



Cisco Prime IP Express 9.0 Installation Guide

First Published: 2016-12-22

Last Modified: 2018-09-11

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Installation Overview	1
	Overview	1
	About Cisco Prime IP Express	1

CHAPTER 2	Configuration Options	3
	Mixed DHCP and DNS Scenarios	3
	One-Machine Mixed Configuration	3
	Two-Machine Mixed Configuration	3
	Three-Machine Mixed Configuration	4
	Four-Machine Mixed Configuration	4
	DHCP-Only Scenarios	4
	One-Machine DHCP Configuration	5
	Two-Machine DHCP Configuration	5
	DNS-Only Scenarios	5
	One-Machine DNS Configuration	5
	Two-Machine DNS Configuration	5
	Three-Machine DNS Configuration	5

CHAPTER 3	Installation Requirements	7
	System Requirements	7
	Recommendations	9
	Installation Modes	9
	License Files	9

CHAPTER 4	Preparing for the Installation	13
	Installation Checklist	13

Before You Begin 14

Obtaining Cisco Prime IP Express License Files 14

Running Other Protocol Servers 15

Backup Software and Virus Scanning Guidelines 15

Server Event Logging 16

Modifying ACLs in Windows Installations 16

CHAPTER 5 **Installing and Upgrading Cisco Prime IP Express 17**

Installing Cisco Prime IP Express 17

 Upgrading on Windows 23

 Upgrading on Linux 24

Reverting to an Earlier Product Version 24

Moving an Installation to a New Machine 26

Moving a Regional Cluster to a New Machine 26

Troubleshooting the Installation 27

Troubleshooting Local Cluster Licensing Issues 28

CHAPTER 6 **Next Steps 31**

Starting Cisco Prime IP Express 31

Starting and Stopping Servers 32

 Starting and Stopping Servers on Windows 32

 Starting and Stopping Servers on Linux 32

 Starting or Stopping Servers using the Local Web UI 33

Starting and Stopping Servers using the Regional Web UI 33

CHAPTER 7 **Uninstalling Cisco Prime IP Express 35**

Uninstalling on Windows 35

Uninstalling on Linux 36

Running Performance Monitoring Software on Windows 36

CHAPTER 8 **Cisco Prime IP Express Virtual Appliance 37**

System Requirements 37

Installing and Upgrading Cisco Prime IP Express Virtual Appliance 38

 Preparing to Deploy the Cisco Prime IP Express Virtual Appliance 38

Deploying the Regional Cluster OVA or Local Cluster OVA on VMware	39
Booting and Configuring Cisco Prime IP Express Virtual Appliance	40
Deploying the Regional Cluster or Local Cluster on a KVM Hypervisor	41
Deploying the Regional Cluster or Local Cluster on OpenStack	42
Upgrading the Cisco Prime IP Express Virtual Appliance	43
Upgrading a Cisco Prime IP Express Installation to run on a Cisco Prime IP Express Virtual Appliance	43
Upgrading to a new Version of the Virtual Appliance Operating System	45
Upgrading the Cisco Prime IP Express Application	45
Next Steps: Cisco Prime IP Express Virtual Appliance	45
Configuring Cisco Prime IP Express with the CLI on Virtual Appliance	45
Configuring the Virtual Appliance to Automatically Power Up	46
Managing the Cisco Prime IP Express Virtual Appliance	47

APPENDIX A	Performing a Silent Installation	49
	Performing a Silent Installation	49

APPENDIX B	Lab Evaluation Installations	53
	Lab Evaluation Installations	53
	Installing Cisco Prime IP Express in a Lab	53
	Testing the Lab Installation	54
	Uninstalling in a Lab Environment	54

APPENDIX C	Installing the Cisco Prime IP Express SDK	55
	Installing on Linux	55
	Installing on Windows	56
	Testing Your Installation	56
	Compatibility Considerations	56

APPENDIX D	Enhancing Security for Web UI	59
	Enhancing Security for Web UI	59

APPENDIX E	Hardening Guidelines	61
	Hardening Guidelines	61

APPENDIX F

Configuring Network Access on CentOS 7.2 using nmcli 63

Configuring Network Access on CentOS 7.2 using nmcli 63



CHAPTER 1

Installation Overview

This chapter contains the following sections:

- [Overview, on page 1](#)
- [About Cisco Prime IP Express, on page 1](#)

Overview

This guide describes how to install Cisco Prime IP Express Release 9.0 on Windows and Linux operating systems, and how to install the Cisco Prime IP Express Virtual Appliance. You can also see the following documents for important information about configuring and managing Cisco Prime IP Express:

- For configuration and management procedures for Cisco Prime IP Express and Cisco Prime IP Express Virtual Appliance, see the *Cisco Prime IP Express 9.0 Administrator Guide*.
- For details about commands available through the command line interface (CLI), see the *Cisco Prime IP Express 9.0 CLI Reference Guide*.

About Cisco Prime IP Express

Cisco Prime IP Express is a network server suite that automates managing enterprise IP addresses. It provides a stable infrastructure that increases address assignment reliability and efficiency.

- Dynamic Host Configuration Protocol (DHCP) server
- Domain Name System (DNS) server
- Caching Domain Name System (CDNS) server
- Simple Network Management Protocol (SNMP) server

You can control these servers by using the Cisco Prime IP Express web-based user interface (web UI) or the command line interface (CLI). These user interfaces can also control server clusters that run on different platforms.

You can install Cisco Prime IP Express in either local or regional mode:

- Local mode is used for managing local cluster protocol servers.
- Regional mode is used for managing multiple local clusters through a central management model.

A regional cluster centrally manages local cluster servers and their address spaces. The regional administrator can perform the following operations:

- Manage licenses for Cisco Prime IP Express. An installation must have at least one regional cluster for license management purposes.
- Push and pull configuration data to and from the local DNS and DHCP servers.
- Obtain subnet utilization and IP lease history data from the local clusters.



CHAPTER 2

Configuration Options

Cisco Prime IP Express DHCP, Authoritative DNS, and Caching DNS components are licensed and managed from the regional server. You need to have a regional server and all services in the local clusters are licensed through the regional cluster. Only a regional install asks for a license file and only the regional server accepts new license files. Then the regional server can authorize individual local clusters based on available licenses.

The sample configuration shown in this chapter is based on the typical use cases described in the following sections:

- [Mixed DHCP and DNS Scenarios, on page 3](#)
- [DHCP-Only Scenarios, on page 4](#)
- [DNS-Only Scenarios, on page 5](#)

Mixed DHCP and DNS Scenarios

You can set up Cisco Prime IP Express for a mixed DHCP and DNS configuration with different numbers of machines.

One-Machine Mixed Configuration

Configure both DHCP and Auth DNS servers on a single machine, initially enabling the servers as primaries, and enabling the SNMP traps. Then configure at least one forward zone and corresponding reverse zone, at least one scope.

Configure both DHCP and Caching DNS servers on a single machine, initially enabling the servers as primaries, and enabling the SNMP traps. Then you can configure forwarders and exception lists.

Two-Machine Mixed Configuration

A mixed DHCP configuration on two machines offers a few alternatives:

- Configure one machine as primary DHCP and Auth DNS server, and the second machine as a secondary Auth DNS server. Then configure a zone distribution and DNS access controls on the first machine and optionally access controls on the second machine.
- Configure one machine as DHCP and Auth DNS main servers and the second machine as DHCP and Auth DNS backup servers. Perform minimal configuration on the backup machine (changing the password,

enabling DHCP and Auth DNS, and selecting partner backup roles). On the main machine, build the configuration, creating server pairs and scheduling synchronization tasks with the backup machine.

- Configure one machine as a DHCP server and the second machine as a Auth DNS primary then configure either machine with DNS Update and push the configuration to the other machine.
- Configure one machine with both DHCP server and Auth DNS server and the second machine as a Caching DNS server with the Auth DNS server as the Forwarder.

Three-Machine Mixed Configuration

A mixed configuration on three machines offers a few additional alternatives:

- Configure one machine as a DHCP server, the second machine as an Auth DNS primary, and the third machine as an Auth DNS secondary. Optionally revisit the machines to make the DHCP main the Auth DNS backup, and make the Auth DNS main the DHCP backup.
- Configure one machine as DHCP failover and Auth DNS High-Availability (HA) main servers, the second machine as DHCP failover and Auth DNS HA backup servers, and the third machine as a Auth DNS secondary server.
- Configure one machine as a DHCP server, the second machine as the Auth DNS server and the third machine as a Caching DNS, with the Auth DNS as the Forwarder.
- Configure one machine as a DHCP primary server and Auth DNS primary, the second machine as a DHCP secondary and Auth DNS secondary server and the third machine as a Caching DNS, with the primary Auth DNS of the first machine as the Forwarder.

Four-Machine Mixed Configuration

A mixed configuration on four machines could include:

- DHCP and Auth DNS main and backup pairs, with the first machine as a DHCP main, the second machine as a DHCP backup, the third machine as an Auth DNS main configured with DNS Update, and the fourth machine as an Auth DNS backup.
- An add-on to the three-machine scenario, with the first machine as a DHCP main, the second machine as an Auth DNS main, the third machine as DHCP and Auth DNS backups, and the fourth machine as an Auth DNS secondary.
- Configure the first machine as DHCP main, second machine as DHCP backup, third machine as Auth DNS, and Caching in fourth, with Auth DNS as Forwarder.

DHCP-Only Scenarios

A DHCP-only configuration could be on a single machine or two machines.

One-Machine DHCP Configuration

Initially configure only DHCP, skip the class-of-service and failover options, and revisit the setup to enable class-of-service and policy options.

Two-Machine DHCP Configuration

Configure the first machine as a DHCP main and the second machine as a backup, with minimal backup configuration (changing password, enabling DHCP, and selecting the backup role), and set up the first machine with failover load balancing, optionally scheduling failover synchronization tasks.

DNS-Only Scenarios

A DNS-only configuration could be on one, two, or three machines.

One-Machine DNS Configuration

Initially configure DNS as an Auth primary, Auth secondary, or caching server.

Two-Machine DNS Configuration

Configure the first machine as an Auth DNS primary and the second machine as a secondary, or the first machine as a main primary and the second machine as a backup primary.

Configure the first machine as an Auth DNS and the second machine as Caching DNS.

Three-Machine DNS Configuration

Configure the first machine as an Auth DNS main primary, the second machine as a backup primary, and the third machine as a secondary server.

Configure the first machine as Auth DNS primary, the second machine as secondary, and the third machine as Caching DNS.



CHAPTER 3

Installation Requirements

This chapter contains the following sections:

- [System Requirements, on page 7](#)
- [Installation Modes, on page 9](#)
- [License Files, on page 9](#)

System Requirements

Review the system requirements before installing the Cisco Prime IP Express 9.0 software:

- **Java**—You must have the Java Runtime Environment (JRE) 1.7 or later, or the equivalent Java Development Kit (JDK) installed on your system. (The JRE is available from Oracle on its website.)
- **Operating system**—We recommend that your Cisco Prime IP Express machine run on the Windows or Linux operating systems as described in the server minimum requirements table below. Cisco Prime IP Express is supported on 64-bit operating systems.

Cisco Prime IP Express supports running in VMWARE ESXi 5.5 or later environment.



Note For the 64-bit Linux kit, Cisco Prime IP Express applications are 64-bit executable programs and require the 64-bit operating system and applications (Java JRE/JDK, OpenLDAP library).

