel libgcc libgomp libstdc++ libstdc++-devel libX11
libX11-common libXau libxcb libXext libXft libXi libXmu libXp libXpm libXtst mpfr nscd
nss-softokn-freebl openmotif22 pam ppl rpm-build sshpass tcl tzdata --qf
"%{name}/%{version}/%{release}/%{arch}\n"
```

Installing Prime Central on the Server

Step 1 Insert the Cisco Prime Central 2.1USB drive into the USB port and navigate to the Base Application folder, which contains the following files:

- linuxamd64_12102_database_1of2.zip
- linuxamd64_12102_database_2of2.zip
- primecentral_v 2.1.bin.

Step 2 Use SSH to connect to the server.

Step 3 Copy the 3 files listed in Step 1 to the server.

Step 4 Change file permissions and ownership:

chmod 755 *

Step 5 Run the installer:

./primecentral_v2.1.bin

Step 6 In the **Welcome** window, click **Next**.

Tip You can also press the Tab key + space bar to activate the Next (or Previous) button.

Step 7 In the **License Agreement** window, read the license agreement, click the **I accept the terms of the License Agreement** radio button, and click **Next**.

Step 8 In the **Install Type** window, click the **Single-Server Install** radio button; then, click **Next**.

Step 9 In the **Validating Environment** window, review the information for accuracy; then, click **Next**.

Step 10 In the **Server Information** window, confirm that the fully qualified domain name (FQDN) of the local server is correct; if not, enter the correct FQDN. (Be sure to use the hostname of the server where Prime Central will be mounted.) Then, click **Next**.

Step 11 In the **Choose Install Folder** window, specify where to install Prime Central. Then, click **Next**.

The "o" (other or world) UNIX users must have at least execute permissions on the installation directory path.

Step 12 In the **OS User Information** window, provide the information required to create an OS user to start and stop processes. The username is primeusr and cannot be changed. Then, click **Next**.

Step 13 In the **Admin User Information** window, enter the password for the admin user who will be used for the first system login. The username is centraladmin and cannot be changed. Then, click **Next**.

Step 14 In the **Install Mode** window, specify one of the following installation modes:

- **Simple Install**—Click **Next**; then, continue to the next step.
- **Advanced Install**—Click **Next**; in the **Advanced Configuration** window, enter the desired port numbers and configuration values for the third-party servers; then, click **Next**.

Step 15 In the **Validating Port Configuration** window, review the information for accuracy; then, click **Next**.

Step 16 In the **Database Type** window, specify one of the following database types; then, click **Next**:

Embedded Database:

a) In the **Embedded DB Information** window, enter the required information for your local or remote embedded database; then, click **Next**.
b) In the **Prime Central DB User Information** window, enter the password for the database user that will be created for Prime Central. The username is primedba and cannot be changed. Then, click **Next**.

Note Be sure to note down the database user password for future reference. For example, if you decide to register an application with Prime Central, you will need this password.

External Database:

a) In the **Database Information** window, enter the required information for your preinstalled local or remote external database; then, click **Next**.
b) In the **Prime Central DB User Information** window, enter the password for the database user that will be created for Prime Central. The username is primedba and cannot be changed. Then, click **Next**.
c) In the **Database File Directory** window, specify where to store database data files; then, click **Next**. The directory you choose must exist, must be owned by the oracle user, and must not contain any data files. For a remote server, the Oracle database file directory must be present on the remote server where Oracle is installed.

For example, the database file directory /dbdata owned by the oracle user is as follows:

```
drwxr-xr-x   2 oracle   oinstall     512 Dec  8 14:04 dbdata
```

d) In the **DB Server Information** window, enter the home directory for the Oracle database. Then, click **Next**.

Step 17 Verify that the information in the **Pre-Installation Summary** window is correct; then, click **Install**.

It might take 30 minutes or longer to install Prime Central, depending on your system performance and whether you are using an embedded or external database.

Step 18 In the **Install Complete** window, click **Done**.

If the installation fails, see Troubleshooting the Installation, and make sure to uninstall Prime Central before attempting new installation. For more information, see Uninstalling Prime Central.

Explanation of Fields in the Embedded DB Information Window

The following table describes the required information for your local or remote embedded database.

Table 12: Fields in the Embedded DB Information Window

Field	Description
Oracle User	The default username is *oracle*.
Oracle Home Directory	The installer creates /export/home/oracle by default. If you want to use a different directory, choose one that is not already present on the server.
Data Files Location	The default is /export/home/oracle/oradata/primedb.
Redo Files Location	The default is /export/home/oracle/redo.
Enable backups on the database	Check this optional check box to enable backups on the Oracle database.
Archive Log Location	(Required if "Enable backups on the database" is checked) The default is /export/home/oracle/arch.
Backup Destination	(Required if "Enable backups on the database" is checked) The default is /export/home/oracle/backup.
Install database on remote server	Check this optional check box to install the embedded database on a remote server. The SSH user and password are used to establish an SSH connection between Prime Central and the remote database server.
Remote SSH User	(Required if "Install database on remote server" is checked) The remote SSH user's home directory cannot be the / directory.
Remote SSH User Password	(Required if "Install database on remote server" is checked) Enter the password for the remote SSH user. The password cannot contain a percent sign (%).
Server IP Address	Enter the IP address of the server where the database will be installed.
Root Password	Enter the root password for the server where the database will be installed. The password cannot contain following special characters (%, ^, $, *).

Installing Prime Central in a Dual-Server Setup

Installing the Prime Central portal and Prime Central integration layer on separate servers—called a *distributed* or *dual-server* installation—is a three-part process:

1. Prepare both servers for installation.
2. Install the Prime Central portal.
3. Install the Prime Central integration layer.

Note You must install the Prime Central portal before installing the Prime Central integration layer. During the installation, the variables that you define must adhere to the constraints described in Pathname, Group Name, Username, and Password Constraints.

Preparing Both Servers for Installation

Before you install the Prime Central portal and the Prime Central integration layer on separate servers, you must first connect to each server and, if using X server, verify the display settings.

Do the following on both servers:

Step 1 Use one of the following options to connect to the server:

- VNC (recommended)—See http://www.realvnc.com.
- X server—For this option, Reflection X is recommended. See http://www.attachmate.com/Products/PC+X+Server/rx/.

Step 2 As the root user, launch a terminal on the server. (If you logged in as a nonroot user, enter the **su -** command to become the root user.) The C shell (csh) is recommended, but you can also use the Bash shell.

- To start the C shell, enter: **/bin/csh**
- To start the Bash shell, enter: **/bin/bash**

If you are using X server, continue to Step 3.

If you are using VNC, skip to Step 5.

Step 3 Set the DISPLAY variable:

setenv DISPLAY *hostname-or-IP-address*:**0.0**

Step 4 Verify that the display is set correctly:

echo $DISPLAY

In the command output, you should see:

hostname-or-IP-address:0.0

Step 5 Set the ulimit value.

If using a C shell, enter: **limit descriptors 1048576**

In the command output, you should see:

```
# limit descriptors
descriptors  1048576
```

If using a Bash shell, enter: **ulimit -n 1048576**

In the command output, you should see:

```
# ulimit -n
1048576
```

Step 6 (For an external database only; not applicable to an embedded database) If you are using a local or remote external database,

download prePCInstallForExt12c.sh from the scripts folder in the Base Application folder (where images/primecentral_v2.0.bin is located) Copy prePCInstallForExt12c.sh to ORACLE_HOME/network/admin and execute.

Step 7 Verify that the following Red Hat RPM packages are installed
To verify the RHEL 5 RPM packages, enter:

```
rpm -q compat-db compat-glibc compat-glibc-headers compat-libstdc++-296 compat-libstdc++-33 elfutils
 elfutils-libs gtk2 gtk2-engines kernel-headers ksh libgcc libXft libXmu libXp libXpm libXtst nscd
openmotif22 pam --qf "%{name}/%{version}/%{release}/%{arch}\n"
```

To verify the RHEL 6 RPM packages, enter:

```
rpm -q cloog-ppl compat-db compat-glibc compat-libcap1 compat-libstdc++-296 compat-libstdc++-33 cpp
 elfutils elfutils-libs expect gcc gcc-c++ glibc glibc-common glibc-devel glibc-headers gmp gtk2
gtk2-engines kernel-headers ksh libaio-devel libgcc libgomp libstdc++ libstdc++-devel libX11
libX11-common libXau libxcb libXext libXft libXi libXmu libXp libXpm libXtst mpfr nscd
nss-softokn-freebl openmotif22 pam ppl rpm-build sshpass tcl tzdata --qf
"%{name}/%{version}/%{release}/%{arch}\n"
```

Installing the Prime Central Portal

Step 1 Insert the Cisco Prime Central 2.1USB drive into the USB port and navigate to the Base Application folder.

Step 2 Change file permissions and ownership:

chmod 755 *

Step 3 From the Base Application folder, run the installer:

./primecentral_v2.1.bin

Step 4 In the **Welcome** window, click **Next**.

Step 5 In the **License Agreement** window, read the license agreement, click the **I accept the terms of the License Agreement** radio button, and click **Next**.

Step 6 In the **Install Type** window, click the **Distributed Install** radio button; then, click **Next**.

Step 7 In the **Distributed Install Components** window, click the **Portal** radio button; then, click **Next**.

Step 8 In the **Validating Environment** window, review the information for accuracy; then, click **Next**.

Step 9 In the **Server Information** window, confirm that the FQDN of the local server is correct; if not, enter the correct FQDN. Then, click **Next**.

Step 10 In the **Choose Install Folder** window, specify where to install the Prime Central portal. Then, click **Next**.

The "o" (other or world) UNIX users must have at least execute permissions on the installation directory path.

Step 11 In the **OS User Information** window, provide the information required to create an OS user to start and stop processes. The username is primeusr and cannot be changed. Then, click **Next**.

Step 12 In the **Admin User Information** window, enter the password for the admin user who will be used for the first system login. The username is centraladmin and cannot be changed. Then, click **Next**.

Step 13 In the **Install Mode** window, specify one of the following installation modes:

- **Simple Install**—Click **Next**; then, continue to the next step.
- **Advanced Install**—Click **Next**; in the **Advanced Configuration** window, enter the desired port numbers and configuration values for the third-party servers; then, click **Next**.

Step 14 In the **Validating Port Configuration** window, review the information for accuracy; then, click **Next**.

Step 15 In the **Database Type** window, specify one of the following database types; then, click **Next**:

Embedded Database:

a) In the **Embedded DB Information** window, enter the required information for your local or remote embedded database; then, click **Next**.
b) In the **Prime Central DB User Information** window, enter the password for the database user that will be created for Prime Central. The username is primedba and cannot be changed. Then, click **Next**.

Note Be sure to note down the database user password for future reference. For example, if you decide to register a domain manager with Prime Central, you will need this password.

External Database:

a) In the **Database Information** window, enter the required information for your preinstalled local or remote external database; then, click **Next**.
b) In the **Prime Central DB User Information** window, enter the password for the database user that will be created for Prime Central. The username is primedba and cannot be changed. Then, click **Next**.
c) In the **Database File Directory** window, specify where to store database data files; then, click **Next**. The directory you choose must exist, must be owned by the oracle user, and must not contain any data files. For a remote server, the Oracle database file directory must be present on the remote server where Oracle is installed.

   For example, the database file directory /dbdata owned by the oracle user is as follows:

```
drwxr-xr-x   2 oracle   oinstall     512 Dec  8 14:04 dbdata
```

d) In the **DB Server Information** window, enter the home directory for the Oracle database. Then, click **Next**.

Step 16 Verify that the information in the **Pre-Installation Summary** window is correct; then, click **Install**.

It might take 30 minutes or longer to install Prime Central, depending on your system performance and whether you are using an embedded or external database.

Step 17 In the **Install Complete** window, click **Done**.

If the installation fails, see Troubleshooting the Installation, and make sure to uninstall Prime Central before attempting new installation. For more information, see Uninstalling Prime Central.

Installing the Prime Central Integration Layer

Step 1 Insert the Cisco Prime Central 2.1 USB drive into the USB port and navigate to the Base Application folder.

Step 2 Change file permissions and ownership:

chmod 755 *

Step 3 From the Base Application folder, run the installer:

./primecentral_v2.1.bin

Step 4 In the **Welcome** window, click **Next**.

Step 5 In the **License Agreement** window, read the license agreement, click the **I accept the terms of the License Agreement** radio button, and click **Next**.

Step 6 In the **Install Type** window, click the **Distributed Install** radio button; then, click **Next**.

Step 7 In the **Distributed Install Components** window, click the **Integration Layer** radio button; then, click **Next**.

Step 8 In the **Validating Environment** window, review the information for accuracy; then, click **Next**.

Step 9 In the **Database Information** window, enter the following Prime Central database connection information; then, click **Next**:

- Server IP address or hostname.
- Port—The default is 1521.
- SID—The default is primedb.
- Prime database user—The username is primedba and cannot be changed.
- Prime database password.

Step 10 To scale the integration layer to support multiple application instances and provide the option of high availability, Prime Central 2.0uses a distributed integration layer architecture. In the **Integration Layer Profile** window, specify one or both of the following integration layer profiles:

- **Prime Central integration layer: Messaging**—Installs a separate JMS broker to enable the integration layer messaging framework to be configured as a JMS cluster for messaging service high availability. Click **Next**; in the confirmation popup window, click one of the following:
  - **Yes**—To change the connection transport type, request timeout, or reconnect delay. In the **Integration Layer-JMS Data** window, make the desired changes; then, click **Next**.
  - **No**—To use the default values for connection transport type, request timeout, and reconnect delay. Then, continue to the next step.
- **Prime Central integration layer: Core**—Installs the integration layer core components. Click **Next**; then, continue to the next step.

Step 11 In the **Server Information** window, confirm that the FQDN is correct; if not, enter the correct FQDN. Then, click **Next**.

Step 12 In the **Choose Install Folder** window, specify where to install the Prime Central integration layer. Then, click **Next**.

The "o" (other or world) UNIX users must have at least execute permissions on the installation directory path.

Step 13 In the **OS User Information** window, provide the information required to create an OS user to start and stop processes. The username is primeusr and cannot be changed. Then, click **Next**.

Step 14 In the **Install Mode** window, specify one of the following installation modes:

- **Simple Install**—Click **Next**; then, continue to the next step.
- **Advanced Install**—Click **Next**; in the **Advanced Configuration** window, enter the desired port numbers and configuration values for the third-party servers; then, click **Next**.

Step 15 In the **Validating Port Configuration** window, review the information for accuracy; then, click **Next**.

Step 16 Verify that the information in the **Pre-Installation Summary** window is correct; then, click **Install**.

It might take 10 minutes or longer to install the Prime Central integration layer, depending on your system performance and whether you are using an embedded or external database.

Step 17 In the **Install Complete** window, click **Done**.

If the installation fails, see Troubleshooting the Installation, on page 54, and make sure to uninstall Prime Central before attempting new installation. For more information, see Uninstalling Prime Central.

Pathname, Group Name, Username, and Password Constraints

During the Prime Central installation, the variables that you define must adhere to the constraints listed in the following table.

Table 13: Pathname, Group Name, Username, and Password Constraints

Variable	Constraints
Choose Install Folder Window	
Installation directory pathname	The installation directory pathname cannot: • Exceed 100 characters. • Contain non-ASCII characters. • Contain special shell characters (; & ( ) | < > ' " ` $ *). • Contain whitespace characters (<newline>, <space>, <tab>).
User Information Windows (OS User, Admin User, Prime Central Database User, Fault Management Application User)	
OS user group name	The OS user group name must: • Contain from 1 to 8 alphanumeric characters. • Begin with a letter (a-z, A-Z). • Contain at least one lowercase letter (a-z). • Not contain any special characters except hyphen (-) or underscore (_).

Variable	Constraints
Fault management application username	The Fault Management application username must: • Contain from 1 to 8 alphanumeric characters. • Begin with a letter (a-z, A-Z). • Contain at least one lowercase letter (a-z). • Not contain any special characters except hyphen (-) or underscore (_).

All user passwords	Except where noted, the following constraints apply to all user passwords:
	• Character count:
	  • Prime Central database user passwords only—8 to 12 characters.
	  • All other user passwords—8 to 32 characters.
	• Alphanumeric characters:
	  • At least one uppercase letter (A-Z).
	  • At least one lowercase letter (a-z).
	  • At least one number (0-9).
	  • No character repeated three or more times.
	  • Does not contain the username or the username in reverse.
	  • Does not contain cisco, ocsic, or any variation.
	• Special characters:
	  • All user passwords—At least one special character from the following:
	  ~ @ # % ^ * ( ) _ - + = | { [}] : ; < , > . /
	  No other special characters are allowed.
	  • Prime Central database user only—At least one special character is required, but the password cannot *begin* with a special character.

Verifying the Prime Central Installation

Step 1 As the primeusr, log in to the Linux server with the primeusr password that you specified during the installation.

Step 2 Verify that the Prime Central portal is running:

portalctl status

In the output, you should see:

```
Prime Central Platform Status
Started
```

Step 3 Open a web browser and log in to the Prime Central portal at **https://***server-hostname***:***https-port-number*, where:

- *server-hostname* is the hostname of the newly installed Prime Central server.
- *https-port-number* is the SSL port number that was configured during installation.

Step 4 Enter the username **`centraladmin`** and the admin user password that you specified during the installation.

Checking the Prime Central Version

Step 1 As the primeusr, log in to the Prime Central server.

Step 2 On the command line, enter the **version**.

The following is an example of the output of the **version** command:

```
# version
Running Integration Layer(PC-IL-CORE,PC-IL-JMS) + Platform (v

 2.1(build number)) with Patch(0.0.0.0)
```

Note If you reinstall a new build on an existing server, or if you install or uninstall applications, be sure to open a new browser window with a clear cache.

Installing Prime Central Silently

You can install Prime Central without user interaction. In a silent installation, no messages or prompts appear on-screen, and interactive dialogs are not displayed. Information and answers that you would normally provide are read from a properties file.

A silent installation allows for unattended product installations based on the values that are provided in the silent installation properties file.

Step 1 As the root user, launch a terminal on the server where you want to silently install Prime Central. (If you logged in as a nonroot user, enter the **su -** command to become the root user.) The C shell (csh) is recommended. To start the C shell, enter:

/bin/csh

Step 2 Insert the Cisco Prime Central 2.1 USB drive into the USB port and navigate to the local folder where the drive is mounted.

Step 3 Create an install.properties file based on the samples provided in Sample install.properties Files. Depending on the input that you provide, Prime Central will be installed in either a single-server setup or a dual-server (distributed) setup.

Caution Be careful to enter correct values in the install.properties file. The silent installation does not perform any validation on the values you enter.

Step 4 Save your changes to the install.properties file.

Step 5 Change file permissions:

chmod 755 *

Step 6 Run the installer:

./primecentral_2.1.bin -i silent -f install.properties

The silent installation log files are available in the *installation-directory*/install/logs/ and in /tmp folder.

Note If the installation fails, see Troubleshooting the Installation, on page 54, and make sure to uninstall Prime Central before attempting new installation. For more information, see Uninstalling Prime Central.

It is mandatory to verify the log files for any errors before proceeding further.

Sample install.properties Files

The following examples show a typical install.properties file for each of the following scenarios:

- Example 1: Installing Prime Central in a Single-Server Setup with a Local Embedded Database
- Example 2: Installing Prime Central in a Single-Server Setup with a Remote Embedded Database
- Example 3: Installing Prime Central in a Single-Server Setup with an External Database
- Example 4: Installing the Prime Central Portal in a Dual-Server Setup with a Local Embedded Database
- Example 5: Installing the Prime Central Portal in a Dual-Server Setup with a Remote Embedded Database
- Example 6: Installing the Prime Central Portal in a Dual-Server Setup with an External Database
- Example 7: Installing the Prime Central Integration Layer in a Dual-Server Setup

Caution The values shown in the following examples are for illustrative purposes only. Be careful to enter actual values that are appropriate for your operating environment.

Example 1: Installing Prime Central in a Single-Server Setup with a Local Embedded Database

```
Installer_UI=silent

########## Basic ##########

USER_INSTALL_DIR=/opt/primecentral
SUITEFW_INSTALL_TYPE=Single-Server Install
SUITEFW_DISTRIBUTED_INSTALL_TYPE=
SUITEFW_BOTH_SERVER_HOSTNAME=prime-dev.cisco.com

########## OS User (primeusr is fixed, do not change it) ##########

SUITEFW_OS_USER=primeusr
SUITEFW_OS_GROUP=primegrp
SUITEFW_OS_PASSWD=Admin123~
SUITEFW_OS_TYPE=Linux

########## Application Admin user (centraladmin) password ###
```

```
SUITEFW_ADMIN_USER_PASSWD=Admin123~

########## DATABASE ##########

SUITEFW_DB_TYPE=Embedded Database

### Database User (primedba is fixed. do not change it) ###

SUITEFW_DB_USER=primedba
SUITEFW_DB_USER_PASSWD=Admin123~

### External Database

SUITEFW_DB_HOST_IP_ADDRESS=
SUITEFW_DB_SYSTEM_PASSWD=
SUITEFW_DB_SYSTEM_USER=system
SUITEFW_DB_PORT=1521
SUITEFW_DB_SID=
SUITEFW_DBF_FILES_DIR=

### Embedded Database

SUITEFW_EMBEDDED_REMOTE=0
SUITEFW_EMBEDDED_ROOT_PASSWD=poPPee
SUITEFW_EMBEDDED_HOST_IP=209.165.201.30
SUITEFW_EMBEDDED_DBPROFILE=2
SUITEFW_EMBEDDED_SMTP=self
SUITEFW_EMBEDDED_SSH_USER=
SUITEFW_EMBEDDED_SSH_USER_PASSWORD=
SUITEFW_EMBEDDED_ORACLE_HOME=/export/home/oracle
SUITEFW_EMBEDDED_ORACLE_USER=oracle
SUITEFW_EMBEDDED_DATAFILES=/export/home/oracle/oradata/primedb
SUITEFW_EMBEDDED_REDO=/export/home/oracle/redo
SUITEFW_EMBEDDED_BACKUP=1
SUITEFW_EMBEDDED_ARCHIVE=/export/home/oracle/arch
SUITEFW_EMBEDDED_BACKUP_DEST=/export/home/oracle/backup

##########  Install Mode ##########

SUITEFW_BOTH_INSTALL_MODE=Simple Install

### Portal

SUITEFW_PORTAL_HTTPS_PORT=8443
SUITEFW_PORTAL_HTTP_PORT=8080
SUITEFW_PORTAL_AJP_PORT=8009
SUITEFW_PORTAL_SHUTDOWN_PORT=8005

### IL

SUITEFW_IL_MTOSI_PORT=9110
SUITEFW_IL_CONNECTION_TRANSPORTTYPE=nio
SUITEFW_IL_CONNECTION_PORT=61616
SUITEFW_IL_NIO_TRANSPORT_PORT=61616
SUITEFW_IL_SSL_TRANSPORT_PORT=61615
SUITEFW_IL_NIO_TRANSPORT_FAILOVER_PORT=61614
SUITEFW_IL_REQUEST_TIMEOUT=135000
SUITEFW_IL_3GPP_PORT=9220
SUITEFW_IL_ALARM_MGMT_PORT=9020
SUITEFW_IL_RECONNECT_DELAY=10

### IL Profiles
# needed for distributed - IL
```

```
#SUITEFW_IL_PROFILES=PC-IL-JMS PC-IL-CORE

#### RPM VERIFICATION ######
SUITEFW_OVERRIDE_RPM_STATUS=
```

Example 2: Installing Prime Central in a Single-Server Setup with a Remote Embedded Database

```
Installer_UI=silent

########## Basic ##########

USER_INSTALL_DIR=/opt/primecentral
SUITEFW_INSTALL_TYPE=Single-Server Install
SUITEFW_DISTRIBUTED_INSTALL_TYPE=
SUITEFW_BOTH_SERVER_HOSTNAME=prime-dev.cisco.com

########## OS User (primeusr is fixed, do not change it) ##########

SUITEFW_OS_USER=primeusr
SUITEFW_OS_GROUP=primegrp
SUITEFW_OS_PASSWD=Admin123~
SUITEFW_OS_TYPE=Linux

########## Application Admin user (centraladmin) password ###

SUITEFW_ADMIN_USER_PASSWD=Admin123~

########## DATABASE ##########

SUITEFW_DB_TYPE=Embedded Database

### Database User (primedba is fixed. do not change it) ###

SUITEFW_DB_USER=primedba
SUITEFW_DB_USER_PASSWD=Admin123~

### External Database

SUITEFW_DB_HOST_IP_ADDRESS=
SUITEFW_DB_SYSTEM_PASSWD=
SUITEFW_DB_SYSTEM_USER=system
SUITEFW_DB_PORT=1521
SUITEFW_DB_SID=
SUITEFW_DBF_FILES_DIR=