- **User Interface**—Cisco Prime IP Express currently includes two user interfaces: a web UI and a CLI:
 - The web UI has been tested on Microsoft Internet Explorer 9, Mozilla Firefox 21 later and Google Chrome. Internet Explorer 8 is not supported.
 - The CLI runs in a Windows or Linux command window.



Tip Include a network time service in your configuration to avoid time differences between the local and regional clusters. This method ensures that the aggregated data at the regional server appears consistently. The maximum allowable time drift between the regional and local clusters is five minutes. If the time skew exceeds five minutes, then the installation process will not be able to correctly register the server with the regional. In this case, unset and set the password on the regional cluster, and sync again.

Table 1: Cisco Prime IP Express Server Minimum Requirements

Component	Operating System	
	Linux	Windows
OS version ¹	Red Hat Enterprise Linux ES 6.5, CentOS 7.2 ²	Windows Server 2012 R2 ³
Disk space ⁴	With basic DHCP and optimal hardware configuration: <ul style="list-style-type: none"> • For expected peak load between 500 and 1000 DHCP leases per second, 7500 RPM SATA⁵ drives are recommended. • For expected peak load above 1000 DHCP leases per second, 15000 RPM SAS drives are recommended. Recommended hard drive-146 GB 	
Memory ⁶	Small networks-8 GB, Average networks-16 GB, or Large networks-32 GB	

¹ Cisco Prime IP Express is supported on 64-bit operating systems. We highly recommend customers move to a 64-bit operating system.

² Cisco Prime IP Express 9.0 supports Red Hat Enterprise Linux ES 6.5, running standalone or on VMWare (ESX Server 5.5 or later) on Cisco Unified Computing System (CUCS) and other hardware supported by VMWare.

³ Cisco Prime IP Express 9.0 supports Windows Server 2012 R2, running standalone or on VMWare (ESX Server 5.5 or later) on Cisco Unified Computing System (CUCS) and other hardware supported by VMWare.

⁴ Higher I/O bandwidth usually results in higher average leases per second.

⁵ Serial Advanced Technology Attachment (Serial ATA).

⁶ Faster CPU and more memory typically result in higher peak leases per second.

System Requirements for Linux OS (RH 6.5 and CentOS 7.2)

To run Cisco Prime IP Express (64-bit kit) on Red Hat Enterprise Linux ES 6.5 (64-bit), ensure that the Java Runtime Environment (JRE) (64-bit) is installed along with the dependencies. The Linux OS has the following packages. To support External Authentication using AD and GSS TSIG features ensure installation of the following:

- krb5-libs
- cyrus-sasl-gssapi

Recommendations

When Cisco Prime IP Express is deployed on virtual machines, review the following recommendations:

- Do NOT deploy HA DNS or DHCP failover partners on the same physical server (in separate VMs). This will not provide high availability when the server goes down. Ideally, the high available/failover partners should be sufficiently "separate" that when one fails (because of a hardware, power, networking failure), the other does not.
- When deploying multiple CPIPE VMs on the same physical server (or servers served by a common set of disk resources), you should stagger the automatic nightly shadow backups (by default, they occur at 23:45 in the server's local time). To know how to alter this time, see the *"Setting Automatic Backup Time"* section in *Cisco Prime IP Express 9.0 Administrator Guide*.



Note It may be acceptable to not follow the above recommendations for lab environments; but they must be followed for production.

Installation Modes

The modes of installation that exist for the local and regional clusters are new installations and upgrades from a previous version. These installations or upgrades are performed by using operating system-specific software installation mechanisms:

- Windows—**InstallShield** setup program
- Linux—**install_cnr** script that uses Red Hat Package Manager

License Files

Cisco Prime IP Express uses the FLEXlm licensing tool. Your license file defines the features of Cisco Prime IP Express to which you have access. For Cisco Prime IP Express, the licensing is done according to the services that you require. The following are the types of licenses available:

- enterprise-system—Licenses the CCM services. This license is mandatory if you want to run Cisco Prime IP Express.
- enterprise-dhcp—Licenses DHCP services and, optionally, an initial count of leases
- enterprise-dns—Licenses authoritative DNS services and, optionally, an initial count of RRs
- enterprise-cdns—Licenses caching DNS services and, optionally, an initial count of servers
- enterprise-dhcp—Licenses an incremental number of active leases
- enterprise-dns—Licenses an incremental number of RRs
- enterprise-cdns—Licenses an incremental number of caching server instances

The different services provided by Cisco Prime IP Express are associated with the different license types as follows:

- CCM services—enterprise-system
- DHCP services—enterprise-dhcp and enterprise-dhcp
- Authoritative DNS services—enterprise-dns and enterprise-dns
- Caching DNS services—enterprise-system and enterprise-cdns



Note Licenses for Cisco Prime IP Express 8.x are not valid for Cisco Prime IP Express 9.x. You should have a new license for Cisco Prime IP Express 9.x.



Note You should have at least one enterprise license for a server to enable that service.

License management is done from the regional cluster when Cisco Prime IP Express is installed. You must install the regional server first, and load all licenses in the regional server. When you install the local cluster, it registers with regional to obtain its license.

When you install the regional, you are prompted to provide the license file. You can store the license file in any location provided the location and file are accessible during the installation.

The utilization of licenses are calculated by obtaining statistics from all the local clusters in the Cisco Prime IP Express system for all counted services (DHCP, DNS, and CDNS). The regional CCM server maintains the license utilization history for a predetermined time period.

Utilization is calculated for different services as:

- DHCP services—total number of active DHCP leases (including v4 and v6)
- Auth DNS services—the total number of DNS resource records (all RR types)
- Caching DNS services—total number of Caching DNS servers being run in the Cisco Prime IP Express system

The services on each local cluster will be restricted based on the services for which licenses are present.

When you configure DHCP failover, only simple failover is operational and supported (see Failover scenarios section in the Configuring DHCP Failover chapter of the *Cisco Prime IP Express 9.0 DHCP User Guide*).

To learn about obtaining the license files for Cisco Prime IP Express, see [Obtaining Cisco Prime IP Express License Files](#), on page 14.

Market Segment Specific Licensing

Cisco Prime IP Express license types are offered specific to market segments. Market specific licensing generates license keys for use by market segments, that is, Service Provider, Smart Grid, and so on. Cisco Prime IP Express features are enabled based on the market segment specific license you choose. For example, the PNR license offers features designed for the Service Provider market segment whereas the PNR-SG license offers features designed for the Smart Grid market segment.

Cisco Prime IP Express offers the following market segment specific licenses:

- Prime Network Registrar—PNR

- Prime Network Registrar Connected Grid—PNR-SG
- Prime IP Express—PNR-ENT



Note If the licenses for all market segments are installed, then only the PNR license will be active.

The regional server which uses the PNR-SG license can be converted to PNR by installing the PNR license. Local cluster licenses will be converted automatically at the next compliance check, or can be manually updated by resynchronizing the local cluster.

For a given market segment license, only the counts from corresponding market segment license will apply. For example, if the PNR count license is applied when the PNR-SG base license is active, the Right to Use count will not be updated. If the PNR-SG count license is applied when the PNR base license is active, the Right to Use count will not be updated.

PNR Licenses

The PNR license provides all the features available for the Cisco Prime Network Registrar release you install.

PNR-SG Licenses

The PNR-SG license disables the following PNR features which have been identified as not necessary for Smart Grid implementations:

- Tenants
- External Authentication

The DHCP service PNR-SG license offers you the PNR features with the exception of:

- Extensions
- Lightweight Directory Access Protocol (LDAP)
- TCP Listeners (Dynamic Lease Notification, Bulk leasequery, Active leasequery/Client Notification)
- Trivial File Transfer Protocol (TFTP)
- Regional lease history and subnet utilization
- BYOD

PNR-ENT Licenses

The Cisco Prime IP Express (PNR-ENT) license offers the following PNR features with the exception of (identified as not necessary for Enterprise market):

- Tenants
- TCP Listeners (DHCP Features - Dynamic Lease Notification, Bulk leasequery)
- Trivial File Transfer Protocol (TFTP)
- Regional subnet utilization history



CHAPTER 4

Preparing for the Installation

This chapter covers any tasks that you have to perform before installing Cisco Prime IP Express.

- [Installation Checklist, on page 13](#)
- [Before You Begin, on page 14](#)
- [Obtaining Cisco Prime IP Express License Files, on page 14](#)
- [Running Other Protocol Servers, on page 15](#)
- [Backup Software and Virus Scanning Guidelines, on page 15](#)
- [Server Event Logging, on page 16](#)
- [Modifying ACLs in Windows Installations, on page 16](#)

Installation Checklist

This section explains the procedures you must follow to install Cisco Prime IP Express.

Before you perform the installation or upgrade, ensure that you are prepared by reviewing this checklist:

Table 2: Installation Checklist

Task	Checkoff
Does my operating system meet the minimum requirements to support Cisco Prime IP Express 9.0? (See the System Requirements, on page 7 section.)	<input type="checkbox"/>
Does my hardware meet the minimum requirements? (See the System Requirements, on page 7 section.)	<input type="checkbox"/>
If necessary, have I excluded Cisco Prime IP Express directories and subdirectories from virus scanning? (See the section Backup Software and Virus Scanning Guidelines, on page 15 .)	<input type="checkbox"/>
On Windows, are other applications closed, including any virus-scanning or automatic-backup software programs? Is the Debugger Users group included in the Local Users and Groups?	<input type="checkbox"/>
Do I have the proper software license? (See the License Files, on page 9 section.)	<input type="checkbox"/>
Am I authorized for the administrative privileges needed to install the software?	<input type="checkbox"/>
Does the target installation server have enough disk space?	<input type="checkbox"/>
Is this a new installation or an upgrade?	<input type="checkbox"/>

Task	Checkoff
Is the cluster mode of operation regional or local?	<input type="checkbox"/>
Is this a full or client-only installation?	<input type="checkbox"/>
Is the Java Runtime Environment (JRE) 1.7 or later, or the equivalent Java Development Kit (JDK), installed on the system? If so, where?	<input type="checkbox"/>
Should the web UI use an HTTP or HTTPS connection, or both?	<input type="checkbox"/>
Am I upgrading from an earlier version of Cisco Prime IP Express? If so:	<input type="checkbox"/>
<ul style="list-style-type: none"> • Are there any active user interface sessions? 	<input type="checkbox"/>
<ul style="list-style-type: none"> • Is my database backed up? 	<input type="checkbox"/>
<ul style="list-style-type: none"> • Am I upgrading from a supported version (Cisco Prime IP Express 8.2 and later)? 	<input type="checkbox"/>

Before You Begin

Verify that you are running a supported operating system and that your environment meets all other current system requirements (see [System Requirements, on page 7](#)).

To upgrade the operating system:

1. Use the currently installed Cisco Prime IP Express release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.
2. Back up your database. The installation program tries to detect configuration data from an earlier installation and will upgrade the data.
3. Upgrade your operating system.

Obtaining Cisco Prime IP Express License Files

When you purchase Cisco Prime IP Express 9.0, you receive a FLEXlm license file in an e-mail attachment from Cisco, after you register the software.

You must copy the license file to a location which will be accessible during the regional cluster installation before you attempt to install the software. The installation process will ask you for the location of the license file.

To obtain a license file:

1. Read the Software License Claim Certificate document packaged with the software.
2. Note the Product Authorization Key (PAK) number printed on the certificate.
3. Log into one of the websites described on the certificate, and follow the registration instructions. The PAK number is required for the registration process.

You should receive the license file through e-mail within one hour of registration.