### Embedded Database

SUITEFW_EMBEDDED_REMOTE=1
SUITEFW_EMBEDDED_ROOT_PASSWD=poPPee123
SUITEFW_EMBEDDED_HOST_IP=209.165.200.254
SUITEFW_EMBEDDED_DBPROFILE=2
SUITEFW_EMBEDDED_SMTP=self
SUITEFW_EMBEDDED_SSH_USER=test
SUITEFW_EMBEDDED_SSH_USER_PASSWORD=Admin123~
SUITEFW_EMBEDDED_ORACLE_HOME=/export/home/oracle
SUITEFW_EMBEDDED_ORACLE_USER=oracle
SUITEFW_EMBEDDED_DATAFILES=/export/home/oracle/oradata/primedb
SUITEFW_EMBEDDED_REDO=/export/home/oracle/redo
SUITEFW_EMBEDDED_BACKUP=1
SUITEFW_EMBEDDED_ARCHIVE=/export/home/oracle/arch
SUITEFW_EMBEDDED_BACKUP_DEST=/export/home/oracle/backup

##########  Install Mode ##########
```

```
SUITEFW_BOTH_INSTALL_MODE=Simple Install

### Portal

SUITEFW_PORTAL_HTTPS_PORT=8443
SUITEFW_PORTAL_HTTP_PORT=8080
SUITEFW_PORTAL_AJP_PORT=8009
SUITEFW_PORTAL_SHUTDOWN_PORT=8005

### IL

SUITEFW_IL_MTOSI_PORT=9110
SUITEFW_IL_CONNECTION_TRANSPORTTYPE=nio
SUITEFW_IL_CONNECTION_PORT=61616
SUITEFW_IL_NIO_TRANSPORT_PORT=61616
SUITEFW_IL_SSL_TRANSPORT_PORT=61615
SUITEFW_IL_NIO_TRANSPORT_FAILOVER_PORT=61614
SUITEFW_IL_REQUEST_TIMEOUT=135000
SUITEFW_IL_3GPP_PORT=9220
SUITEFW_IL_ALARM_MGMT_PORT=9020
SUITEFW_IL_RECONNECT_DELAY=10

### IL Profiles
# needed for distributed - IL
#SUITEFW_IL_PROFILES=PC-IL-JMS PC-IL-CORE

#### RPM VERIFICATION ######
SUITEFW_OVERRIDE_RPM_STATUS=
```

Example 3: Installing Prime Central in a Single-Server Setup with an External Database

```
Installer_UI=silent

########## Basic ##########

USER_INSTALL_DIR=/opt/primecentral
SUITEFW_INSTALL_TYPE=Single-Server Install
SUITEFW_DISTRIBUTED_INSTALL_TYPE=
SUITEFW_BOTH_SERVER_HOSTNAME=prime-dev.cisco.com

########## OS User (primeusr is fixed, do not change it) ##########

SUITEFW_OS_USER=primeusr
SUITEFW_OS_GROUP=primegrp
SUITEFW_OS_PASSWD=Admin123~
SUITEFW_OS_TYPE=Linux

########## Application Admin user (centraladmin) password ###

SUITEFW_ADMIN_USER_PASSWD=Admin123~

########## DATABASE ##########

SUITEFW_DB_TYPE=External Database

### Database User (primedba is fixed. do not change it) ###

SUITEFW_DB_USER=primedba
SUITEFW_DB_USER_PASSWD=Admin123~

### External Database

SUITEFW_DB_HOST_IP_ADDRESS=209.165.200.225
SUITEFW_DB_SYSTEM_PASSWD=manager
```

```
SUITEFW_DB_SYSTEM_USER=system
SUITEFW_DB_PORT=1521
SUITEFW_DB_SID=service-name
SUITEFW_DBF_FILES_DIR=/export/home/oracle/prime_test
SUITEFW_EMBEDDED_ORACLE_HOME=/export/home/oracle

##########  Install Mode ##########

SUITEFW_BOTH_INSTALL_MODE=Simple Install

### Portal

SUITEFW_PORTAL_HTTPS_PORT=8443
SUITEFW_PORTAL_HTTP_PORT=8080
SUITEFW_PORTAL_AJP_PORT=8009
SUITEFW_PORTAL_SHUTDOWN_PORT=8005

### IL

SUITEFW_IL_MTOSI_PORT=9110
SUITEFW_IL_CONNECTION_TRANSPORTTYPE=nio
SUITEFW_IL_CONNECTION_PORT=61616
SUITEFW_IL_NIO_TRANSPORT_PORT=61616
SUITEFW_IL_SSL_TRANSPORT_PORT=61615
SUITEFW_IL_NIO_TRANSPORT_FAILOVER_PORT=61614
SUITEFW_IL_REQUEST_TIMEOUT=135000
SUITEFW_IL_3GPP_PORT=9220
SUITEFW_IL_ALARM_MGMT_PORT=9020
SUITEFW_IL_RECONNECT_DELAY=10

### IL Profiles
# needed for distributed - IL
#SUITEFW_IL_PROFILES=PC-IL-JMS PC-IL-CORE

#### RPM VERIFICATION ######
SUITEFW_OVERRIDE_RPM_STATUS=
```

Example 4: Installing the Prime Central Portal in a Dual-Server Setup with a Local Embedded Database

```
Installer_UI=silent

######### Basic ##########

USER_INSTALL_DIR=/opt/primecentral
SUITEFW_INSTALL_TYPE=Distributed Install
SUITEFW_DISTRIBUTED_INSTALL_TYPE=Portal
SUITEFW_BOTH_SERVER_HOSTNAME=prime-dev.cisco.com

########## OS User (primeusr is fixed, do not change it) ##########

SUITEFW_OS_USER=primeusr
SUITEFW_OS_GROUP=primegrp
SUITEFW_OS_PASSWD=Admin123~
SUITEFW_OS_TYPE=Linux

########## Application Admin user (centraladmin) password ###

SUITEFW_ADMIN_USER_PASSWD=Admin123~

########## DATABASE ##########

SUITEFW_DB_TYPE=Embedded Database

### Database User (primedba is fixed. do not change it) ###
```

```
SUITEFW_DB_USER=primedba
SUITEFW_DB_USER_PASSWD=Admin123~

### External Database

SUITEFW_DB_HOST_IP_ADDRESS=
SUITEFW_DB_SYSTEM_PASSWD=
SUITEFW_DB_SYSTEM_USER=system
SUITEFW_DB_PORT=1521
SUITEFW_DB_SID=
SUITEFW_DBF_FILES_DIR=

### Embedded Database

SUITEFW_EMBEDDED_REMOTE=0
SUITEFW_EMBEDDED_ROOT_PASSWD=poPPee
SUITEFW_EMBEDDED_HOST_IP=209.165.201.30
SUITEFW_EMBEDDED_DBPROFILE=2
SUITEFW_EMBEDDED_SMTP=self
SUITEFW_EMBEDDED_SSH_USER=
SUITEFW_EMBEDDED_SSH_USER_PASSWORD=
SUITEFW_EMBEDDED_ORACLE_HOME=/export/home/oracle
SUITEFW_EMBEDDED_ORACLE_USER=oracle
SUITEFW_EMBEDDED_DATAFILES=/export/home/oracle/oradata/primedb
SUITEFW_EMBEDDED_REDO=/export/home/oracle/redo
SUITEFW_EMBEDDED_BACKUP=1
SUITEFW_EMBEDDED_ARCHIVE=/export/home/oracle/arch
SUITEFW_EMBEDDED_BACKUP_DEST=/export/home/oracle/backup

##########  Install Mode ##########

SUITEFW_BOTH_INSTALL_MODE=Simple Install

### Portal

SUITEFW_PORTAL_HTTPS_PORT=8443
SUITEFW_PORTAL_HTTP_PORT=8080
SUITEFW_PORTAL_AJP_PORT=8009
SUITEFW_PORTAL_SHUTDOWN_PORT=8005

### IL

SUITEFW_IL_MTOSI_PORT=9110
SUITEFW_IL_CONNECTION_TRANSPORTTYPE=nio
SUITEFW_IL_CONNECTION_PORT=61616
SUITEFW_IL_NIO_TRANSPORT_PORT=61616
SUITEFW_IL_SSL_TRANSPORT_PORT=61615
SUITEFW_IL_NIO_TRANSPORT_FAILOVER_PORT=61614
SUITEFW_IL_REQUEST_TIMEOUT=135000
SUITEFW_IL_3GPP_PORT=9220
SUITEFW_IL_ALARM_MGMT_PORT=9020
SUITEFW_IL_RECONNECT_DELAY=10

### IL Profiles
# needed for distributed - IL
#SUITEFW_IL_PROFILES=PC-IL-JMS PC-IL-CORE

#### RPM VERIFICATION ######
SUITEFW_OVERRIDE_RPM_STATUS=
```

Example 5: Installing the Prime Central Portal in a Dual-Server Setup with a Remote Embedded Database

```
Installer_UI=silent

########## Basic ##########

USER_INSTALL_DIR=/opt/primecentral
SUITEFW_INSTALL_TYPE=Distributed Install
SUITEFW_DISTRIBUTED_INSTALL_TYPE=Portal
SUITEFW_BOTH_SERVER_HOSTNAME=prime-dev.cisco.com

########## OS User (primeusr is fixed, do not change it) ##########

SUITEFW_OS_USER=primeusr
SUITEFW_OS_GROUP=primegrp
SUITEFW_OS_PASSWD=Admin123~
SUITEFW_OS_TYPE=Linux

########## Application Admin user (centraladmin) password ###

SUITEFW_ADMIN_USER_PASSWD=Admin123~

########## DATABASE ##########

SUITEFW_DB_TYPE=Embedded Database

### Database User (primedba is fixed. do not change it) ###

SUITEFW_DB_USER=primedba
SUITEFW_DB_USER_PASSWD=Admin123~

### External Database

SUITEFW_DB_HOST_IP_ADDRESS=
SUITEFW_DB_SYSTEM_PASSWD=
SUITEFW_DB_SYSTEM_USER=system
SUITEFW_DB_PORT=1521
SUITEFW_DB_SID=
SUITEFW_DBF_FILES_DIR=

### Embedded Database

SUITEFW_EMBEDDED_REMOTE=1
SUITEFW_EMBEDDED_ROOT_PASSWD=poPPee123
SUITEFW_EMBEDDED_HOST_IP=209.165.200.254
SUITEFW_EMBEDDED_DBPROFILE=2
SUITEFW_EMBEDDED_SMTP=self
SUITEFW_EMBEDDED_SSH_USER=test
SUITEFW_EMBEDDED_SSH_USER_PASSWORD=Admin123~
SUITEFW_EMBEDDED_ORACLE_HOME=/export/home/oracle
SUITEFW_EMBEDDED_ORACLE_USER=oracle
SUITEFW_EMBEDDED_DATAFILES=/export/home/oracle/oradata/primedb
SUITEFW_EMBEDDED_REDO=/export/home/oracle/redo
SUITEFW_EMBEDDED_BACKUP=1
SUITEFW_EMBEDDED_ARCHIVE=/export/home/oracle/arch
SUITEFW_EMBEDDED_BACKUP_DEST=/export/home/oracle/backup

##########  Install Mode ##########

SUITEFW_BOTH_INSTALL_MODE=Simple Install

### Portal

SUITEFW_PORTAL_HTTPS_PORT=8443
```

```
SUITEFW_PORTAL_HTTP_PORT=8080
SUITEFW_PORTAL_AJP_PORT=8009
SUITEFW_PORTAL_SHUTDOWN_PORT=8005

### IL

SUITEFW_IL_MTOSI_PORT=9110
SUITEFW_IL_CONNECTION_TRANSPORTTYPE=nio
SUITEFW_IL_CONNECTION_PORT=61616
SUITEFW_IL_NIO_TRANSPORT_PORT=61616
SUITEFW_IL_SSL_TRANSPORT_PORT=61615
SUITEFW_IL_NIO_TRANSPORT_FAILOVER_PORT=61614
SUITEFW_IL_REQUEST_TIMEOUT=135000
SUITEFW_IL_3GPP_PORT=9220
SUITEFW_IL_ALARM_MGMT_PORT=9020
SUITEFW_IL_RECONNECT_DELAY=10

### IL Profiles
# needed for distributed - IL
#SUITEFW_IL_PROFILES=PC-IL-JMS PC-IL-CORE

#### RPM VERIFICATION ######
SUITEFW_OVERRIDE_RPM_STATUS=
```

Example 6: Installing the Prime Central Portal in a Dual-Server Setup with an External Database

```
Installer_UI=silent

########## Basic ##########

USER_INSTALL_DIR=/opt/primecentral
SUITEFW_INSTALL_TYPE=Distributed Install
SUITEFW_DISTRIBUTED_INSTALL_TYPE=Portal
SUITEFW_BOTH_SERVER_HOSTNAME=prime-dev.cisco.com

########## OS User (primeusr is fixed, do not change it) ##########

SUITEFW_OS_USER=primeusr
SUITEFW_OS_GROUP=primegrp
SUITEFW_OS_PASSWD=Admin123~
SUITEFW_OS_TYPE=Linux

########## Application Admin user (centraladmin) password ###

SUITEFW_ADMIN_USER_PASSWD=Admin123~

########## DATABASE ##########

SUITEFW_DB_TYPE=External Database

### Database User (primedba is fixed. do not change it) ###

SUITEFW_DB_USER=primedba
SUITEFW_DB_USER_PASSWD=Admin123~

### External Database

SUITEFW_DB_HOST_IP_ADDRESS=209.165.200.225
SUITEFW_DB_SYSTEM_PASSWD=manager
SUITEFW_DB_SYSTEM_USER=system
SUITEFW_DB_PORT=1521
SUITEFW_DB_SID=service-name
SUITEFW_DBF_FILES_DIR=/export/home/oracle/prime_test
SUITEFW_EMBEDDED_ORACLE_HOME=/export/home/oracle
```

```
##########  Install Mode ##########

SUITEFW_BOTH_INSTALL_MODE=Simple Install

### Portal

SUITEFW_PORTAL_HTTPS_PORT=8443
SUITEFW_PORTAL_HTTP_PORT=8080
SUITEFW_PORTAL_AJP_PORT=8009
SUITEFW_PORTAL_SHUTDOWN_PORT=8005

### IL

SUITEFW_IL_MTOSI_PORT=9110
SUITEFW_IL_CONNECTION_TRANSPORTTYPE=nio
SUITEFW_IL_CONNECTION_PORT=61616
SUITEFW_IL_NIO_TRANSPORT_PORT=61616
SUITEFW_IL_SSL_TRANSPORT_PORT=61615
SUITEFW_IL_NIO_TRANSPORT_FAILOVER_PORT=61614
SUITEFW_IL_REQUEST_TIMEOUT=135000
SUITEFW_IL_3GPP_PORT=9220
SUITEFW_IL_ALARM_MGMT_PORT=9020
SUITEFW_IL_RECONNECT_DELAY=10

### IL Profiles
# needed for distributed - IL
#SUITEFW_IL_PROFILES=PC-IL-JMS PC-IL-CORE

#### RPM VERIFICATION ######
SUITEFW_OVERRIDE_RPM_STATUS=
```

Example 7: Installing the Prime Central Integration Layer in a Dual-Server Setup

```
Installer_UI=silent

########## Basic ##########

USER_INSTALL_DIR=/opt/primecentral
SUITEFW_INSTALL_TYPE=Distributed Install
SUITEFW_DISTRIBUTED_INSTALL_TYPE=Integration Layer
SUITEFW_BOTH_SERVER_HOSTNAME=prime-dev.cisco.com

########## OS User (primeusr is fixed, do not change it) ##########

SUITEFW_OS_USER=primeusr
SUITEFW_OS_GROUP=primegrp
SUITEFW_OS_PASSWD=Admin123~
SUITEFW_OS_TYPE=Linux

########## Application Admin user (centraladmin) password ###

SUITEFW_ADMIN_USER_PASSWD=Admin123~

########## DATABASE ##########

SUITEFW_DB_TYPE=External Database

### Database User (primedba is fixed. do not change it) ###

SUITEFW_DB_USER=primedba
SUITEFW_DB_USER_PASSWD=Admin123~

### External Database
```

```
SUITEFW_DB_HOST_IP_ADDRESS=198.51.100.1
SUITEFW_DB_SYSTEM_PASSWD=Admin123~
SUITEFW_DB_SYSTEM_USER=primedba
SUITEFW_DB_PORT=1521
SUITEFW_DB_SID=service-name
SUITEFW_DBF_FILES_DIR=/export/home/oracle/prime_test
SUITEFW_EMBEDDED_ORACLE_HOME=/export/home/oracle

### Portal

SUITEFW_PORTAL_HTTPS_PORT=8443
SUITEFW_PORTAL_HTTP_PORT=8080
SUITEFW_PORTAL_AJP_PORT=8009
SUITEFW_PORTAL_SHUTDOWN_PORT=8005

### IL

SUITEFW_IL_MTOSI_PORT=9110
SUITEFW_IL_CONNECTION_TRANSPORTTYPE=nio
SUITEFW_IL_CONNECTION_PORT=61616
SUITEFW_IL_NIO_TRANSPORT_PORT=61616
SUITEFW_IL_SSL_TRANSPORT_PORT=61615
SUITEFW_IL_NIO_TRANSPORT_FAILOVER_PORT=61614
SUITEFW_IL_REQUEST_TIMEOUT=135000
SUITEFW_IL_3GPP_PORT=9220
SUITEFW_IL_ALARM_MGMT_PORT=9020
SUITEFW_IL_RECONNECT_DELAY=10

### IL Profiles
# needed for distributed - IL
SUITEFW_IL_PROFILES=PC-IL-JMS PC-IL-CORE
#### RPM VERIFICATION ######
SUITEFW_OVERRIDE_RPM_STATUS=
```

Verifying the Silent Installation

Step 1 Open a web browser and log in to the Prime Central portal at **https://***server-hostname***:***https-port-number*, where:

- *server-hostname* is the hostname of the newly installed Prime Central server.
- *https-port-number* is the SSL port number that was configured during installation.

Step 2 Enter the username **centraladmin** and the admin user password that you specified for the silent installation.

If you cannot log in to the Prime Central portal, check the silent installation log files in the *installation-directory*/install/logs/ folder. If the installation failed, the log files contain errors and exceptions that you can use for troubleshooting.

Installing Prime Central Fault Management

Installing the Prime Central Fault Management component—which has its own installation DVD and installation binary—is a two-part process:

1. Prepare the server for installation.
2. Install the Prime Central Fault Management component.

Note During the installation, the variables that you define must adhere to the constraints described in Pathname, Group Name, Username, and Password Constraints.

Preparing the Server for Installation

Before you install the Prime Central Fault Management component, you must first connect to the server and, if using X server, verify the display settings.

Step 1 Use one of the following options to connect to the server where you want to install Prime Central Fault Management:

- VNC (recommended)—See http://www.realvnc.com.
- X server—For this option, Reflection X is recommended. See http://www.attachmate.com/Products/PC+X+Server/rx/.

Step 2 As the root user, launch a terminal on the server where you want to install Prime Central Fault Management. The C shell (csh) is recommended. To start the C shell, enter:

/bin/csh

If you are using X server, continue to the next step.

If you are using VNC, you are finished; continue to Installing Prime Central Fault Management on the Server.

Step 3 Set the DISPLAY variable:

setenv DISPLAY *hostname-or-IP-address*:**0.0**

Step 4 Verify that the display is set correctly:

echo $DISPLAY

In the command output, you should see:

hostname-or-IP-address:0.0

Step 5 If the hosts do not have DNS access, or their hostnames are not registered in the DNS, update the /etc/hosts file on the server:

 # IP-address FQDN hostname

For example:

```
192.168.1.170 fm-server.cisco.com fm-server
```

Step 6 Save the /etc/hosts file.

Step 7 Run the following tests:

 # hostname -a

fm-server

 # hostname -f

fm-server.cisco.com

 # hostname -i

192.168.1.170

 # ipcalc -h 192.168.1.170

HOSTNAME=fm-server.cisco.com

If any of the tests return incorrect results, check the /etc/hosts file for typos. Check also the /etc/sysconfig/network file and verify that the HOSTNAME entry contains your server's FQDN (fm-server.cisco.com in this example).

Step 8 Move (or remove) all *.log files from the /tmp folder.

Step 9 Verify that the Red Hat RPM packages listed here are installed.

- To verify the RHEL 5 RPM packages, enter:

  rpm -q compat-db compat-glibc compat-glibc-headers compat-libstdc++-296 compat-libstdc++-33 elfutils elfutils-libs gtk2 gtk2-engines kernel-headers ksh libgcc libXft libXmu libXp libXpm libXtst nscd openmotif22 pam --qf "%{name}/%{version}/%{release}/%{arch}\n"

- To verify the RHEL 6 RPM packages, enter:

  rpm -q atk audit-libs cairo compat-db compat-glibc compat-libstdc++-296 compat-libstdc++-33 compat-libtermcap compat-readline5 cracklib db4 elfutils elfutils-libs expat fontconfig freetype gamin gdk-pixbuf2 glib2 glibc glibc-common glibc-devel glibc-headers gtk2 gtk2-engines jasper-libs kernel-headers ksh libICE libSM libX11 libXau libXcomposite libXcursor libXdamage libXext libXfixes libXft libXi libXinerama libXmu libXp libXpm libXrandr libXrender libXt libXtst libgcc libjpeg-turbo libpng libselinux libstdc++ libthai libtiff libuuid libxcb ncurses-libs nss-softokn-freebl openmotif22 pam pango pixman rpm-build xulrunner zlib --qf "%{name}/%{version}/%{release}/%{arch}\n"

Step 10 Set the unlimit value.

If using a C shell, enter: **limit descriptors 1048576**

In the command output, you should see:

```
# limit descriptors
descriptors 1048576
```

If using a Bash shell, enter: **ulimit -n 1048576**

In the command output, you should see:

```
# ulimit -n
1048576
```

Installing Prime Central Fault Management on the Server

Step 1 Insert the Cisco Prime Central 2.1 USB, navigate to the Fault Management folder, and locate the FM 2.1 Build.tar.gz file.

Step 2 Use SSH to connect to the server.

Step 3 Copy the FM 2.1 Build.tar.gz file to the server.

Step 4 Distribute the file:

```
 # tar -zxf FM2.1.0Build.tar.gz
# cd Disk1/InstData/VM
# chmod 755 primefm_v2.1.bin
```

Step 5 Run the installer:

./primecentral_v2.1.bin

Step 6 In the **Introduction** window, click **Next**.

Step 7 In the **License Agreement** window, read the license agreement, click the **I accept the terms of the License Agreement** radio button, and click **Next**.

Step 8 In the **Environment Validation** window, review the information for accuracy; then, click **Next**.

Step 9 In the **Server Information** window, confirm that the FQDN is correct; if not, enter the correct FQDN. Then, click **Next**.

Step 10 In the **UNIX OS User Information** window, provide the information required to create a UNIX OS user to start and stop processes; then, click **Next**.

- The username is primeusr and cannot be changed.
- The group name is ncoadmin and cannot be changed.

Step 11 In the **App User Information** window, enter the username and password for the Prime Central Fault Management application user; then, click **Next**.

Step 12 In the **Database Information** window, enter the following database connection information; then, click **Next**:

- Server IP address or hostname.
- Port—The default is 1521.
- SID—The default is primedb.
- Prime database username—The default is primedba.
- Prime database password.

Note If you specify the IP address of the Prime Central server in this window, skip ahead to Step 14.

Step 13 In the **Choose Install Folder** window, specify where to install the Fault Management server; then, click **Next**. The installation directory defaults to /opt/primeusr/faultmgmt.

Step 14 In the **Install Mode** window, specify one of the following installation modes:

- **Simple Install**—Click **Next**; then, continue to the next step.
- **Advanced Install**—Click **Next**; in the **Advanced Configuration** window, enter the desired port numbers for the Fault Management database server, gateway, and web server; then, click **Next**.

Step 15 Verify that the information in the **Pre-Installation Summary** window is correct; then, click **Install**.

Step 16 Confirm that both the Prime Central portal and the Prime Central integration layer are running on the Prime Central server.

It might take 90 minutes or longer to install Prime Central Fault Management, depending on your system performance.

Step 17 Verify that the Red Hat RPM packages listed under table are installed.

- To verify the RHEL 5 RPM packages, enter:

```
rpm -q compat-db compat-glibc compat-glibc-headers compat-libstdc++-296 compat-libstdc++-33
elfutils elfutils-libs gtk2 gtk2-engines kernel-headers ksh libgcc libXft libXmu libXp libXpm
libXtst nscd openmotif22 pam --qf "%{name}/%{version}/%{release}/%{arch}\n"
```

- To verify the RHEL 6 RPM packages, enter:

```
rpm -q compat-db compat-glibc compat-libstdc++-296 compat-libstdc++-33 elfutils elfutils-libs
gtk2 gtk2-engines kernel-headers ksh libgcc libXft libXmu libXp libXpm libXtst nscd openmotif22
 pam rpm-build --qf "%{name}/%{version}/%{release}/%{arch}\n"
```

Step 18 In the **Install Complete** window, click **Done**.

The installation log files are available in the *installation-directory*/install/logs/ folder.

Step 19 Complete the installation by logging into the Prime Central integration layer as the primeusr and entering the following commands to restart it:

```
itgctl stop
itgctl start
```

Configuring Mail Service for Alarm Reports

After successful installation of Fault Management, configure mail service for receiving alarm reports.

Step 1 Go to `~/faultmgmt/tipv2Components/TCRComponent/cognos/configuration` folder.

Step 2 Open **cogstartup.xml** file in **vi** editor.

Step 3 Scroll down to the below parameters:

```
<crn:parameter disabled="true" name="smtpMailServer">
       <crn:value xsi:type="cfg:hostPort">mailserver:25</crn:value>
     </crn:parameter>
```

Step 4 Replace **mailserver** with **localhost**.

Step 5 Save the file and close it.

Step 6 Restart Prime Central Fault Management TIP component, by logging in as *primeusr*:

```
fmctl stop tip
fmctl start tip
```

Installing Prime Central Fault Management Silently

Step 1 As the root user, launch a terminal on the server where you want to silently install Prime Central Fault Management. The C shell (csh) is recommended. To start the C shell, enter:

/bin/csh

Step 2 Insert the Cisco Prime Central 2.1 USB drive into the USB port and navigate to the local folder where the drive is mounted.

Step 3 Create a PrimeFM_install.properties file based on the sample provided in Sample PrimeFM_install.properties File.

The silent properties file is the same whether you are installing the Fault Management component on the same server as Prime Central, or on a separate server. If you are installing the Fault Management component on the same server as Prime Central, the OS user primeusr is already created. Therefore, when you create the PrimeFM_install.properties file, be sure to enter the correct password for the OS user primeusr.

Caution If you are installing the Fault Management component on the same server as Prime Central, you must install it as faultmgmt in a subdirectory immediately underneath Prime Central (for example, /opt/primecentral/faultmgmt).

Caution Be careful to enter correct values in the PrimeFM_install.properties file. The silent installation does not perform any validation on the values you enter.

Step 4 Save your changes to the PrimeFM_install.properties file.

Step 5 Change file permissions:

chmod 755 *

Step 6 Run the installer:

./primefm_v2.1.bin -i silent -f PrimeFM_install.properties

The silent installation log files are available in the *installation-directory*/install/logs/ and in /tmp folder.

It is mandatory to verify the log files for any errors before proceeding further.

Sample PrimeFM_install.properties File

The following example shows a typical PrimeFM_install.properties file for Prime Central Fault Management.

Caution The values shown in the following example are for illustrative purposes only. Be careful to enter actual values that are appropriate for your operating environment.

Note the following:

- For the PRIMEFM_OS_USER parameter, the value *primeusr* is fixed; do not change it.
- For the PRIMEFM_OS_GROUP and PRIMEFM_PA_GROUP parameters, the value *ncoadmin* is fixed; do not change it.
- For the PRIMEFM_INSTALL_TYPE parameter, if you enter **Simple Install**, the default port values will be used. If you want to use different ports, enter **Advanced Install**.

Sample PrimeFM_install.properties File when Installing Prime Central Fault Management

```
##########User Information###########
PRIMEFM_OS_USER=primeusr
PRIMEFM_OS_GROUP=ncoadmin
PRIMEFM_OS_PASSWD=Prime123@
PRIMEFM_PA_USER=primefm_pa
PRIMEFM_PA_GROUP=ncoadmin
PRIMEFM_PA_PASSWD=Prime123@
PRIMEFM_APP_USER=primefm
PRIMEFM_APP_USER_PASSWD=Prime123@
# Fully qualified hostname of the FM Server
PRIMEFM_SERVER_HOSTNAME=fm-server.cisco.com
```