A typical license file might look like:

```
INCREMENT base-system cisco 9.0 permanent uncounted \
VENDOR_STRING=<Count>1</Count> HOSTID=ANY \
NOTICE="<LicFileID>20110919130037832</LicFileID><LicLineID>4</LicLineID> \
<PAK></PAK><CompanyName></CompanyName>" SIGN=521EA9F0925C
```

Running Other Protocol Servers

You cannot run the Cisco Prime IP Express DNS, CDNS, or DHCP servers concurrently with any other DNS or DHCP servers. If the Cisco Prime IP Express installation process detects that a conflict exists, it displays a warning message.

On Windows systems, use one of the following methods to change the configuration from the Service Control Manager:

- Stop the Cisco Prime IP Express protocol server that conflicts with the Microsoft protocol server by using the Stop function in one of the user interfaces.
- Change the Microsoft servers from a Startup Type of Automatic to Manual or Disabled.

If you want to disable a protocol server and prevent the Cisco Prime IP Express server from starting automatically after a system reboot, use the **server {dns | cdns | dhcp} disable start-on-reboot** command in the CLI.

Backup Software and Virus Scanning Guidelines

If you have automatic backup or virus scanning software enabled on your system, exclude the Cisco Prime IP Express directories and their subdirectories from being scanned. If they are not excluded, file locking issues can corrupt the databases or make them unavailable to the Cisco Prime IP Express processes. If you are installing on the default locations, exclude the following directories and their subdirectories:



Note In this documentation set, when *install-path* is used, it refers to all or part of the installation paths that were specified when installing Cisco Prime IP Express. As an example using the Linux default local cluster paths of `/opt/nwreg2/local` and `/var/nwreg2/local`, the *install-path* may represent these paths.

- Windows—
 - install-path*\data (for example, `C:\CiscoPrimeIPExpress\Local\data` and `C:\CiscoPrimeIPExpress\Regional\data`)
 - install-path*\logs (for example, `C:\CiscoPrimeIPExpress\Local\logs` and `C:\CiscoPrimeIPExpress\Regional\logs`)
- Linux—

install-path/data (for example, */var/nwreg2/local/data* and */var/nwreg2/regional/data*)

install-path/logs (for example, */var/nwreg2/local/logs* and */var/nwreg2/regional/logs*)

Server Event Logging

System activity begins logging when you start Cisco Prime IP Express. The server maintains all the logs by default in the following directories:

- Windows—Local cluster: *C:\CiscoPrimeIPExpress\Local\logs*;
Regional cluster: *C:\CiscoPrimeIPExpress\Regional\logs*
 - Linux—Local cluster: */var/nwreg2/local/logs*;
Regional cluster: */var/nwreg2/regional/logs*
- To monitor the logs, use the **tail -f** command.



Caution

In Windows, to avoid losing the most recent system Application Event Log entries if the Event Log fills up, use the Event Viewer system application and check the **Overwrite Events as Needed** check box in Event Log Settings for the Application Log. If the installation process detects that this option is not set properly, it displays a warning message advising corrective action.

Modifying ACLs in Windows Installations

The Cisco Prime IP Express installation program for Windows does not try to modify ACLs to restrict access to the installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities—**cacls** and **icacls**—to manually change file and directory permissions.

If you decide to manually change ACLs, we recommend that you control the settings so that the contents of the entire installation area are read-only to everyone except those in the Administrators system group.

The following files and sub directories contain data that you may want only the Administrators system group to access:

- *installdir\conf\cnr.conf*
- *installdir\tomcat\conf\server.xml*
- *installdir\conf\priv*
- *installdir\data*

Modifying the ACLs is strictly optional, and Cisco Prime IP Express will function normally without making any changes to them. See the documentation supplied by Microsoft for information about how to use the **cacls** and **icacls** utilities.



CHAPTER 5

Installing and Upgrading Cisco Prime IP Express

This chapter contains the following sections:

- [Installing Cisco Prime IP Express, on page 17](#)
- [Reverting to an Earlier Product Version, on page 24](#)
- [Moving an Installation to a New Machine, on page 26](#)
- [Moving a Regional Cluster to a New Machine, on page 26](#)
- [Troubleshooting the Installation, on page 27](#)
- [Troubleshooting Local Cluster Licensing Issues, on page 28](#)

Installing Cisco Prime IP Express



Note If using the Authoritative or Caching DNS server, assure that connection tracking (contrack) is not being used. For more information, see the *"Firewall Considerations" section in Cisco Prime IP Express 9.0 Administration Guide*.

Step 1 Log into the target machine using an account that has administrative privileges:

- Windows—Account in the Administrators group
- Linux—**su** (superuser) or root account

Windows—Close all open applications, including any antivirus software.

Step 2 Download and install the Java Runtime Environment (JRE) 1.7 or later, or the equivalent Java Development Kit (JDK), if you have not already done so. These are available from the Oracle website.

Note On Windows, add the full path of the bin subdirectory of your Java installation folder to your PATH environment variable; for example, C:\Program Files (x86)\Java\jdk1.7\bin.

Step 3 If you are not configuring secure login to the web UI, skip to **Step 4**. If you are configuring secure login, you must create a keystore file by using the Java **keytool** utility, which is located in the bin subdirectory of the Java installation (see **Step 2**). Use the utility to define a self-signed certificate, or to request and later import a certificate from an external signing authority:

- a) To create a keystore file containing a self-signed certificate, run this command and respond to the prompts:

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore k-file
Enter keystore password: password
What is your first and last name? [Unknown]: name
What is the name of your organizational unit? [Unknown]: org-unit
What is the name of your organization? [Unknown]: org-name
What is the name of your City or Locality? [Unknown]: local
What is the name of your State or Province? [Unknown]: state
What is the two-letter country code for this unit? [Unknown]: cc
Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc correct? [no]: yes
Enter key password for <tomcat> (RETURN if same as keystore password):
```

The keystore filename (k-file) is its fully qualified path. You will be entering the keystore path and password in **Step 16**.

Note You must use 128-bit SSL to disable weak ciphers in the web UI. For more information, see [Enhancing Security for Web UI, on page 59](#).

- b) To create a Certificate Signing Request (CSR) that you will submit to the Certificate Authority (CA) when you request a certificate, create the keystore file as in the previous substep, then execute this command:

```
> keytool -certreq -keyalg RSA -alias tomcat -file certreq.cer -keystore k-file
```

Submit the resulting certreq.cer file to the CA. Once you receive the certificate from the CA, first download the Chain Certificate from the CA, then import the Chain Certificate and your new Certificate into the keystore file, as follows:

```
> keytool -import -alias root -keystore k-file -trustcacerts -file chain-cert-file
> keytool -import -alias tomcat -keystore k-file -trustcacerts -file new-cert-file
```

For details on the **keytool** utility, see the documentation at the Java website of Oracle. For details on the **keystore** file and Tomcat, see the documentation at the website of the Apache Software Foundation.

Caution The Cisco Prime IP Express installation program for Windows does not try to modify ACLs to restrict access to the installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities to manually change file and directory permissions. See [Modifying ACLs in Windows Installations, on page 16](#).

Step 4

Load the installation CD, or browse to the network resource where the Cisco Prime IP Express software is located. If you download a distribution file from the Cisco website, run it from a different directory than where you will install Cisco Prime IP Express.

- Windows—The `pipe_version-windows.exe` file is a self-extracting executable file that places the setup file and other files in the directory where you run it. (If you are not configured for Autostart, run the setup.exe file in that directory.) The Welcome to Cisco Prime IP Express window appears.

Click **Next**. The second welcome window introduces the setup program and reminds you to exit all current programs, including virus scanning software. If any programs are running, click **Cancel**, close these programs, and return to the start of **Step 4**. If you already exited all programs, click **Next**.

- **Linux**—Be sure that the **gzip** and **gtar** utilities are available to uncompress and unpack the Cisco Prime IP Express installation files. See the GNU organization website for information on these utilities. Do the following:

1. Download the distribution file.
2. Navigate to the directory in which you will uncompress and extract the installation files.
3. Uncompress and unpack the .gtar.gz file. Use **gtar** with the **-z** option:

```
gtar -zxpf cpipe_9_0-linux-x86_64.gtar.gz
or
gtar -zxpf cpipe_9_0-linux-i686.gtar.gz
```

To unpack the .gtar file that **gunzip** already uncompressed, omit the **-z** option:

```
gtar -xpf cpipe_9_0-linux-i686.gtar
```

The command creates the *cpipe_9_0* directory into which the Cisco Prime IP Express installation files are extracted.

4. Run the following command or program:

- **Linux**—Run the `install_cnr` script from the directory containing the installation files:

```
# ./install_cnr
```

The `install-path` is the CD-ROM directory that contains the installation files or the directory that contains the extracted Cisco Prime IP Express installation files, if they were downloaded electronically.

Step 5

Specify whether you want to install Cisco Prime IP Express in the local or regional cluster mode (see [About Cisco Prime IP Express, on page 1](#)):

Note Since a regional server is required for license management, install the regional server first so that you can register the local to the regional. If you face any problem with synchronizing the regional cluster to the local cluster after registration, unset and set the password on the regional cluster, and sync again.

Tip Include a network time service in your configuration to avoid time differences between the local and regional clusters. This method ensures that the aggregated data at the regional server appears consistently. The maximum allowable time drift between the regional and local clusters is five minutes. If the time skew exceeds five minutes, then the installation process will not be able to correctly register the server with the regional. In this case, unset and set the password on the regional cluster, and sync again.

- **Windows**—Keep the default Cisco Prime IP Express Local or choose Cisco Prime IP Express Regional. Click **Next**. The Select Program Folder appears, where you determine the program folder in which to store the program shortcuts in the Start menu. Accept the default, enter another name, or choose a name from the Existing Folders list. Click **Next**.

- **Linux**—Enter **1** for a local, or **2** for regional. The default mode is 1.

Step 6

On Linux, specify if you want to run Cisco Prime IP Express Local Server Agent as a non-root *nradmin* user. If you choose to run Cisco Prime IP Express for a non-root user, a user *nradmin* is created with the requisite privileges to run the Cisco Prime IP Express services. When running Cisco Prime IP Express as a non-root user (*nradmin*), some changes occur in the CLI operation of the product. Though it is still possible to run as root, it is not recommended. Instead,

create regular Linux users and add them to the *nradmin* group. Users in this group will have full access to the Cisco Prime IP Express files. To start and stop Cisco Prime IP Express, these users may use the new `cnr_service` program in the path which is in `<install directory>/bin/cnr_service`.

Note The root user is only needed for installation and uninstallation.

Step 7

Note these Cisco Prime IP Express installation default directories and make any appropriate changes to meet your needs:

Note The installation directory path with spaces is not supported on non-Windows platforms and not recommended on Windows (except for the "Program Files" path).

Note If you are upgrading, the upgrade process autodetects the installation directory from the previous release.

Windows default locations:

Caution Do not specify the *\Program Files (x86)* or *\Program Files* or *\ProgramData* for the location of the Cisco Prime IP Express data, logs, and temporary files. If you do this, the behavior of Cisco Prime IP Express may be unpredictable because of Windows security.

- Local cluster
 - Program files (64-bit OS)—C:\Program Files (x86)\Cisco Prime IP Express\Local
 - Data files—C:\CiscoPrimeIPExpress\Local\data
 - Log files—C:\CiscoPrimeIPExpress\Local\logs
 - Temporary files—C:\CiscoPrimeIPExpress\Local\temp
- Regional cluster
 - Program files (64-bit OS)—C:\Program Files (x86)\Cisco Prime IP Express\Regional
 - Data files—C:\CiscoPrimeIPExpress\Regional\data
 - Log files—C:\CiscoPrimeIPExpress\Regional\logs
 - Temporary files—C:\CiscoPrimeIPExpress\Regional\temp

Linux default locations:

- Local cluster
 - Program files— /opt/nwreg2/local
 - Data files— /var/nwreg2/local/data
 - Log files— /var/nwreg2/local/logs
 - Temporary files— /var/nwreg2/local/temp
- Regional cluster
 - Program files— /opt/nwreg2/regional
 - Data files— /var/nwreg2/regional/data

- Log files— /var/nwreg2/regional/logs
- Temporary files— /var/nwreg2/regional/temp

Step 8 If there are no defined administrators, create an administrator by providing the username and password. You have to confirm the password entered.

If you are installing a regional, continue; else go to **Step 10**.

Step 9 Enter the filename, as an absolute path, for your base license see the "License Files" section.

Note Ensure that you use the absolute path and not a relative path for your base license as there are chances that there might be changes to the default path from what you started the install with.

Entering the filename during installation is optional. However, if you do not enter the filename now, you must enter it when you first log into the web UI or CLI.

Note If you install Cisco Prime IP Express using a Remote Desktop Connection to the Windows Server, you will not be able to enter the license information during the installation. Cisco Prime IP Express will reject the licenses as invalid. You must therefore skip the license information step, and add the license after the installation completes, using either the web UI or CLI. See [Starting Cisco Prime IP Express, on page 31](#) for details.

Step 10 Register the local to the regional by providing the regional IPv4 or IPv6 address and SCP port.

After the local is registered to the regional, it can provide those services for which the licenses are present in the regional.

Note If you face any problem synchronizing the regional cluster to the local cluster after registration, unset and set the password on the regional cluster, and sync again. This can happen due to time skew of more than five minutes between local and regional clusters.

Include a network time service in your configuration to avoid time differences between the local and regional clusters. This method ensures that the aggregated data at the regional server appears consistently. The maximum allowable time drift between the regional and local clusters is five minutes. If the time skew exceeds five minutes, then the installation process will not be able to correctly register the server with the regional. In this case, unset and set the password on the regional cluster, and sync again.

Step 11 After you register local to the regional, you can select the required services from the licensed services.

Note If a service is not selected, upgrade process will use the existing configuration. To remove a service wait until the upgrade process is completed.

Step 12 Choose whether to archive the existing binaries and database in case this installation does not succeed. The default and recommended choice is **Yes** or **y**:

If you choose to archive the files, specify the archive directory. The default directories are:

- Windows—Local cluster (*C:\CiscoPrimeIPExpress\Local.sav*); Regional cluster (*C:\CiscoPrimeIPExpress\Regional.sav*). Click **Next**.
- Linux—Local cluster (*/opt/nwreg2/local.sav*); Regional cluster (*/opt/nwreg2/regional.sav*)

Step 13 Choose the appropriate installation type: server and client (the default), or client-only:

- Windows—Choose **Both server and client (default)** or **Client only**. Click **Next**. The Select Port window appears.

- Linux—Entering **1** installs the server and client (the default), or **2** installs the client only.

Note Choose **Client only** in a situation where you want the client software running on a different machine than the protocol servers. Be aware that you must then set up a connection to the protocol servers from the client.

Step 14 Enter CCM management SCP port number that the server agent uses for internal communication between servers. The default value is 1234 for local cluster and 1244 for regional cluster.

Step 15 Enter the location of the Java installation (JRE) 1.7 or JDK selected in **Step 2**. (The installation or upgrade process tries to detect the location.):

- Windows—A dialog box reminds you of the Java requirements. Click **OK** and then choose the default Java directory or another one. Click **OK**. The Select Connection Type window appears.
- Linux—Enter the Java installation location.

Note Do not include the bin subdirectory in the path. If you install a new Java version or change its location, rerun the Cisco Prime IP Express installer then specify the new location in this step.

Step 16 Choose whether to enable the web UI to use a nonsecure (HTTP) or secure (HTTPS) connection for web UI logins:

- Windows—Choose **Non-secure/HTTP (default)**, **Secure/HTTPS (requires JSSE)**, or **Both HTTP and HTTPS**.
- Linux—Enter **1** for Non-secure/HTTP (default), **2** for Secure/HTTPS (requires JSSE), or **3** for both HTTP and HTTPS.

Enabling the secure HTTPS port configures security for connecting to the Apache Tomcat web server (see **Step 3** for configuration). (To change the connection type, rerun the installer, and then make a different choice at this step.)

- If you choose HTTPS, or HTTP and HTTPS, click **Next** and continue with **Step 17**.
- If you choose the default HTTP connection, click **Next**, and go to **Step 18**.

Step 17 If you enabled HTTPS web UI connectivity, you are prompted for the location of the necessary keystore and keystore files:

- For the keystore location, specify the fully qualified path to the keystore file that contains the certificate(s) to be used for the secure connection to the Apache Tomcat web server. This is the keystore file that you created in **Step 3**.
- For the keystore password, specify the password given when creating the keystore file. On Windows, click **Next**.

Caution Do not include a dollar sign (\$) in the keystore password as it will result in an invalid configuration on the Apache Tomcat web server.

Step 18 Enter a port number for the web UI connection. The defaults are:

- HTTP local cluster—8080
- HTTP regional cluster—8090
- HTTPS local cluster—8443
- HTTPS regional cluster—8453

On Windows, click **Next**.

- Step 19** Choose **Yes** if you want to enable the Cisco Prime IP Express web services.
- Step 20** Select the security mode to be configured. **Optional. Allow fallback to unsecure connection** is selected by default. Click **Next**.
- Step 21** If you are installing a regional, select **Yes** to enable BYOD service.
- The Cisco Prime IP Express installation process begins. Status messages report that the installer is transferring files and running scripts. This process may take a few minutes:
- Windows—The Setup Complete window appears. Choose **Yes, I want to restart my computer now** or **No, I will restart my computer later**, and then click **Finish**.
 - Linux—Successful completion messages appear.
- Note** When you upgrade Cisco Prime IP Express, the upgrade process takes place during the installation. Therefore, the installation and upgrade processes take a longer time depending on the number of scopes, prefixes, and reservations that you have configured.
- Step 22** Verify the status of the Cisco Prime IP Express servers:
- Windows—In the Services control panel, verify that the Cisco Prime IP Express Local Server Agent or Cisco Prime IP Express Regional Server Agent is running after rebooting the system when the installation has completed successfully.
 - Linux—Use the `install-path/usrbin/cnr_status` command to verify status. See [Starting and Stopping Servers, on page 32](#).
- If the upgrade fails, you can revert to the earlier Cisco Prime IP Express version. For details about reverting to the earlier version, see the [Reverting to an Earlier Product Version, on page 24](#).

Upgrading on Windows

To upgrade to Cisco Prime IP Express 9.0:

-
- Step 1** Ensure that your environment meets the current system requirements (see [System Requirements, on page 7](#)).
- Step 2** Use the currently installed release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.
- Step 3** Uninstall the previous version of Cisco Prime IP Express. Your existing configuration data will remain in place after the uninstall.
- Step 4** Back up your Cisco Prime IP Express data on a different machine or a shared network device and upgrade your operating system to Windows Server 2012 R2. See documentation supplied by Microsoft for information about how to install/upgrade Windows servers.
- Note** If you install Windows Server 2012 R2 instead of upgrading and the disk is reformatted, you must restore the Cisco Prime IP Express data to the `C:\MPEXpress\{Local | Regional}\data` folder.
- Step 5** Install Cisco Prime IP Express 9.0 on the Windows Server 2012 R2 machine. For installation instructions, see [Installing Cisco Prime IP Express, on page 17](#). Ensure that you specify the path where your existing data can be found, for example, `C:\CiscoPrimeIPExpress\{Local | Regional}`, to run the upgrade.

Note Ensure that you keep the old Cisco Prime IP Express configuration and license information handy as you may need to re-enter this information during the Cisco Prime IP Express installation.

We recommend upgrading the regional cluster before upgrading any local clusters, because an older version of a regional cluster cannot connect to newer local clusters.

Upgrading on Linux

To upgrade to Cisco Prime IP Express 9.0:

-
- Step 1** Ensure that your environment meets the current system requirements (see [System Requirements, on page 7](#)).
- Step 2** Use the currently installed release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.
- Step 3** Stop the Cisco Prime IP Express server agent and backup the current system (or at least install-path/data directories and contents). To stop the Cisco Prime IP Express Local/Regional server agent:
- If local—`/etc/init.d/nwreglocal stop`
 - If regional—`/etc/init.d/nwregregion stop`
- Step 4** Install Cisco Prime IP Express 9.0. For installation instructions, see the section "Installing and Upgrading Cisco Prime IP Express".
-

Reverting to an Earlier Product Version

The Cisco Prime IP Express installation program provides the capability to archive the existing product configuration and data when you upgrade to a newer version and to revert to an earlier version of the product. If you chose this option, and the upgrade process fails, use the following procedure to revert to the earlier product version and configuration:



Caution To complete this process, you must have access to the product installer and license key or license file for the earlier Cisco Prime IP Express version. Any attempt to proceed otherwise may destabilize the product.

If the installer had successfully performed the upgrade but you want to roll back to the earlier version at some later point, this procedure can result in network destabilization and data loss; for example, you will lose updates made to the Cisco Prime IP Express database after the upgrade, including DHCP lease data and DNS dynamic updates.

- Step 1** Verify that the archive directory that you specified during the upgrade process exists and is valid. These examples assume the default archive location provided during installation. Ensure that the path to the `cnr_data_archive` directory reflects the value of the archive directory that you specified during installation. If you are using:
- Windows—`C:\CiscoPrimeIPExpress\`

{Local.sav | Regional.sav}

- Linux—/opt/nwreg2/{local.sav | regional.sav}

Step 2 Uninstall Cisco Prime IP Express using the procedure described in the [Uninstalling Cisco Prime IP Express, on page 35](#).

Step 3 Other than the contents of the specified archive directory, delete any remaining files and directories in the Cisco Prime IP Express installation paths.

Step 4 Reinstall the original version of Cisco Prime IP Express. Ensure that you follow the reinstallation procedure described in *Cisco Prime IP Express Installation Guide* that is specific to the original product version.

Step 5 After the installation ends successfully, stop the Cisco Prime IP Express server agent:

- Windows—Local: **net stop nwreglocal**
Regional: **net stop nwregregion**
- Linux—Local: **/etc/init.d/nwreglocal stop**
Regional: **/etc/init.d/nwregregion stop**

Step 6 Delete the contents of the Cisco Prime IP Express install-path/data subdirectory.

Step 7 Extract the contents of the backup file to the reinstalled version of Cisco Prime IP Express.

- Change to the root directory of the filesystem. On Windows, this directory would be the base drive (such as C:); on Linux, it would be /.
- Using the fully qualified path to the archive directory, extract the archive. These examples assume the default archive location provided during installation.

- Windows—Copy the C:\CiscoPrimeIPExpress\{Local.sav|Regional.sav}\cnr_data_archive\ contents to the target Cisco Prime IP Express data directory. The following assume the default installation locations for a local cluster:

```
xcopy/s C:\CiscoPrimeIPExpress\Local.sav\cnr_data_archive
C:\CiscoPrimeIPExpress\Local\data\
```

Note There is also a cnr_file_archive directory which contains the installed files and generally this should not be recovered over a re-installation.

- Linux

- Change to the root directory of the filesystem—cd /.
- Using the fully qualified path to the archive directory containing the cnr_data_archive.tar file, extract the archive. These examples assume the default archive location provided during installation. Ensure that the paths to the tar executable and cnr_data_archive.tar file reflect the value of the archive directory that you specified during installation.