```
#########Prime Central Database Information##########
PRIMEFM_DB_HOST_IP_ADDRESS=209.165.200.225
PRIMEFM_DB_PORT=1521
PRIMEFM_DB_SID=primedb
PRIMEFM_DB_SYSTEM_USER=primedba
PRIMEFM_DB_SYSTEM_PASSWD=Prime123@
##########User Install Directory#########
USER_INSTALL_DIR=/opt/primecentral/faultmgmt
##########Install Type##########
PRIMEFM_INSTALL_TYPE=Simple Install
#########Port Information##############
PRIMEFM_DB_SERVER_PORT=4100
PRIMEFM_GATEWAY_PORT=4300
PRIMEFM_PROXY_PORT=4400
PRIMEFM_PROCESS_AGENT_PORT=4200
PRIMEFM_SNMP_PROBE_PORT=1162
PRIMEFM_WEB_SERVER_PORT=16310
PRIMEFM_CORR_HTTP_PORT=9080
PRIMEFM_CORR_ADMIN_PORT=9060
PRIMEFM_CORR_DB_PORT=5435
PRIMEFM_CORR_CLI_PORT=2000
PRIMEFM_WEB_SERVER_SOAP_PORT=16313
PRIMEFM_PN_GATEWAY_PORT=6081
##########Disaster Recovery##########
# Options: 'Regular' or 'DR'
PRIMEFM_INSTALL_MODE=Regular
# Run the 'list' command on PC server and find the id value for cfm type
# Use a value of 0 for Regular mode. Use a positive value for DR mode.
PRIMEFM_CFM_ID=0
#### RPM VERIFICATION ######
PRIMEFM_OVERRIDE_RPM_STATUS=
```

Manually Registering Fault Management to Retrieve Alarm Data

If an application is integrated with Prime Central but is not up and running when the Fault Management component is installed, you must manually register with the application if you want to receive alarms immediately. (Within 10 minutes of the Fault Management installation, an automatic cron job starts alarm retrieval.)

To bypass the 10-minute waiting period and begin receiving alarms immediately:

Step 1 As the primeusr, log in to the Prime Central Fault Management server.

Step 2 After the application is integrated with Prime Central, go to the *installation-directory*/prime_integrator/scripts folder and enter:

./DMRegistration.sh

Note The Fault Management component does not retrieve alarm data for Prime Provisioning or Cisco InTracer.

Installing the Gateways Used with Prime Central

You can install IBM Tier 1 and Tier 2 gateways that are available for use with Prime Central through a separately purchased license. The gateways have their own installation binary. The installation procedure for the following gateways is mentioned below:

- **Tier 1**
  - SNMP Forwarder
  - Socket Writer
  - Flat File Writer
  - ODBC
  - MessageBus (XML)
  - JDBC
  - Oracle
  - Tivoli EIF
- **Tier 2**
  - HP/Peregrine Service Center
  - Remedy ARS
  - Tivoli Service Request Manager (TSRM)

Note The following steps do not apply to the data source adaptors (DSAs) that are included in the Prime Central base application.

Step 1 Insert the Cisco Prime Central 2.1 USB drive into the USB port, navigate to the Gateways folder, and unzip the PC_Gateways.zip file.

Step 2 From the list of files displayed in the PC_Gateways/Tier1 or PC_Gateways/Tier2 folder, copy the desired file to the workstation on which you want to install the gateway.

Step 3 Uncompress (unzip) the file:

gunzip *filename*

Step 4 Extract the .tar archive contents:

tar -xvf *filename*

Step 5 Open the README.txt file that is packaged with the gateway and follow the gateway installation steps.

Troubleshooting the Installation

If your Prime Central installation fails, you can check the log files to locate the problem and take the appropriate action.

Step 1 Check the following log files in the *installation-directory*/install/logs/ folder:

- DBUserAction.log
- ExitCode.log
- installXMP.log
- startXMP.log

The Table 14: Prime Central Log Files describes these and other log files to scan for information. The Table 15: Troubleshooting the Prime Central Installation lists specific errors you might encounter and possible solutions.

Step 2 Uninstall Prime Central as explained in Uninstalling Prime Central.

Step 3 Restart the installation.

Prime Central Log Files

Table 14: Prime Central Log Files

Log File	Description
CreateOSGroup.log	Output and errors during OS user and group creation.
CreateOSUser.log	
dbPasswdEncryption.log	Output and errors during the database and admin user password encryption process.
DBUserAction.log	Output and errors during database user and schema creation.
ExitCode.log	Exit codes for important installation actions. You can determine installation status from the exit codes.
insertESB-PC-IL-COMMON.log	Output and errors while persisting Prime Central integration layer information to the suite database.
insertESB-PC-IL-CORE.log	
insertESB-PC-IL-JMS.log	
insertESB.log	Output and errors while persisting Prime Central portal information to the suite database.
insertPortal.log	
installESB-PC-IL-CORE.log	Output and errors during the Prime Central integration layer installation.
installESB-PC-IL-JMS.log	
installXMP.log	Output and errors during XMP installation.

Log File	Description

prime_embedded_oracle.log	Embedded database installation information.
	• The local server log file is saved in *installation-directory*/local/scripts/embedded_oracle.
	• The remote server log files are saved in two locations:
	  • Local server: *installation-directory*/local/scripts/embedded_oracle.
	  • Remote server: *SSH-user-home-directory*/ORA.

primecentral_uninstall.log	Uninstallation console output that is saved to /tmp.
startXMP.log	Output and errors during XMP startup. If an error is noted during XMP startup, check the *installation-directory*/XMP_Platform/logs/Startup.log file. **Note** Installation console output is captured and stored in *installation-directory*/install/logs/primecentral_install.log.
UNINSTALL_LOG_*time-stamp*	Uninstallation information that is time stamped and saved in /var/adm/Cisco/uninstall; for example, /var/adm/Cisco/uninstall/UNINSTALL_LOG_102711-123237.

Troubleshooting the Prime Central Installation

The following table offers additional troubleshooting steps to help solve installation-related problems.

Table 15: Troubleshooting the Prime Central Installation

Problem	Solution

An embedded database installation fails with the following error in the *installation-directory*/local/scripts/prime_embedded_oracle.log file:
`Removing user 'oracle'`
`ERROR: Failed removing user 'oracle', please remove it manually`
`by running 'userdel oracle'. ABORTING. ***`
If you try to remove the oracle user manually, the following errors are generated:
`# userdel oracle`
`userdel: error deleting password entry`
`userdel: error deleting shadow password entry`
	In the /etc/nsswitch.conf file, remove the nis entry from passwd, shadow, group, and services. Then, remove the oracle user.

Problem	Solution
The installation validation fails with an insufficient disk space error, even though the disk partition used to create the installation directory has more than 20 GB of free space.	Do the following: 1. Enter the following to see if the installer is running on a non-English locale and therefore cannot parse the command outputs: # **env | grep LANG** **LANG=it_IT.UTF-8** 2. Change the locale to **en_US.UTF-8** and retry the installation.

An embedded database installation fails with the following errors in the *installation-directory*/local/scripts/prime_embedded_oracle.log file:
`Checking Temp space: must be greater than 120 MB.`
`Actual 28037 MB`
`Passed`
`Checking swap space: must be greater than 150 MB.`
`Actual 4095 MB`
`Passed`
`Database closed.`
`Database dismounted.`
`ORACLE instance shut down.`
`File created.`
`ORA-27102: out of memory`
`Linux-x86_64 Error: 28: No space left on device`
`Disconnected from Oracle Database 12c Enterprise Edition Release`
`11.2.0.1.0 - 64bit Production`
`With the Partitioning, OLAP and Real Application Testing options`
`0`
`'*** ERROR: Failed to execute the post installation tasks. Check`
`log for more details. ABORTING. ***'`
`'*** ERROR: Installation failed. ABORTING. ***'`
	Verify that the available free memory on the system meets the Oracle installation requirements.

An embedded database installation fails with the following error in the *installation-directory*/local/scripts/prime_embedded_oracle.log file:
`'*** ERROR: Failed to enable automatic backups. Check log for`
`more details. ABORTING. ***'`
	Verify that the available disk space meets the Oracle installation requirements.

Problem	Solution
An embedded database installation fails with the following errors in the *installation-directory*/local/scripts/prime_embedded_oracle.log file: `Running (su - oracle -c "/export/home/oracle/product/11.2.0/db_1/bin/netca /silent /responsefile /export/home/oracle/tmp_prime/netca.rsp") euid: 0 '*** ERROR: Failed to run netca (256)' Wed Aug 21 14:43:59 PDT 2013 Oracle Net Configuration Assistant Parsing command line arguments: Parameter "silent" = true Parameter "responsefile" = /export/home/oracle/tmp_prime/netca.rsp Parameter "log" = /export/home/oracle/tmp_prime/netca.log Done parsing command line arguments. Oracle Net Services Configuration: LISTENER: The information provided for this listener is currently in use by other software on this computer. Default local naming configuration complete. Created net service name: primedb Profile configuration complete. Check the trace file for details: /export/home/oracle/cfgtoollogs/netca/trace_OraDB12Home1-110824 2PM4358.log Oracle Net Services configuration failed. The exit code is 1`	Verify that the /etc/hosts format is correct; for example: `127.0.0.1 localhost.localdomain localhost ::1 localhost6.localdomain6 localhost6 10.10.10.10 core.domain.com core`
An embedded database installation fails with the following errors in the *installation-directory*/local/scripts/prime_embedded_oracle.log file: `ORA-27102: out of memory Linux-x86_64 Error: 28: No space left on device Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production With the Partitioning, OLAP and Real Application Testing options 0 *** ERROR: Failed to execute the post installation tasks. Check log for more details. ABORTING. ***`	Verify that your system meets the requirements listed in Embedded Database Requirements, on page 19.

Problem	Solution
Database connection errors are generated while installing the Prime Central integration layer in a dual-server setup.	Do the following: **1.** Verify that the Prime Central integration layer can access the suite database server. **2.** Verify that the database is up and running. **3.** If there is a firewall on the suite database server that prevents external connections, disable the firewall as well as SELinux by entering the following commands as the root user: To disable the firewall: **service iptables save** **service iptables stop** **chkconfig iptables off** **service ip6tables save** **service ip6tables stop** **chkconfig ip6tables off** To disable SELinux: **vi /etc/selinux/config** **change** **SELINUX=enforcing** **to** **SELINUX=disabled**

An embedded database installation fails with the following errors in the *installation-directory*/local/scripts/prime_embedded_oracle.log file:
`ERROR: Failed to run netca (256) UnsatisfiedLinkError exception`
`loading native library: njni11`
`java.lang.UnsatisfiedLinkError: /export/home/oracle/product/11.2.0/db_1/lib/libnjni11.so: libclntsh.so.11.1: cannot open shared object file: No such file or directory`
`Error: jniGetOracleHome`
`Oracle Net Services configuration failed. The exit code is 1`
`. ABORTING. ***`
	Verify that the correct Oracle system packages are installed in libaio-devel, libaio, and glibc-devel. For example, this problem occurs if glibc-devel-2.5.49 (x86_64) is not installed on the x86_64 system. To verify that the correct Oracle system packages are installed, enter:
	rpm -qa --queryformat "%{NAME}-%{VERSION}.%{RELEASE} (%{ARCH})\n" | sort > /tmp/rpmlist.txt

Problem	Solution
The Prime Central installation quits with an error message about viewing the prime_embedded_oracle.log file on both the local and remote machines. However, no log files exist at the specified locations.	Look at the primecentral_install.log file for exceptions or errors that relate to zip, unzip, or open files. (The primecentral_install.log file is located under /tmp/ or *installation-directory*/install/logs/.) The root cause of this problem is that the ulimit value was not set to ulimit -n 1048576.

An embedded database installation fails because the /etc/oratab file contains an extra user at the bottom of the file, as shown in the following example:
`# This file is used by ORACLE utilities.  It is created by`
`# root.sh and updated by the Database Configuration Assistant`
`# when creating a database.`
`# A colon, ':', is used as the field terminator.  A new line`
`# terminates the entry.  Lines beginning with a pound sign, '#',`
`# are comments.`
`#`
`# Entries are of the form:`
`#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:`
`#`
`# The first and second fields are the system identifier and home`
`# directory of the database respectively.  The third field`
`# indicates to the dbstart utility that the database should,`
`# "Y", or should not, "N", be brought up at system boot time.`
`#`
`# Multiple entries with the same $ORACLE_SID are not allowed.`
`#`
`#`
`orcl:/opt/oracle/app/oracle/product/11.2.0/dbhome_5:N`
	Verify that the /etc/oratab file does not contain any users except for the primedb user. (Because the installation failed, the primedb user might not be present.) If /etc/oratab contains any user other than the primedb user, delete the extra user. Then, rerun the installation.

Problem	Solution
The Prime Central installation fails after installing the database. As part of the failed installation, the installer copies the /var/.com.zerog.registry.xml file to the system. If you later try to reinstall Prime Central, the presence of the /var/.com.zerog.registry.xml file prevents you from performing any subsequent installations.	Do the following: 1. Uninstall Prime Central (if the uninstall folder exists). 2. If the uninstall folder does not exist, do the following as the root user: 1. Check for any users: **su - primeusr** 2. If any users exist, remove them: **userdel primeusr** 3. Delete the /var/.com.zerog.registry.xml file manually. 3. Reinstall Prime Central.

While registering an application with Prime Central, you receive error messages similar to the following:
`********* Running DMIntegrator on hostname at Thu Dec 19 06:26:52 PDT 2013 **********`
`- Initializing`
`- Checking property file`
`- Validating Java`
`- Setting ENVIRONMENT`
`- User Home Directory: /opt/CiscoTransportManagerServer`
`- Extracting DMIntegrator.tar`
`mkdir: Failed to make directory "DMIntegrator"; File exists`
`- Setting Java Path`
`mkdir: Failed to make directory "lib"; File exists`
`- JAVA BIN : /opt/jdk1.6.0_24/bin/java -classpath /opt/CiscoTransportManagerServer/prime_integrator/DMIntegrator/lib/*:/opt/CiscoTransportManagerServer/prime_integrator/DMIntegrator/lib`
`- Creating Data Source`
`- Encrypting DB Passwd`
`- Created /opt/CiscoTransportManagerServer/prime_integrator/datasource.properties`
`- PRIME_DBSOURCE: /opt/CiscoTransportManagerServer/prime_integrator/datasource.properties`
`- Checking DB connection parameters`
`@@@@ Aborting Due to: Database connection error. Please verify DB connection parameters. Exiting. @@@@@@@`
	Add the entry **dns** next to “hosts:” in the /etc/nsswitch.conf file.

Problem	Solution
Installation of the Fault Management component fails.	Review the installation log files in the *installation-directory*/install/logs folder: • CheckLogs.log—Indicates which main log file has an error. • PrimeFM-install.log—Provides the status of the IBM component installation process. • PrimeFM-post.log—Provides the status of the configuration process. • primefm.log—Provides a summary (which includes additional error information) of the PrimeFM-install and PrimeFM-post processes. If Impact failed, this typically indicates that either the FQDN of the Fault Management server was not entered during the installation process or the FQDN of the Fault Management server was incorrectly entered in DNS or the /etc/hosts file. If TCR failed, this typically indicates that an RPM is missing. Verify that all of the required RPMs have been installed.
`mbind: Invalid Argument` errors are present in the Fault Management log files.	Remove the numactl-devel RPM package: **1.** Log in as the root user. **2.** Enter the following command: **rpm -ev numactl-devel** You will also need to delete the `mbind: Invalid Argument` errors from the following files (making sure that the password property is set to the {aes}xyz value): • ~/faultmgmt/impact/etc/NCI_ReportsHSQLDB.ds • ~/faultmgmt/impact/etc/NCI_defaultobjectserver.ds • ~/faultmgmt/impact/etc/NCI_wsadmin.props

Problem	Solution
`Could not reserve enough space for object heap` error occurs during initialization of VM.	Add the following environment variable to your session prior to running the installation binary: **export _JAVA_OPTIONS="-Xms128m -Xmx512m"** If the error still appears, try doubling the Xmx value.

Prime Central/ Fault Management installation fails because of RPM installation error as in /opt/primecentral/install/logs/installUtils.log or /opt/primecentral/install/logs/installRPM.log :
`Verifying required RPMs installed or not`
`Verifying...`
`Following packages are missing:`
`nscd-2.12-1.209.el6_9.1.x86_64`
`gmp-4.3.1-12.el6.i686`
`libgomp-4.4.7-18.el6.i686`
`Comparing: Installed [tzdata-2013g-1.el6.noarch] vs Required [tzdata-2017b-1.el6.noarch]`
`Installed RPM [tzdata-2013g-1.el6.noarch] is older than required RPM [tzdata-2017b-1.el6.noarch]`
	Install the missing RPMs or RPMs of same version first and then install Prime Central/ Fault Management

Prime Central Portal GUI is not displayed properly after VM reboot or after rollback (in case of upgrade failure).	As the primeusr, restart the Prime Central portal by entering the following commands:
	`portalctl stop`
	`portalctl start`

Prime Central GUI is not launching completely after successful installation.	Add the hostname of Prime Components in `/etc/hosts` of windows, which allows access to browser and also to enable the java security.
Domain Manager status shows down in Prime Central.	Make sure that all nodes are Syncronized with same the NTP server.
After the installation of secondary Prime central the `itgctl` status shows stopped.	Manually execute `itgctl start and portalctl` in the Secondary Prime Central.

Configuring Prime Carrier Management Suite Scale Setup

Before starting the integration process, perform the Prime Carrier Management suite scale setup.

Note The following steps are applicable only to Extremely Large scale setups.

Step 1 Switch to Oracle User:

su - oracle

Step 2 Login to sql prompt as sysdba:

sqlplus / as sysdba

Step 3 Enter the following query @ sql prompt:

alter system set sga_max_size=8G scope=spfile;

Step 4 Come out of sql prompt and oracle user using **exit** command.

Step 5 Switch to the primeusr to restart emdbctl and portalctl (Oracle Database) with the following commands:

su - primeusr

portalctl stop

emdbctl --stop

emdbctl --start

portalctl start

Step 6 Come out of primeusr user using **exit** command.

Step 7 Switch again to Oracle User to increase db_cache size:

su - oracle

Step 8 Login to sql prompt as sysdba:

sqlplus / as sysdba

Step 9 Enter the following query @ sql prompt:

alter system set db_cache_size=4G;

Step 10 Come out of sql prompt and oracle user using **exit** command.

Configuring Applications as Suite Components

You can integrate an existing installation of the following applications with Prime Central:

- Cisco InTracer
- Prime Network, including the Prime Network integration layer
- Prime Optical, including the Prime Optical integration layer
- Prime Performance Manager
- Prime Provisioning
- Agora-NG

This section assumes that you have already installed the application in standalone mode, and now you want it to join the Prime Carrier Management suite.

Before starting the integration process, perform the Prime Carrier Management suite scale setup. For more information on the required network size for installation, see Prime Carrier Management Sizing guide.

Integration Process

When you install an individual application, it contains the following files, which the Prime Central portal and Prime Central integration layer require to identify and route to the application:

- DMIntegrator.sh—Wrapper script to invoke the API to register the application with the Prime Central platform.
- DMIntegrator.tar—Tar bundle that contains the libraries required to register the application.

The application integration (also known as *registration*) process is as follows:

1. The DMIntegrator.sh and DMIntegrator.tar files integrate the application with Prime Central. (These files are bundled with the application installers.)
2. The DMIntegrator.prop file is generated when the application is installed. (This file contains information to populate the application in the Prime Central database and is provided as input to the DMIntegrator.sh script.)
3. The DMIntegrator.sh script runs in *interactive* or *silent* mode:
   - Interactive mode—You are prompted for database information such as username, password, IP address, service name, and so on.
   - Silent mode—Database information is passed as CLI arguments to the DMIntegrator.sh script.

   These modes are useful for both:
   - Standalone application integration
   - Seamless installation as a suite component
4. The DMIntegrator.sh script calls the DMSwitchToSuite.sh script, which switches between the standalone application installer and the integrated application installer.
5. The application installer installs the application in either *standalone* or *integrated* mode. In integrated mode, the application installer calls the DMIntegrator.sh script to make the integration seamless.

Note the following:

- Once Prime Provisioning is integrated with Prime Central, it cannot be reverted to standalone mode, even after unregistering Prime Provisioning.
- The DMIntegrator.sh, DMIntegrator.tar, and DMIntegrator.prop files reside in the *application-installation-directory*/prime_integrator/ folder on the application server.
- The DMIntegrator.sh file generates the following output, which is available in the *application-installation-directory*/prime_integrator/ folder:
  - datasource.properties—Contains connection information for the Prime Central database; the password is encrypted.

- dmid.xml—Contains a unique ID that the application uses to update its information in the Prime Central database.
- pc.xml—Contains the name of the Prime Central server with which the application integrates.

- If Prime Network is installed on an IPv6-only gateway, you *cannot* integrate it with Prime Central.

Contents of the DMIntegrator.prop File

The DMIntegrator.prop file is generated by entering environment values for each application. The file contains the following name-value pairs:

```
TYPE={cfm | cit | ful | net | opt | ppm}
DISPLAY={Fault Management | CIT | Prime Network | Prime Optical | Prime Performance Manager
 |
Prime Provisioning}
HOSTNAME=
DESCRIPTION=
VERSION=
PATCH=
DB_VERSION=
DB_LOCATION=
DB_SID=
DB_PORT=
DB_TYPE=
INSTALL_DATE_TIME=
INSTALL_LOCATION=
OS_USERNAME=
SWITCH_TO_SUITE_LOC=
PROTOCOL_PORT_PAIR=<name:value,name:value,name:value,...>
BUILD_NUMBER=
```

where:

- DISPLAY is the application.
- SWITCH_TO_SUITE_LOC is the location of the DMSwitchToSuite.sh script on the application.
- PROTOCOL_PORT_PAIR is a comma-separated pair of protocols and ports relevant to the application.
- BUILD_NUMBER is the build number of the installed application.

DMIntegrator.sh Script Usage

The DMIntegrator.sh script shows the following usage:

```
./DMIntegrator.sh [-n] prop-file server-hostname service-name db-user db-password db-port
./DMIntegrator.sh [-a] prop-file server-hostname service-name db-user db-password db-port
./DMIntegrator.sh [-i] prop-file
```

where:

- -n is for noninteractive, single application instance registration
- -a is for noninteractive, multiple application instance registration
- -i is for interactive mode for both single and multiple application instance registration

When multiple instances of Prime Network are integrated with Prime Central, they all must be the same version.

For example:

```
./DMIntegrator.sh -a DMIntegrator.prop db-server db-sid db-user db-password db-port
```

where:

- db-server—Prime Central database server hostname or IP address.
- db-sid—Prime Central database service name (*primedb* for an embedded database; user provided for an external database).
- db-user—Prime Central database user (*primedba* for an embedded or external database).
- db-password—Prime Central database user password.
- db-port—Prime Central database port number (*1521* for an embedded database; user provided for an external database).

Note The DMIntegrator.sh script output is available in the DMIntegrator.log file.

Integrating Cisco InTracer with Prime Central

Step 1 As the application user, shut down Cisco InTracer.

Step 2 Verify that the JAVA_HOME environment variable points to Java 1.7, which the DMIntegrator.sh script requires.

Step 3 Verify that the /usr/bin/scp secure copy tool is present on the Cisco InTracer server.

Step 4 Under the Cisco InTracer home folder, create a prime_integrator folder (if it does not already exist) and copy the following files to it:

- DMIntegrator.prop
- DMIntegrator.sh
- DMIntegrator.tar

Step 5 Verify that permissions are correct.

Step 6 Run the DMIntegrator.sh script. (For usage details, see DMIntegrator.sh Script Usage.)

$ ./DMIntegrator.sh

Step 7 As the primeusr user, log in to the Prime Central integration layer and restart it:

a) Enter the following command, which lists all integration layer instances (and their profiles) that are running:

itgctl list

b) Note down the ID of the integration layer instance with the "PC-IL-CORE" profile.

c) Stop the PC-IL-CORE profile instance:

itgctl stop *ID*

d) Restart the integration layer:

itgctl start *ID*

Step 8 Start Cisco InTracer.

Step 9 After Cisco InTracer is integrated with Prime Central, use the Prime Central portal to create new users, even if they already existed in standalone mode.

Integrating Prime Network with Prime Central

Step 1 As the application user, shut down Prime Network:

networkctl stop

Step 2 Enter:

cd $PRIME_NETWORK_HOME/Main ; runRegTool.sh localhost set suite-integ/enabled true

Note Complete this step *only* if you are registering a Prime Network instance that was previously unregistered. If this is not the case, proceed to Step 3.

Step 3 Verify that the JAVA_HOME environment variable points to Java 1.7 , or 1.8 from Prime Network 4.3 onwards which the DMIntegrator.sh script requires:

java –version

Step 4 Verify that the correct value is configured for the HOSTNAME object in the DMIntegrator.prop file.

a) Enter the following command:

hostname – –fqdn

b) On the primary Prime Network server, navigate to the $PRIME_NETWORK_HOME/prime_integrator directory.

c) Open the DMIntegrator.prop file and confirm that the value configured for the HOSTNAME object is the same as the gateway listed after running the **hostname –fqdn** command.

Note Only complete this step if Prime Network is installed in a local and Geographical redundancy configuration. Otherwise, proceed to Step4 .

Step 5 Run the DMIntegrator.sh script.

./DMIntegrator.sh -a DMIntegrator.prop Prime-Central-DB-hostname db-SID db-user db-password port

Step 6 Start Prime Network:

networkctl start

Step 7 Restart the Prime Central integration layer so that it recognizes the recently added Prime Network server:

itgctl stop

itgctl start

Step 8 Now that Prime Network is integrated with Prime Central, you must also integrate the Prime Network integration layer. Continue to Integrating the Prime Network Integration Layer with Prime Central.

Step 9 After Prime Network is integrated with Prime Central, use the Prime Central portal to create new users, even if they already existed in standalone mode (or provide PN scope to the users).

To provide Prime Network scope to users, see the topic "Creating New Device Scopes to Control Device Access" in the Cisco Prime Network 5.1 Administrator Guide, Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."

Integrating the Prime Network Integration Layer with Prime Central

Step 1 As the Prime Network user, log in to the Prime Network gateway:

ssh root@*Prime-Network-host-IP-address*

su - prime

Note In this example, *prime* is the Prime Network user.

Step 2 Disable the Prime Network integration layer health checker by entering the following command on the Prime Network gateway server:

$PRIMEHOME/local/scripts/il-watch-dog.sh disable

Step 3 Stop the Prime Network integration layer:

$PRIMEHOME/bin/itgctl stop

Step 4 Change directories to the $PRIMEHOME/integration directory:

cd $PRIMEHOME/integration

Step 5 Verify that the correct value is configured for the HOSTNAME object in the ILIntegrator.prop file.

a) Enter the following command:

hostname —fqdn

b) On the primary Prime Network server, navigate to the $PRIMEHOME/pnil directory.

c) Open the ILIntegrator.prop file and confirm that the value configured for the HOSTNAME object is the same as the gateway listed after running the **hostname —fqdn** command.

Note Only complete this step if Prime Network is installed in a local and Geographical redundancy configuration. Otherwise, proceed to Step 6.

Step 6 Run the DMIntegrator script.

./DMIntegrator.sh -a ILIntegrator.prop *Prime-Central-DB-hostname db-SID db-user db-password port*

Step 7 Reload the user profile:

source $HOME/.cshrc

Step 8 Enable the Prime Network integration layer health checker by entering the following command on the Prime Network gateway server:

$PRIMEHOME/local/scripts/il-watch-dog.sh enable

Step 9 Start the Prime Network integration layer:

$PRIMEHOME/bin/itgctl start

Step 10 Restart Prime Central integration layer in order for the new Prime Network server to be recognized by the application:

(as primeusr)

itgctl stop

itgctl start

Note The Prime Network integration layer will remain in **Unknown** state (even after integration), if the Prime Central integration layer is not restarted.

Integrating Prime Network in a High Availability Configuration with Prime Central

Step 1 As the application user, shut down Prime Network.

Step 2 Verify that the JAVA_HOME environment variable points to Java 1.7 , or 1.8 from Prime Network 4.3 onwards, which the DMIntegrator.sh script requires.

Step 3 Verify that the /usr/bin/scp secure copy tool is present on the Prime Network server.

Step 4 Under the Prime Network home folder, create a prime_integrator folder (if it does not already exist) and copy the following files to it:

- DMIntegrator.prop
- DMIntegrator.sh
- DMIntegrator.tar

Step 5 Verify that permissions are correct.

Step 6 In the DMIntegrator.prop file, change the HOSTNAME value to **ana-cluster-ana**.

Step 7 Add the hostname **ana-cluster-ana** to the /etc/hosts file on the Prime Central machine.

Step 8 On the client workstation, repeat the preceding step. If you are using a Windows workstation, use the C:\Windows\system32\drivers\etc\hosts file.

Step 9 Run the DMIntegrator.sh script.

./DMIntegrator.sh -a DMIntegrator.prop *Prime-Central-DB-hostname db-SID db-user db-password port*

Note For the database IP address or hostname, use the virtual IP address of the HA server.

Step 10 As the Prime Network user, run the jars script:

a) Enter:

cd ~/prime_integrator/PN_PC_Integration/

perl runPrimeCentralUpgrade.pl

b) When prompted, enter the Prime Central IP address, Prime Central root username and password, and the system's Prime Central username (usually primeusr).

Step 11 If you are reintegrating the same Prime Network instance with a different COM-URI, you must restart the Prime Central portal. (The COM-URI is the Prime Network identifier and can be found in the Prime Central portal > Suite Monitoring portlet.) To do so, log in to the Prime Central portal as the primeusr user and enter:

portalctl stop

portalctl start

Step 12 Start Prime Network.

Step 13 After Prime Network is integrated with Prime Central, use the Prime Central portal to create new users, even if they already existed in standalone mode.

Integrating the Prime Network Integration Layer in a High Availability Configuration with Prime Central

Prime Central supports integration with the Prime Network integration layer in the following high availability configurations:

- Local redundancy *only*, which uses two active local servers for automatic failover.
- Geographical disaster recovery *only*, which uses a server at a remote geographical site for a full disaster recovery.

Complete the integration procedure specific to the configuration you have in place.

Local Redundancy Configuration

Step 1 As the root user, log in to the Prime Network primary cluster node.

Step 2 Freeze the “ana” service:

clusvcadm -Z ana

Step 3 Switch users to the Prime Network Gateway application user:

su – anauser

Step 4 Stop the Prime Network integration layer:

$PRIMEHOME/bin/itgctl stop

Step 5 Change to the $PRIMEHOME/integration directory:

cd $PRIMEHOME/integration

Step 6 Open the ILIntegrator.prop file:

vi $PRIMEHOME/integration/ILIntegrator.prop

Step 7 Change the HOSTNAME value to ana-cluster-ana.

Step 8 Run the DMIntegrator.sh script.

./DMIntegrator.sh -a ILIntegrator.prop *Prime-Central-database-server service-namedb-user db-password db-port*

where *Prime-Central-database-server* is the server's hostname or IP address.

Note If you specify the IP address of the database server, use the virtual IP address of the HA server.

Step 9 Reload the user profile:

source $HOME/.cshrc

Step 10 Start the Prime Network Integration layer:

$PRIMEHOME/bin/itgctl start

Step 11 As the root user, unfreeze the "ana" service:

clusvcadm -U ana

Step 12 If you install a Prime Network instance after Prime Performance Manager is integrated with Prime Central, enter the following commands in Prime Performance Manager GW server to integrate Prime Performance Manager with Prime Network:

/opt/CSCOppm-gw/bin/sgmInventoryImportUtility.sh -installCrossLaunchPoints

/opt/CSCOppm-gw/bin/sgmInventoryImportUtility.sh -installTrapSupport

Geographical Disaster Recovery Configuration

Complete the following procedures for both the primary and geographical disaster recovery Prime Network servers.

Configuring the Primary Server

Step 1 As the root user, log in to the primary Prime Network primary server:

ssh root@*server*

where *server* is the primary server's hostname or IP address.

Step 2 Switch users to the Prime Network application user:

su – *username*

Step 3 Disable the Prime Network integration layer health monitor and stop the Prime Network integration layer:

$PRIMEHOME/local/scripts/il-watch-dog.sh disableandstop

Step 4 Change to the $PRIMEHOME/integration directory:

cd $PRIMEHOME/integration

Step 5 Run the DMIntegrator.sh script.

./DMIntegrator.sh -a ILIntegrator.prop *Prime-Central-database-server service-name db-user db-password db-port*

where *Prime-Central-database-server* is the server's hostname or IP address.

Step 6 Reload the user profile:

source $HOME/.cshrc

Step 7 Run the **itgctl list** command to obtain the Prime Network integration layer's instance ID value.

You will need this for Step 8 of the Configuring the Geographical Disaster Recovery Serverprocedure.

Step 8 Enable the Prime Network integration layer health monitor:

$PRIMEHOME/local/scripts/il-watch-dog.sh enable

Step 9 Start the Prime Network Integration layer:

$PRIMEHOME/bin/itgctl start

Configuring the Geographical Disaster Recovery Server

Step 1 As the root user, log in to the geographical disaster recovery Prime Network server:

ssh root@*server*

where *server* is the geographical disaster recovery server's hostname or IP address.

Step 2 Change to the /var/adm/cisco/prime-network/scripts/ha/rsync directory:

cd /var/adm/cisco/prime-network/scripts/ha/rsync

Step 3 Rename the rsync_exclude_pnil_cfg.txt file:

mv rsync_exclude_pnil_cfg.txt rsync_exclude_pnil_cfg.txt.org

Step 4 Switch users to the Prime Network application user:

su – *username*

Step 5 Disable the Prime Network integration layer health monitor and stop the Prime Network integration layer:

$PRIMEHOME/local/scripts/il-watch-dog.sh disableandstop

Step 6 Change to the $PRIMEHOME/integration directory:

cd $PRIMEHOME/integration

Step 7 Open the ILIntegrator.prop file:

vi $PRIMEHOME/integration/ILIntegrator.prop

Step 8 Change the HOSTNAME value to the standby Prime Network geographical disaster recovery server's hostname.

Integrating Prime Optical and the Prime Optical Integration Layer with Prime Central

Step 1 As the application user, shut down Prime Optical:

opticalctl stop

Step 2 Under the application home folder, change directories to the /bin directory:

cd /opt/CiscoTransportManagerServer/bin

Step 3 Run the CPOIntegrator.sh script:

CPOIntegrator.sh -a *prop-file server-hostname service-name db-user db-password port-number*

For example:

CPOIntegrator.sh -a DMIntegrator.prop prime-server primedb primedba Test456@ 1521

Note The DMIntegrator.prop file is located in the /opt/CiscoTransportManagerserver/prime_integrator folder by default. (If you want to use a different properties file, you must indicate its complete path.)

Step 4 Start Prime Optical:

opticalctl start

Integrating Prime Performance Manager with Prime Central

Tip Integrate Prime Performance Manager with Prime Central *after* you integrate the Fault Management component and each instance of Prime Network with Prime Central.

Step 1 As the root user, log in to the Prime Performance Manager gateway server and navigate to the *Prime-Performance-Manager-gateway-installation-directory*/bin directory.

Step 2 Enter:

./ppm primecentralintegration

Step 3 Enter the appropriate responses at the prompts:

- Database Host—Enter the Prime Central database server hostname or IP address.
- Database SID [primedb]—Enter the Prime Central database service name, which is *primedb* by default.
- Database User [primedba]—Enter the Prime Central database username, which is *primedba* by default.
- Database Password [*****]—Enter the Prime Central database user password; for example, *Test456@*.
- Database Port [1521]—Enter the Prime Central database port number, which is *1521* by default.

Step 4 Restart Prime Performance Manager for the changes to take effect.

Step 5 As the primeusr user, log in to the Prime Central integration layer and restart it:

itgctl stop

itgctl start

Step 6 If you are reintegrating Prime Performance Manager after a previous integration, you must unregister it from Prime Central before you reintegrate it. See Unregistering Prime Performance Manager.

Step 7 If remote units are connected to the gateway, complete the below steps to enable SSL on remote units:

a) Log into the remote unit.

b) Enable SSL on the unit:

/opt/CSCOppm-unit/bin/ppm ssl enable

Prime Performance Manager:

- Stops the unit.
- Generates RSA private key.

c) When prompted, enter the SSL distinguishing information for the unit:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Prime Performance Manager generates the server.key, server.crt, and server.csr on the **unit /opt/CSCOppm-unit/etc/ssl directory**:

d) Import the unit certificate to the gateway:

1. Copy the**/opt/CSCOppm-unit/etc/ssl/server.crt**to a temporary location on the gateway, for example,**/tmp/server.crt**.
2. Enter the following command to import the unit certificate:

/opt/CSCOppm-gw/bin/ppm certtool import myhostname-unit -file filename

Where alias is a string that is an alias for the certificate file and filename is the full path name for the certificate file, for example,**/tmp/server.crt.** Each imported certificate must have a unique alias when imported.

e) Import the gateway certificate to the unit:

1. Copy the**/opt/CSCOppm-gw/etc/ssl/server.crt**to a temporary location on the unit machine, for example,**/tmp/server.crt**.
2. Import the gateway certificate:

/opt/CSCOppm-unit/bin/ppm certtool import myhostname-gateway -file filename

Where alias is a string that is an alias for the certificate file and filename is the full path name for the certificate file, for example,**/tmp/server.crt**.

Note The gateway imports the certificate file for each unit that connects to it. Each unit then imports the gateway certificate file for the gateway that it connects to.

f) Restart the gateway:

/opt/CSCOppm-gw/bin/ppm restart

g) Restart the remote unit:

/opt/CSCOppm-unit/bin/ppm restart unit

Step 8 After Prime Performance Manager is integrated with Prime Central, use the Prime Central portal to create new users. (Any users that existed before the integration are removed during the integration.)

Step 9 If you install a Prime Network instance *after* Prime Performance Manager is integrated with Prime Central, enter the following commands to integrate Prime Performance Manager with Prime Network:

/opt/CSCOppm-gw/bin/sgmInventoryImportUtility.sh -installCrossLaunchPoints

/opt/CSCOppm-gw/bin/sgmInventoryImportUtility.sh -installTrapSupport

Step 10 If Prime Performance Manager is configured to send alarms directly to the Prime Central Fault Management server, verify that an upstream OSS host is configured correctly in the System Event Editor of Prime Performance Manager.

Step 11 If you install the Fault Management component after Prime Performance Manager is integrated with Prime Central, enter the following command and select Fault Management as the trap destination to integrate it with Prime Performance Manager:

./ppm setpctrapdestination

For example:

```
# ./ppm setpctrapdestination

Trap destinations registered with Prime Central:

1. Prime Central Fault Management (hostname)
2. Prime Network (hostname-1)
3. Prime Network (hostname-2)
4. Prime Network (hostname-3)

Enter trap destination: [1, 2, 3, 4] 1, 2, 3
```

Integrating Prime Provisioning with Prime Central

Step 1 As the application user, shut down Prime Provisioning.

./prime.sh stop

Step 2 Set the Prime Provisioning environment:

./prime.sh shell

Step 3 Run the DMIntegrator.sh script. (For usage details, see DMIntegrator.sh Script Usage.)

$ ./DMIntegrator.sh

Step 4 As the primeusr user, log in to the Prime Central integration layer and restart it:

a) Enter the following command, which lists all integration layer instances (and their profiles) that are running:

itgctl list

b) Note down the ID of the integration layer instance with the "PC-IL-CORE" profile.

c) Stop the PC-IL-CORE profile instance:

itgctl stop *ID*

d) Restart the integration layer:

itgctl start *ID*

Step 5 If you are reintegrating Prime Provisioning with a different COM-URI, you must restart the Prime Central portal. (The COM-URI is the Prime Provisioning identifier and can be found in the Prime Central portal > Suite Monitoring portlet.) To do so, log in to the Prime Central portal as the primeusr user and enter:

portalctl stop

portalctl start

Step 6 Start Prime Provisioning.

As Prime Provisioning user, log in to the Prime Provisioning server and run:

./prime.sh start

Step 7 After Prime Provisioning is integrated with Prime Central, use the Prime Central portal to create new users, even if they already existed in standalone mode.

Integrating Cisco ME 4600 Series Agora-NG with Prime Central

Step 1 Log in to the Agora-NG server as the user *agorang*.

Step 2 Enter the following commands:

~$ cd share/primecentral

~/share/primecentral$ bash DMIntegrator.sh -n DMIntegrator.prop *pc-server pc-db-sid pc-db-user pc-db-password pc-db-port*

~/share/primecentral$ agorang restart

where:

- *pc-server*—Prime Central server hostname or IP address.
- *pc-db-sid*—Prime Central database service name.
- *pc-db-user*—Prime Central database user.
- *pc-db-password*—Prime Central database user password.
- *pc-db-port*—Prime Central database port number.

Once Agora-NG restarts, integration with Prime Central is complete.

Integrating Cisco Broadband Access Center (BAC) with Prime Central

Before you integrate Cisco BAC with Prime Central, we recommend that you first install Cisco BAC's Regional Distribution Unit (RDU) and Device Provisioning Engine (DPE) components.

To integrate Cisco Broadband Access Center (BAC) with Prime Central, refer to the procedure in section **Integrating Serving Node with Prime Central Active Server** in the Cisco RAN Management System Installation Guide, Release 5.1.

For AP Boot Notification Alarm configuration, refer to the section **Configuring SNMP Trap for CPEs** in the Cisco Broadband Access Center 3.10 Administrator Guide.

Integrating RAN Management System (RMS) with Prime Central

The 'configure_fm_server.sh' script is used to integrate Cisco RMS with the Prime Central NMS for fault notification. This script allows the registration of the Domain Manager for RMS in the Prime Central NMS. Prime Central allows the receipt of SNMP traps from RMS only if DM registration for RMS is completed

The 'configure_fm_server.sh' script:

- Accepts the following NMS interface details and updates the FMServer.properties file (for FM Server) and /etc/snmp/snmpd.conf (for snmp)

  .
- NMS interface IP address, port number (162 or 1162), community string, supported SNMP version (v1 or v2c)

  .
- Adds the ip tables rules to allow the SNMP traps to be notified to the specified NMS interfaces

Subsequently, during deployment the script prompts you to specify whether one of the configured NMS is Prime Central. If it is Prime Central, the script accepts the Prime Central database server details such as, Prime Central DB server IP, DB server listening port, DB user credentials (user-ID and password), and registers the Domain Manger for RMS in Prime Central.

To integrate RAN Management System (RMS) with Prime Central, refer to the procedure in section **Integrating FM, PMG, LUS, and RDU Alarms on Central Node with Prime Central NMS** in the Cisco RAN Management System Installation Guide, Release 5.1.

Integrating Cisco Prime Access Registrar (CPAR) with Prime Central

Step 1 From the **Fault Source Management** portlet, click **Add** to add the Fault Source details.
The **Add New Fault Source** dialog box appears.

Step 2 Enter the **Fault Source Type** from the drop-down as **CAR** and specify the Fault Source details in the appropriate fields.

Step 3 Click **OK**.
For more Information about how to add a Fault Source and the field descriptions, refer to the section **Adding a Fault Source** in the Prime central 2.1 User Guide.

Note After the CPAR Fault Source is added, CPAR is registered with Prime Central as a domain manager instance.

Configuring Prime Central as Trap Listener in CPAR to Receive Traps

Step 1 Login to CPAR server.

Step 2 Go to CPAR installation directory and change it to `/ucd-snmp/share/snmp` directory.

Step 3 Add the following command to **snmpd.conf** file.

trap2sink <<ip-addr-FM-Server>> public <FM-port>

Note The Prime Central Fault Management SNMP port is **1162**.

Step 4 To reflect the changes, enter the following command for restarting the CPAR server:

cd <CPAR installation directory>/bin

./arserver restart

Step 5 Check if the following options, in the path `/radius/advanced/snmp` (in aregcmd prompt), are enabled:

enabled = true

masteragent = true

Step 6 If the above options are not enabled, perform the following steps to enable these options:

a) Go to **<CPAR-Installation directory>/bin**.

b) Enter the following commands:

./aregcmd

cd /radius/advanced/snmp

set enabled true

set masteragent true

save

reload

Integrating Cisco Prime Network Registrar (CPNR) with Prime Central

Step 1 From the **Fault Source Management** portlet, click **Add** to add the Fault Source details.
The **Add New Fault Source** dialog box appears.

Step 2 Enter the Fault Source Type from the drop-down as **CNR** and specify the Fault Source details in the appropriate fields.

Step 3 Click **OK.**

For more Information about how to add a Fault Source and the field descriptions, refer to the section **Adding a Fault Source** in the . Prime Central 2.0 User Guide.

After the CPNR Fault Source is added, CPNR is registered with Prime Central as a domain manager instance.

Configuring Prime Central as Trap Listener in CPNR to Receive Traps

Step 1 Login to CPNR server.

Step 2 Go to CPNR installation directory and change it to `/local/usrbin` directory.

Step 3 Enter the following command:

./nrcmd

Step 4 Provide the CPNR user credentials.
The **nrcmd** prompt appears

Step 5 Execute the following command to add an FM server as a trap recipient for CPNR:

nrcmd> trap-recipient <name> create ip-addr=<ip-addr-FM-Server> port-number=<portnumber of FM server

Note The Prime Central FM SNMP port is 1162.

Step 6 To reflect the changes, enter the following command for restarting the SNMP server:

nrcmd > snmp stop

nrcmd > snmp start

Integrating SpiderNet with Prime Central

Step 1 From the **Fault Source Management** portlet, click **Add** to add the Fault Source details.
The **Add New Fault Source** dialog box appears.

Step 2 Enter the **Fault Source Type** from the drop-down as **SpiderCloud** and specify the Fault Source details in the appropriate fields.

Step 3 Click **OK**.
For more Information about how to add a Fault Source and the field descriptions, refer to the section **Adding a Fault Source** in the Prime Central 2.0 User Guide

After the SpiderNet Fault Source is added, SpiderNet is registered with Prime Central as a domain manager instance.

Note If SpiderNet is in HA mode, add two fault sources for standby and active IP addresses respectively.

eRMS is integrated only with Primary Prime Central because eRMS has to be integrated from Prime Central GUI. The integration of eRMS is done with secondary Prime Central after the switchover.

Configuring Prime Central as Trap Listener in SpiderNet to Receive Traps

Step 1 Login to SpiderNet server GUI.

Step 2 Create a SNMP Managers Group:

a) Choose **Administration** > **Northbound Interface** > **New SNMP Manager Group**.

b) Enter Prime Central details:

- In **Port** field, enter 1162 port number.
- In **Host Names or IP Addresses** field, enter Prime Central FM server hostname or IP address.
- Select **Alarm Forwarding** checkbox and in **SNMP Version** choose V2C. In **Community**, enter Public.
- Uncheck **Enable the Heartbeat Trap** check box, as this trap is not supported in Prime Central.
- Click **OK**.

Step 3 Configure Events:

a) Choose **Administration** > **Fault Management** > **Events Configuration**.
b) Select **Forward to SNMP** check box and choose **Prime Central SNMP Manager** group in the drop-down.
c) Click **Save**.

Step 4 Configure a Trap Target:

a) Choose **Network Control** > **Services Nodes**. Right click on the required node, go to **Show Configuration** > **Advanced** > **System** > **Event Management** > **Target**. Right click on Target, and click **Add Target**.

- Provide **Target Index** and click **OK**.
- Select **SNMP Trap** in newly created index and enable **SNMP Trap**. In **IP Address** field, enter Management Server IP Address.
- Click **Save**.