```
/opt/nwreg2/{local.sav | regional.sav}/tar -xf /opt/nwreg2/{local.sav |
regional.sav}/cnr_data_archive.tar
```

Note There is also a cnr_file_archive.tar which contains the installed files and generally this should not be recovered over a re-installation.

Step 8 Start the Cisco Prime IP Express server agent:

- Windows—Local: **net start nwreglocal**
Regional: **net start nwregregion**

- Linux—Local: `/etc/init.d/nwreglocal start`
Regional: `/etc/init.d/nwregregion start`

Step 9 Verify if the previous configuration, including scopes and zones, is intact.

Moving an Installation to a New Machine

Before you begin, ensure that the new machine meets the current system requirements (see [System Requirements, on page 7](#)).

To move an existing Cisco Prime IP Express installation to a new machine on the same platform:

Step 1 Stop the server agent on the old machine.

- Windows—Local: `net stop nwreglocal`;
Regional: `net stop nwregregion`
- Linux-Local: `/etc/init.d/nwreglocal stop`;
Regional: `/etc/init.d/nwregregion stop`

Step 2 Zip up the data directory on the old machine.

Step 3 Copy the zip file over to the same location on the new machine and unzip the file.

Step 4 Install Cisco Prime IP Express on the new machine (on Linux, use the `-a` option). The installation will detect an upgrade and will do so based on the copied data.

This procedure preserves your original data on the old machine.

Step 5 Login to the web UI and navigate to the **List Licenses** page under the **Administration** menu.

Step 6 Edit the regional server information as necessary. Ensure that the regional server information provided is where you would like to register your new machine.

Step 7 Click the **Register** button to register with the regional server.

Moving a Regional Cluster to a New Machine

License management is done from the regional cluster when Cisco Prime IP Express is installed. The regional server is installed first and all licenses are loaded in the regional server. When the local cluster is installed, it registers with the regional server to obtain its license.

When you want to move a regional cluster to a new machine, you need to back up the data on the old regional cluster and copy the data to the same location on the new machine.



Note When the regional server goes down or is taken out of service, the local cluster is not aware of this action. If the outage lasts for less than 24 hours, it results in no impact on the functioning of the local clusters. However, if the regional cluster is not restored for more than 24 hours, the local cluster will get warning messages that the local cluster is not properly licensed (in the web UI, CLI, or SDK). This does not impact the operation of the local clusters and the local clusters continue to work and service requests.

To move an existing Cisco Prime IP Express installation to a new machine:

Step 1 Stop the server agent on the old regional server:

- Windows:

```
net stop nwregregion
```

- Linux:

```
# etc/init.d/nwregregion stop
```

Step 2 Zip up the data directory on the old regional server.

Step 3 Copy the zip file over to the same location on the new server and unzip the file.

Step 4 Install Cisco Prime IP Express (regional cluster) on the new server. For more information, see [Installing Cisco Prime IP Express, on page 17](#).

The installation will detect an upgrade and will do so based on the copied data. This procedure preserves your original data from the old regional server.

Note When you install Cisco Prime IP Express on the new machine, you must choose the data directory on which you have copied the data from the old regional server.

Step 5 Start the Cisco Prime IP Express web UI or CLI. For more information, see [Starting Cisco Prime IP Express, on page 31](#).

Step 6 Log in as superuser to the CLI for the new regional cluster.

Step 7 To list the local clusters:

```
nrcmd-R>cluster listnames
```

Step 8 To synchronize the data as well as the license information:

```
nrcmd-R>cluster <name of local cluster> sync
```

Troubleshooting the Installation

The Cisco Prime IP Express installation process creates a log file, `install_cnr_log`, in the Cisco Prime IP Express log file directory. For upgrades, one additional log file is created: `lease_upgrade_log`. The log directory is set to these locations by default:

- Windows:

- Local cluster: C:\CiscoPrimeIPExpress\Local\logs
- Regional cluster: C:\CiscoPrimeIPExpress\Regional\logs
- Linux:
 - Local cluster: /var/nwreg2/local/logs
 - Regional cluster: /var/nwreg2/regional/logs

If the installation or upgrade does not complete successfully, first check the contents of these log files to help determine what might have failed. Some examples of possible causes of failure are:

- An incorrect version of Java is installed.
- Insufficient disk space is available.
- Inconsistent data exists for an upgrade.

If the log messages do not clearly indicate the failure, you can gather additional debug information by using the `debug_install` utility script. This script appears only if the installation failed and is located by default in the Cisco Prime IP Express program files directory:

- Windows:
 - Local cluster: C:\Program Files(x86)\Cisco Prime IP Express\Local\debug_install.cmd
 - Regional cluster: C:\Program Files\Cisco Prime IP Express\Regional\debug_install.cmd
- Linux:
 - Local cluster: /opt/nwreg2/local/debug_install.sh
 - Regional cluster: /opt/nwreg2/regional/debug_install.sh

If you need help determining the cause or resolution of the failure, forward the output of this script to Cisco Systems for further analysis. To contact Cisco for assistance, see the following Cisco website:

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

Troubleshooting Local Cluster Licensing Issues

If your regional cluster and local cluster are located in isolated networks, are separated by a firewall, or the time skew between the regional and local clusters is more than five minutes, then the local cluster may be unable to register with the regional server. The firewall may block the return connection used to validate the local cluster admin credentials that are sent from the local cluster to the regional cluster.

To register a local cluster with the regional cluster:

Step 1 Install Cisco Prime IP Express (local cluster) on the server and create the admin user for the local cluster. For more information, see the section "Installing and Upgrading Cisco Prime IP Express".

When you install Cisco Prime IP Express on the local cluster, you can skip the registration of the local cluster with the regional cluster.

- Step 2** Log into the regional cluster and add the new local cluster to the regional cluster with the admin credentials. For more information, see Adding Local Clusters section of *Cisco Prime IP Express 9.0 CLI Reference Guide*.
- Step 3** To synchronize the data as well as the license information, click the **Resynchronize** icon.
-



CHAPTER 6

Next Steps

This chapter contains the following sections:

- [Starting Cisco Prime IP Express, on page 31](#)
- [Starting and Stopping Servers, on page 32](#)
- [Starting and Stopping Servers using the Regional Web UI, on page 33](#)

Starting Cisco Prime IP Express

To administer the local and regional clusters that you have installed, you must enter the appropriate license file (web UI) or the filename (CLI).

To enter license information in web UI or CLI:

Step 1 Start the Cisco Prime IP Express web UI or CLI:

- To access the web UI, open the web browser and use the HTTP (nonsecure login) or HTTPS (secure login) website:

```
http://hostname:http-port
```

```
https://hostname:https-port
```

where:

- The *hostname* is the actual name of the target host.
- The *http-port* and the *https-ports* are the default HTTP or HTTPS port that are specified during installation. (See the installation procedure in the section "Installing Cisco Prime IP Express " on page 17).

On Windows, you can access the web UI from the Start menu from the local host:

- On a local cluster—Choose **Start > Programs > IP Express 9.0 > IP Express 9.0 local Web UI** (or **IP Express 9.0 local Web UI (secure)** if you enabled secure login).
- On a regional cluster—Choose **Start > Programs > IP Express 9.0 > IP Express 9.0 regional Web UI** (or **IP Express 9.0 regional Web UI (secure)** if you enabled secure login).
- To start the CLI:
 - Windows—Navigate to the `install-path\bin` directory and enter this command:

```
nrcmd -C cluster-ipaddress -N <username> -P <password>
```

- Linux—Navigate to the install-path\usrbin directory and enter this command

```
install-path/usrbin/nrcmd -C clustername -N <username> -P <password>
```

Step 2 If you did not enter license information during the installation procedure, you must do so now:

Note You must add the licenses in the Regional cluster which means the Regional should be installed first. The local cluster has to be registered with the regional cluster at the time of installation or at the time of your first login. You can choose the services (dhcp, dns, cdns) for the local based on the licenses added in the Regional cluster.

- Web UI—Click **Browse** to navigate to the license file.
- CLI—Enter an absolute or relative path for the license filename, as follows:

```
nrcmd> license create filename
```

Step 3 Enter the username and the password, that was created during the installation procedure.

Starting and Stopping Servers

In Windows, you can stop and start the Cisco Prime IP Express server agent from the Services feature of the Windows Control Panel. If the installation completed successfully and you enabled the servers, the Cisco Prime IP Express DNS and DHCP servers start automatically each time you reboot the machine.

All servers in the cluster are controlled by the Cisco Prime IP Express regional or local server agent. You can stop or start the servers by stopping or starting the server agent.

For details on stopping and starting servers, see the *Cisco Prime IP Express 9.0 Administrator Guide*.

Starting and Stopping Servers on Windows

To start and stop servers on Windows:

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Service list, choose **IP Express Local Server Agent** or **IP Express Regional Server Agent**.

Step 3 Click **Restart** or **Stop**, as required, and then click **Close**.

Starting and Stopping Servers on Linux

In Linux, the Cisco Prime IP Express servers automatically start up after a successful installation or upgrade. You do not need to reboot the system.



Note To start and stop Cisco Prime IP Express when running as **nradmin**, you must log into the server as a user in the nradmin group (or root). It is not possible to login as nradmin.

```
#/opt/nwreg2/local/bin/cnr_service start
```

```
#/opt/nwreg2/local/bin/cnr_service stop
```

To start and stop servers on Linux:

Step 1 Log in as superuser.

Step 2 Start the server agent by running the nwreglocal or nwregregion script with the *start* argument:

```
# /etc/init.d/nwreglocal start ;for the local cluster
```

```
# /etc/init.d/nwregregion start ;for the regional cluster
```

Step 3 Enter the **cnr_status** command to check that the servers are running:

```
# install-path/usrbin/cnr_status
```

Step 4 Stop the server agent by running the nwreglocal or nwregregion script with the stop argument:

```
# /etc/init.d/nwreglocal stop ;for the local cluster
```

```
# /etc/init.d/nwregregion stop ;for the regional cluster
```

Starting or Stopping Servers using the Local Web UI

To start or stop servers in the local Web UI:

Step 1 From **Operate** menu, choose **Manage Servers** to open the Manage Servers page.

Step 2 To start or stop the DHCP, DNS, CDNS, or SNMP servers, select the server in the Manage Servers pane and do any of the following

- Click the **Start Server** button to start the server.
- Click the **Stop Server** button stop the server.

Step 3 To reload the server, click the **Restart Server** button.

Starting and Stopping Servers using the Regional Web UI

To start or stop servers in the regional Web UI:

Step 1 From **Operate** menu, choose **Manage Servers** to open the Manage Servers page.

Step 2 To start or stop the BYOD or SNMP servers, select the server in the Manage Servers pane and do any of the following

Note The BYOD web server in the regional cluster will stop by default and must be manually restarted. To automatically restart the BYOD server, you must set autostart to true.

- Click the **Start Server** button to start the server.
- Click the **Stop Server** button stop the server.

Step 3 To reload the BYOD server, click the **Restart Server** button.

Note You can only stop and start the SNMP server. Reload is not possible for SNMP servers.



CHAPTER 7

Uninstalling Cisco Prime IP Express

The uninstallation procedure differs based on the operating system you are using. You must have administrator or superuser privileges to uninstall Cisco Prime IP Express, just as you must to install it.

To back up your database before uninstalling Cisco Prime IP Express, see *Cisco Prime IP Express 9.0 Administrator Guide* for the procedure.



Note Uninstallation stops the Cisco Prime IP Express server agents first. If you find that the server processes are not shutting down, see the [Starting and Stopping Servers, on page 32](#).

- [Uninstalling on Windows, on page 35](#)
- [Uninstalling on Linux, on page 36](#)
- [Running Performance Monitoring Software on Windows, on page 36](#)

Uninstalling on Windows

To uninstall Cisco Prime IP Express on Windows:

Step 1 Choose the Add/Remove Program function from the Windows control panel.

Or,

Choose **Uninstall IP Express 9.0** from the Windows Start menu. The uninstallation program removes the server and user interface components but does not delete user data files. Optionally, delete all Cisco Prime IP Express data by deleting the Cisco Prime IP Express folder.

Note Temporarily stop any service that is related to software that integrates with Performance Monitoring that might interfere with removing shared libraries in the Cisco Prime IP Express folder.

Step 2 Reboot after the uninstallation completes.

Uninstalling on Linux

To uninstall Cisco Prime IP Express on Linux:

Run the **uninstall_cnr** program from the install-path/usrbin directory:

```
./uninstall_cnr
Stopping Server Agent...
Deleting startup files...
Removing IP Express...
cannot remove /opt/nwreg2/usrbin - directory not empty
cannot remove /opt/nwreg2/conf - directory not empty
package optnwreg2 not found in file index
```

Note that any files that have been changed (including your database) have not been uninstalled. You should delete these files by hand when you are done with them, before you reinstall the package.

The checkinstall warnings mean that, although the uninstall program removes the server and user interface components, it cannot delete directories that are not empty. Certain configuration and data files that are created during installation remain deliberately after uninstallation. Optionally, delete the database and log files that are associated with Cisco Prime IP Express, as mentioned in the instructions at the end of the **uninstall_cnr** script execution.

Note When Cisco Prime IP Express is installed as nradmin, the uninstall process will reset the ownership of all the remaining files back to the superuser (root).

Running Performance Monitoring Software on Windows

On Windows systems if you uninstall Cisco Prime IP Express and try to remove the associated data directories while having software installed that integrates with the Windows Performance Monitor, the software might take possession of certain shared libraries. This action prevents you from removing these files from the Cisco Prime IP Express folder and the directory itself. To keep this from happening:

1. Stop the service that is associated with the performance monitoring software.
2. Delete the IP Express folder.
3. Restart the service.



CHAPTER 8

Cisco Prime IP Express Virtual Appliance

The Cisco Prime IP Express virtual appliance includes all the functionality available in a version of Cisco Prime IP Express 9.0 installed on any Linux operating system.

This chapter describes how to install Cisco Prime IP Express virtual appliance and includes the following sections:

- [System Requirements, on page 37](#)
- [Installing and Upgrading Cisco Prime IP Express Virtual Appliance, on page 38](#)
- [Upgrading the Cisco Prime IP Express Virtual Appliance, on page 43](#)
- [Next Steps: Cisco Prime IP Express Virtual Appliance, on page 45](#)

System Requirements

There are three kits that can be used to install the virtual appliance:

- An OVA which runs on VMware ESXi 5.5 or later
- A KVM kit which runs on a KVM hypervisor running on CentOS 7.2 or Red Hat (RHEL)
- A cloud image which can be deployed to Openstack

These kits are effectively identical, and in this guide, when the OVA is discussed, the discussion applies to all three kits unless otherwise noted.

Each of these kits were created to require limited resources: 1 virtual CPU, 4 GB main memory, 6 GB swap partition, and a 7.5 GB system partition with 5.4 GB available (free). The total disk storage required is 14 GB. You will almost certainly want to increase the size of the system disk, and giving the virtual appliance additional virtual CPU's can increase the performance considerably. You should ensure that sufficient resources are available on the host that you are targeting for the deployment to meet these requirements.



Note It is worth some effort to determine the likely amount of disk storage that you need at the time you first install the virtual appliance. If you increase the size of the disk space after you have configured and used the product, you must back up all the work that you have done prior to increasing the disk storage. However, if you increase the disk storage when you first install the product, no backup is necessary, since in the unlikely event something goes wrong while expanding the disk storage, nothing valuable would be lost. At worst, you would simply have to reinstall the virtual appliance.

You must increase the resources used by the virtual appliance or it will not function successfully. There are two different regimes: running a local cluster, or running a regional cluster and local cluster on the same machine. The recommendations below are for running the virtual appliance(s) on a Jumpstart, but these are also useful starting points for any local or regional cluster deployment. For a local cluster:

- CPU: 1 socket, 8 CPUs
- Memory: 12 GB
- Disk: 100 GB or greater

For a regional cluster running on the same Jumpstart as a local cluster:

- CPU: 1 socket, 7 CPUs
- Memory: 3 GB
- Disk: 35 GB

You may need substantially more disk space than listed above based on the size of your deployment. You can increase the disk space by resizing the allocated disk and rebooting the appliance.

Installing and Upgrading Cisco Prime IP Express Virtual Appliance

You can deploy the virtual appliance in any of three environments, VMware ESXi 5.5 or later, CentOS/RHEL 7.2 KVM hypervisor, or OpenStack. After discussing the information that you will need to determine for any deployment, the individual environments are discussed in detail.

Preparing to Deploy the Cisco Prime IP Express Virtual Appliance

In order to deploy the Cisco Prime IP Express virtual appliance and configure its network connection, you have to answer several questions. Some of these questions concern the networking environment in which the virtual appliance is being deployed, and some of them concern values which are unique to the particular virtual appliance being deployed.

The questions that are unique to the installation of this particular virtual appliance are listed below. You must decide on answers to these questions before you deploy the virtual appliance.

- A virtual machine name for the deployed virtual appliance.
- A root password for the underlying Linux CentOS operating system.
- An IPv4 address for the virtual appliance.
- A DNS name associated with the IPv4 address of the virtual appliance.
- A username and password for the initial administrator account for the Cisco Prime IP Express application.

The questions concerning the networking environment are as follows. The answers to these questions are not unique to the virtual appliance, but are instead values that are determined by the environment in which you will deploy the virtual appliance:

- The network mask associated with the IP address of the virtual appliance itself.

- The default gateway address for the virtual appliance.
- The IP address of at least one DNS server that can be accessed by the virtual appliance, although it is best if you have the IP addresses of two DNS servers to provide additional availability.
- Any proxy values necessary for the virtual appliance to access the Internet (if you want the virtual appliance to have access to the Internet).
- If this is a local cluster installation, you will need to determine the IP address of the Cisco Prime IP Express regional cluster to which this local cluster will connect in order to receive its license information. If this is a regional cluster installation, you can ignore this requirement.

Deploying the Regional Cluster OVA or Local Cluster OVA on VMware

The Cisco Prime IP Express virtual appliance is supported for production use on VMware ESXi 5.5 or later and can be accessed or managed using the VMware vSphere client. The Cisco Prime IP Express virtual appliance is made available in an Open Virtual Appliance (OVA) package.

The VMware vSphere client can be connected directly to your ESXi installation, or it can be connected to a vCenter server which in turn is connected to your vSphere installation. Connecting through vCenter provides a number of capabilities that connecting directly to ESXi does not. If a vCenter server is available and associated with the ESXi installation, it should be used.

To install the Cisco Prime IP Express virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a .ova file.

The names are:

- *cpipe_9_0_local.ova* for the local virtual appliance
- *cpipe_9_0_regional.ova* for the regional virtual appliance

Download the virtual appliance of your choice. Every Cisco Prime IP Express local cluster installation must connect to a Cisco Prime IP Express regional cluster in order to receive the necessary license information required to operate. Thus, before you install a Cisco Prime IP Express local virtual appliance you must identify the IP address of the regional cluster to which it will connect to receive the license information.

Using vSphere, connect directly to the ESXi installation or the vCenter server, and select the ESXi installation where the OVA is to be deployed.

If you have a vCenter server available, you can connect the ESXi hypervisor to your existing vCenter server and manage it through that vCenter server. Managing all your VMware hypervisors through a common vCenter server provides many benefits.

The screens that you see while managing the ESXi hypervisor with a vSphere client through a vCenter server are different from the screens that you see while connecting the vSphere client directly to the ESXi hypervisor. You can see additional screens if connected through vCenter server. These screens do not actually provide any benefit for the operations in which you will engage to deploy the Cisco Prime IP Express virtual appliance. The benefits to using the vCenter server approach come after the initial deployment of the virtual appliance.

To deploy a Regional Cluster OVA or Local Cluster OVA:

Step 1 From vSphere menu, choose **File > Deploy OVF Template**.

The Deploy OVF Template Source window appears.

Step 2 To deploy the OVA file, click **Browse** and navigate to select the OVA file (.ova) available on the local machine where vSphere is running.

Note You cannot browse for URLs and you must enter the full path to the file.

Step 3 Click **Next**.

The OVF Template Details window appears. It displays the product name, the size of the OVA file, and the amount of disk space that needs to be available for the virtual appliance.

Step 4 Verify the OVA template details and click **Next**.

Step 5 Provide a name to the new virtual appliance and click **Next**.

Note You must enter the same name while configuring the virtual appliance, so make sure you remember this name.

The Disk Format window appears.

The Thick provisioned format is selected by default.

Step 6 Click **Next** to continue.

Note The virtual appliance is only supported when deployed with thick provisioning.

Step 7 To map the networks used in this OVA template to the networks in your inventory, select the current destination network and choose the destination network from the Destination Networks drop-down list. Click **Next**.

The Ready to Complete window appears.

Step 8 Click **Finish** to begin deployment of the OVF Template.


Booting and Configuring Cisco Prime IP Express Virtual Appliance

To boot and then configure the Cisco Prime IP Express virtual appliance:



Note You must set the memory and CPUs based on the requirements prior to clicking the power on. Once you start the VM you cannot change the memory or CPU settings until you shut down.

Step 1 After deploying the Virtual Appliance OVA, select the virtual machine name in vSphere, right-click on it and select **Open Console**.

Step 2 Click the **Power on** button () on the console and click in the window after clicking the Power on button.

During the initial boot of the newly deployed machine, you will be prompted to enter a root (system) password, which is not the Cisco Prime IP Express application password.

Note This is the root password for the underlying Linux operating system on which the Cisco Prime IP Express 9.0 application is installed. You will be asked to enter this password twice. You will need root access to the underlying Linux operating system at various times in the future, so make sure that you remember this password.

The boot process can take a while, both before you are asked for a root password, as well as after you enter the root password.

The End User License Agreement window appears on the first boot. Read the license agreement in its entirety, and only if you understand and accept the license terms, enter y (Yes).

Step 3 Log into the server as the root user.

Step 4 To configure the network for the Virtual Appliance, see the appendix "Configuring Network Access on RHEL/CentOS 7.x Using nmcli".

Deploying the Regional Cluster or Local Cluster on a KVM Hypervisor

To install the Cisco Prime IP Express virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a .bz2 file.

The names are:

- *cpipe_9_0_local.kvm.tar.bz2* for the local virtual appliance
- *cpipe_9_0_regional.kvm.tar.bz2* for the regional virtual appliance

Download the virtual appliance of your choice. Every Cisco Prime IP Express local cluster installation must connect to a Cisco Prime IP Express regional cluster in order to receive the necessary license information required to operate. Thus, before you install a Cisco Prime IP Express local virtual appliance you must identify the IP address of the regional cluster to which it will connect to receive the license information.

To install Cisco Prime IP Express on a KVM Hypervisor, extract the distribution tar archive (***cpipe_9_0_local.kvm.tar.bz2*** or ***cpipe_9_0_regional.kvm.tar.bz2***) using the following command:

```
root$ tar xvjf cpipe_9_0_local.kvm.tar.bz2
```

If you are unpacking both the local and the regional KVM kits, you must untar them in separate directories to avoid filename conflicts.



Note The extraction takes a few minutes and it requires a minimum of 14 GB free disk space. You should see the following files:

-
- *cpipe_9_0_local-disk1.raw*—contains the disk for the virtual machine
 - *installonkvm*—installs the virtual machine
 - *readme.kvm.txt*—contains the installation instructions

The first file (*-disk1.raw*) is the actual file that will be used as the disk file for the resulting CPIPE KVM virtual machine. This file should be placed in the directory where you want it to reside long-term as the "source path" for the virtual disk in the CPIPE KVM virtual machine. While you can move it even after the virtual machine is installed, it is easier to start with it in the correct location. You should move the *installonkvm* script along with it. The *installonkvm* script needs to be executable in order to operate correctly.

To proceed with the installation, follow the instructions as specified in the *readme.kvm.txt* file.

Once the installation is complete, see the appendix "Configuring Network Access on CentOS 7.2 using nmcli" in this Guide.

Deploying the Regional Cluster or Local Cluster on OpenStack

To install the Cisco Prime IP Express virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a .ova file.

The names are as follows:

- *cpipe_9_0_local.qcow2* for the local virtual appliance
- *cpipe_9_0_regional.qcow2* for the regional virtual appliance

Download the virtual appliance of your choice. Every Cisco Prime IP Express local cluster installation must connect to a Cisco Prime IP Express regional cluster in order to receive the necessary license information required to operate. Thus, before you install a Cisco Prime IP Express local virtual appliance you must identify the IP address of the regional cluster to which it will connect to receive the license information.

To run the local cluster or regional cluster on OpenStack, you must first create a local or regional image out using the **.qcow2** distribution kit.

After this image exists, you may launch an instance of the local or regional cluster. The Flavor you associate with the instance needs at least 1 VCPU, 4 GB of RAM, and at least 14 GB of root disk storage. In order to have an operational instance of CPIPE, you must allocate more than the absolute minimum of 14 GB of root disk storage. See the [System Requirements, on page 7](#) section for the amount of disk space needed for a local or regional cluster.

An instance of Cisco Prime IP Express will be created with a fixed IP address. Cisco Prime IP Express will automatically use any IP addresses associated with interfaces that it can detect when it is started. If the interface available to Cisco Prime IP Express has an IP address allocated to it from a provider network (i.e., it is accessible to the clients that need the DHCP or DNS capabilities provided by Cisco Prime IP Express), then you can configure Cisco Prime IP Express normally.



Note

In keeping with the general approach for OpenStack cloud image deployment, root password based login is DISABLED in the .qcow2 kits. The only way to gain access to the Linux operating system on the instance once it is launched is to login via ssh using the ssh key pair associated with the instance at the time of launch. For example: `ssh -i keypairname.pem root@a.b.c.d` If you did not associate a key pair with the instance, or have lost access to the key pair, you will not be able to login to the instance. There is no default root password, and root password login is disabled.

Once you have gained access to the instance using the **ssh** key pair, if you would like to be able to login with a password, you could create a new Linux user using the **useradd** command and make that user a member of the group wheel. You must also give that user a secure password using the **passwd** command. Then you can always login with **ssh** or to the console as that user and become the root user using **sudo su**.

To create a user to allow password login, use the following command:

```
useradd safeuser -g wheel
passwd safeuser
```

Then, if you need root access, login as safeuser and use the following command:


```
sudo su
```

enter the password for safeuser, and you will become a root user.

If the IP addresses that are associated with the available interfaces are fixed addresses (i.e., they are only accessible to other instances in OpenStack), then you will need to associate a floating address with Cisco Prime IP Express instance. This floating address must then be accessible to the clients of the DHCP or DNS service to be provided by the Cisco Prime IP Express instance. You will have to configure the DHCP server provided by Cisco Prime IP Express to return the IP address of the floating address as its server-id, instead of the fixed IP address that Cisco Prime IP Express can detect that is associated with the interface built into the instance. In order to configure DHCP for this situation, you will need to be in expert mode, and configure the DHCP Policy attribute "dhcp-server-identifier-address" with the floating address allocated to this instance. Then the DHCP server will return the configured IP address (which will be the externally visible IP address of this instance) instead of the IP address that the DHCP server can detect from examining the interface that it is using for communications with clients (which is the fixed IP address).

A local cluster needs to be registered with a regional cluster. After this registration, the regional cluster needs to be able to connect to the local cluster. When the local cluster initially registers with the regional cluster, it sends its IP address to the regional cluster. If the regional cluster can contact the local cluster by using the IP address that the local cluster sees is configured to its network interface, then no action need be taken. This would be the case if the local cluster has a fixed IP address that is only visible within the OpenStack cloud, but the regional cluster was also in the same cloud. If the regional cluster can ping the IP address that the local cluster sees as the IP address on its network interface, then no additional steps are necessary. However, in the event that the regional cluster is not local to the OpenStack cloud on which the local cluster is running, and the local cluster has a floating address in addition to a fixed address, then the regional cluster's configuration for the local cluster needs to have its IP address updated to be that of the floating address (and not the fixed address, which is what it will have from the initial registration).

When allocating a local cluster, you should consider allocating 4 or even 8 VCPUs and at least 8 GB of RAM, with more for large systems. Local clusters will absolutely need more than the 7+ GB free space available in the minimal installation. Regional clusters will probably need additional disk space, but 2 to 4 VCPUs and 6 to 8 GB of RAM will suffice for many installations.

Upgrading the Cisco Prime IP Express Virtual Appliance

This section describes the procedure for upgrading Cisco Prime IP Express to Cisco Prime IP Express virtual appliance and upgrading the operating system to CentOS 7.2 using the data from an existing virtual appliance.

Upgrading a Cisco Prime IP Express Installation to run on a Cisco Prime IP Express Virtual Appliance

This section describes how to upgrade an existing installation of Cisco Prime IP Express to become a Cisco Prime IP Express virtual appliance.



Note This procedure upgrades a current version of Cisco Prime IP Express running on a Linux operating system to a current version of the Cisco Prime IP Express virtual appliance. If you need to move from a different platform, you have to first convert to the Linux platform prior to upgrading to a virtual appliance. If you need to move from a different version of Cisco Prime IP Express to the current version of the virtual appliance, you have to first upgrade to the current version of Cisco Prime IP Express on an external Linux system before upgrading to the virtual appliance. See [Installing and Upgrading Cisco Prime IP Express, on page 17](#).

Step 1 Install the Cisco Prime IP Express virtual appliance.

Step 2 Shut down the Cisco Prime IP Express application being upgraded using the following command: `/etc/init.d/nwreglocal stop`

Step 3 Copy the file `cnr_prepareforupgrade` from `/opt/nwreg2/{local | regional}/usrbin` from the virtual appliance system to the Cisco Prime IP Express installation being upgraded.

Note You have to choose either local or regional from `{local | regional}` based on the upgrade that you are doing, that is, local upgrade or regional upgrade.

You can do it using sftp, for example:

```
[root@cnr-machine-being-upgraded usrbin]# sftp 10.10.10.12
Connecting to 10.10.10.12...
Warning: Permanently added '10.10.10.12' (RSA) to the list of known hosts.
root@10.10.10.12's password:
sftp> cd /opt/nwreg2/local/usrbin
sftp> get cnr_prepareforupgrade
Fetching /opt/nwreg2/local/usrbin/cnr_prepareforupgrade to cnr_prepareforupgrade
/opt/nwreg2/local/usrbin/cnr_prepareforupgrad 100% 3265    3.2KB/s   00:00
```

Step 4 Execute `cnr_prepareforupgrade` on the system being upgraded.

Step 5 If the version of Cisco Prime IP Express which you are moving to the virtual appliance is a version earlier than Cisco Network Registrar 7.2, then perform the following steps:

Note If you are upgrading from 7.2, you do not require the `cnr_mcdexport` kit because 7.2 clusters do not use the MCD DB database technology and you can skip this step.

- a) Download the upgrade preparation kit, `cnr_mcdexport_linux5.tar`, from Cisco.com.
- b) Untar the downloaded archive and run the script `cnr_mcdexport`.

Step 6 Tar the existing `install-path/local/data` directory using the command:

```
tar cvf tarfile.tar data
```

Step 7 Copy the tar file created to the new virtual appliance.

Step 8 Shut down Cisco Prime IP Express on the new virtual appliance using the command:

```
/etc/init.d/nwreglocal stop
```

Step 9 Rename the existing database to **.orig** using the command:

```
mv /var/nwreg2/local/data /var/nwreg2/local/data.orig
```

Step 10 Untar the latest database, transferred in **Step 4**, using **tar xvf tarfile.tar**.

Step 11 Reboot the Cisco Prime IP Express virtual appliance using VMware vSphere.

Upgrading to a new Version of the Virtual Appliance Operating System

To upgrade and to use a new version of the Cisco IP Express virtual appliance, install a new virtual appliance which has the new operating system version on it, and then move the data and configuration from the existing virtual appliance to the new virtual appliance.

To do this follow the steps in the section [Installing and Upgrading Cisco Prime IP Express Virtual Appliance, on page 38](#):

You can now start the new virtual machine. It will have the entire data directory of the existing virtual machine.



Note The new virtual machine with the upgraded operating system will pause during the boot process and instruct you to upgrade the Cisco Prime IP Express database to match the database version of the Cisco Prime IP Express application that resides on the new virtual machine.

Step 1 Press return on the console to complete the boot process.

Step 2 Log in as root and run the displayed command.

After boot completion, you should see your existing configuration running with the new version of Cisco Prime IP Express on the new virtual machine.

Upgrading the Cisco Prime IP Express Application

If you want to upgrade the installation of Cisco Prime IP Express that currently exists on the virtual appliance to a new version of Cisco Prime IP Express, follow the procedure in the Cisco Prime IP Express 9.0 Installation Guide to perform a straightforward software product upgrade. The installation of Cisco Prime IP Express delivered on the virtual appliance is a regular installation of the Cisco Prime IP Express software product.

Next Steps: Cisco Prime IP Express Virtual Appliance

Configuring Cisco Prime IP Express with the CLI on Virtual Appliance

The Cisco Prime IP Express command line interpreter (CLI) can be used to configure the virtual appliance in two ways:

- You can use the nrcmd CLI on the virtual appliance directly by first using SSH to connect into the underlying Linux operating system on the virtual appliance. You can use any username and password

which you have created on the virtual appliance for the SSH login, and you must use an administrator username and password for the Cisco Prime IP Express to use the `nrcmd` CLI to configure Cisco Prime IP Express.



Note As distributed, there is only one valid user for the Linux operating system—root. While you can login as root to use the Cisco Prime IP Express CLI, you might want to add additional users to the system. Use the `useradd` program to add additional users. You can type `man useradd` for more information on how to add additional users.

- Alternatively, you can use the `nrcmd` CLI on some other system in the network to configure and manage Cisco Prime IP Express on the virtual appliance the same way that you would use it to manage any remote installation of Cisco Prime IP Express. This requires installing Cisco Prime IP Express (typically only the client-only installation) on the other system.

Configuring the Virtual Appliance to Automatically Power Up

You can configure the ESXi hypervisor to automatically power up the Cisco Prime IP Express virtual appliance when power is restored to the ESXi hypervisor layer.



Note The KVM kit is installed with automatic power up enabled.

To configure automatic power up:

- Step 1** In the vSphere client, select the ESXi machine to which you are connected. It is not a specific virtual machine that you have to select but the ESXi hypervisor on which they reside.
 - Step 2** Select the **Configuration** tab.
 - Step 3** Click the **Virtual Machine Startup/Shutdown** link under the **Software** area. You should see the virtual machine in the list shown in window.
 - Step 4** Click the **Properties...** link present at the top right corner of the page. If you do not see that, resize the window until you do.
The Virtual Machine Startup and Shutdown page is displayed.
 - Step 5** Check the **Allow virtual machines to start and stop automatically with the system** check box.
 - Step 6** Select the virtual machine running the Cisco Prime IP Express virtual appliance and use the **Move Up** button on the right to move it up into the group labelled **Automatic Startup**
 - Step 7** Click **OK**
- This ensures that whenever power is restored to the ESXi hypervisor the Cisco Prime IP Express appliance powers up automatically.
-

Managing the Cisco Prime IP Express Virtual Appliance

You can manage the underlying Linux operating system, which is based on CentOS 7.2, by logging in as the root user. You may use SSH to log into the virtual appliance with the username root and the root password you specified when you first booted the virtual appliance. On Openstack you may use the key pair created when you launched the instance.

You will probably want to create additional users on the Linux system so that people can access the Linux system with a username other than root.

The Linux system which is included on the virtual appliance is stripped down to a considerable degree and thus does not include things that are not required to run or manage the Cisco Prime IP Express application, such as a window system manager and its associated GUI user interface. However, all the tools necessary to support and manage the Cisco Prime IP Express application are included on the Linux operating system used inside of the virtual appliance.

You may also want to take additional steps to secure the SSH connection. For instance, configuring it to prevent logging on as root, and requiring a user to **su** to gain root privileges after logging on as another user.

You may wish to perform other configuration changes on the underlying Linux operating system in order to lock it down in ways appropriate to your environment.



Note Cisco Prime IP Express customers are solely responsible for keeping their OS up to date regarding patches that they desire to apply and Cisco is not responsible for the same.



APPENDIX **A**

Performing a Silent Installation

This appendix contains the following section:

- [Performing a Silent Installation](#) , on page 49

Performing a Silent Installation

This appendix describes how to perform a silent installation, upgrade, or uninstallation of the Cisco Prime IP Express product. A silent installation or upgrade allows for unattended product installations based on the configuration values that are provided at the time that a silent installation response file was created.



Caution Unpredictable results can occur if you try to use a silent-response file that does not contain the correct settings for the system undergoing the silent installation.

To generate or create a silent-response file:

Step 1 For each silent installation or upgrade, use these commands to create a separate response file:

- Windows:

```
setup.exe -r
```

Complete the installation or upgrade steps as you normally would. This command installs or upgrades Cisco Prime IP Express according to the parameters that you specified.

Note If Cisco Prime IP Express is already installed, **setup.exe** uninstalls the existing version and if Cisco Prime IP Express is not installed, then it does the installation.

It also generates the `setup.iss` silent-response file based on these parameters. Look for this file in the Windows installation directory, such as `C:\WINDOWS`. Each time you use the command, the file is overwritten.

We recommend that you rename or relocate this file before running the silent process in **Step 2**. Rename the file to something distinguishable, such as `local-nr-https-install`, and relocate it to a temporary folder.

- Linux:

Create a text silent-response file that includes the entries listed in the table below.

Table 3: Silent-Response File Entries for Linux

Silent-Response File Entry	Description
BACKUPDIR=	Path where to store the current Cisco Prime IP Express installation files, but only if PERFORM_BACKUP=y
CCM_LOCAL_SERVICES=	Services (dhcp, dns or cdns) to enable
CCM_PORT=	Central Configuration Management (CCM) port; default value is: <ul style="list-style-type: none"> • 1234 if CNR_CCM_MODE=local • 1244 if CNR_CCM_MODE=regional
CCM_RGNL_IP_ADDR=	IPv4 address of the regional server
CCM_RGNL_IPV6_ADDR=	IPv6 address of the regional server
CCM_RGNL_SCP_PORT=	SCP port number on the regional server
CNR_ADMIN=	Superuser name. To skip configuring the superuser name, value should be CNR_ADMIN= unset.
NRADMIN=	Non-root user. To install Cisco Prime IP Express as non-root user, value must be NRADMIN=y.
CNR_PASSWORD=	Superuser password. To skip configuring the superuser password, value should be CNR_PASSWORD= unset.
CNR_CCM_MODE=	CCM mode; set to local or regional .
CNR_CCM_TYPE=	Reserved for GSS installation. Introduced in Cisco Prime Network Registrar 7.0; always set to cnr .
CNR_EXISTS=	If set to y (recommended), tries to kill any open CLI connections when installing or upgrading; otherwise, basically deprecated.
CNR_LICENSE_FILE=	For Cisco Prime Network Registrar 7.x and later only, the fully qualified path to the license file. Set CNR_LICENSE_FILE =unset if CNR_CCM_MODE=local for Cisco Prime IP Express 8.x.
CNR_SECURITY_MODE=	Security mode configuration: <ul style="list-style-type: none"> • required - Fail if the connection cannot be secured. • optional - Allow fallback to insecure connection. • disabled - Do not load security modules at startup.
DATADIR=	Fully qualified path to the data directory

Silent-Response File Entry	Description
JAVADIR=	Fully qualified path to the Java installation (JRE 1.7 or later).
KEYSTORE_FILE=	If USE_HTTPS=y, the fully qualified path to the keystore file.
KEYSTORE_PASSWORD=	If USE_HTTPS=y, the password used when generating the keystore file.
LOGDIR=	Fully qualified path to the log file directory.
PERFORM_BACKUP=	Specifies whether or not to back up the current installation files, if present. Can be set to y even on a clean installation (see also BACKUPDIR).
ROOTDIR=	Fully qualified installation path for the product files; contains bin, classes, cnrwebui, conf, docs, examples, extensions, lib, misc, schema, tomcat, and usrbin subdirectories
START_SERVERS=	Must be set to y for a full installation (with protocol servers) to assure the installation or upgrade is completed; it also results in the Cisco Prime IP Express product being started after the install/upgrade. For a client-only installation, must be set to n .
TEMPDIR=	Fully qualified path to the temp directory.
USE_HTTP=	Sets whether or not the web UI server listens for HTTP connections; one or both of USE_HTTP or USE_HTTPS must be set to y .
USE_HTTPS=	Sets whether or not the web UI server listens for HTTPS connections; one or both of USE_HTTP or USE_HTTPS must be set to y (see also KEYSTORE_FILE and KEYSTORE_PASSWORD).
WEBUI_PORT=	Port number that the web UI uses for HTTP traffic; default value is: <ul style="list-style-type: none"> • 8080 if CNR_CCM_MODE=local • 8090 if CNR_CCM_MODE=regional
WEBUI_SEC_PORT=	Port number that the web UI uses for HTTPS traffic; default value is: <ul style="list-style-type: none"> • 8443 if CNR_CCM_MODE=local • 8453 if CNR_CCM_MODE=regional
WEB_SERVICES=	Set to y or n to enable or disable the web services (DNS ENUM and REST API).

Silent-Response File Entry	Description
CNR_BYOD_ENABLE=	Set to y or n to enable or disable the BYOD services.

Step 2 Use these commands to invoke the silent installation or upgrade for each instance:

- Windows:

```
setup.exe -s -flpath+response-file
```

Note The silent installation fails if you do not specify the **-fl** argument with a fully qualified path to the response file, unless the response file is located in the i386 directory and setup.exe is run from that directory.

- Linux:

```
install_cnr -r response-file
```

Step 3 If you want to uninstall the product:

- Windows—Generate an uninstallation response file and execute:

```
setup.exe -s -fluninstall_response_file
```

- Linux—Invoke the silent uninstallation (this command is noninteractive except during an error):

```
uninstall_cnr
```



APPENDIX **B**

Lab Evaluation Installations

This appendix contains the following sections:

- [Lab Evaluation Installations, on page 53](#)
- [Installing Cisco Prime IP Express in a Lab, on page 53](#)
- [Testing the Lab Installation, on page 54](#)
- [Uninstalling in a Lab Environment, on page 54](#)

Lab Evaluation Installations

This appendix describes how to install, upgrade, and uninstall Cisco Prime IP Express regional and local clusters on a single Linux machine to support smaller test configurations for evaluation purposes.



Note You cannot install both the local and the regional cluster on a single Windows machine.



Caution Installing the regional and local cluster on a single machine is intended only for lab evaluations, and should not be chosen for production environments. The aggregated regional cluster databases are expected to be too large to be reasonably located with a local server that is also running DNS or DHCP services. Running out of free disk space causes these servers to fail.

Installing Cisco Prime IP Express in a Lab

To install Cisco Prime IP Express on a single machine for evaluation purposes:

-
- Step 1** Check whether the machine has enough disk space to accommodate two separate installations of Cisco Prime IP Express.
- Step 2** Install or upgrade the local cluster on the Linux machine, according to the procedures in the section "Installing Cisco Prime IP Express " on page 17. Specify the Local cluster installation.

- Step 3** Install or upgrade the regional cluster on the same machine, according to the same procedures. Specify the Regional cluster installation.
-

Testing the Lab Installation

To test the installation:

- Step 1** Start and log in to the web UI for the local cluster, using the URL appropriate to the port number. By default, the local port numbers are **8080** for HTTP connections and **8443** for HTTPS (secure) connections.
- Step 2** Add DNS zones and DHCP scopes, templates, client-classes, or virtual private networks (VPNs) as a test to pull data to the regional cluster.
- Step 3** Start and log into the web UI for the regional cluster, using the URL appropriate to the port number. By default, the regional port numbers are **8090** for HTTP connections and **8453** for HTTPS (secure) connections.
- Step 4** Test the regional cluster for single sign-on connectivity to the local cluster. Try to pull DNS zone distributions, DHCP scopes, templates, client-classes, or VPNs from the local cluster to the regional replica database.
-

Uninstalling in a Lab Environment

If you need to uninstall Cisco Prime IP Express, follow the procedure in "Uninstalling on Linux" .

No option exists to uninstall only the regional or local cluster in a dual-mode installation environment.



APPENDIX **C**

Installing the Cisco Prime IP Express SDK

This section documents how to install the Cisco Prime IP Express SDK on the Linux and Windows platforms. Before installing the SDK, ensure that you have Java Runtime Environment (JRE) 1.7 or later, or the equivalent Java Development Kit (JDK), installed on your system. The Cisco Prime IP Express SDK is a separate product and is sold separately.

This appendix contains the following sections:

- [Installing on Linux, on page 55](#)
- [Installing on Windows, on page 56](#)
- [Testing Your Installation, on page 56](#)
- [Compatibility Considerations, on page 56](#)

Installing on Linux

To install the Cisco Prime IP Express SDK on a Linux platform:

Step 1 Extract the contents of the distribution .tar file.

a) Create the SDK directory:

```
% mkdir /cnr-sdk
```

b) Change to the directory that you just created and extract the .tar file contents:

```
% cd /cnr-sdk
```

```
% tar xvf sdk_tar_file_location/cnr-sdk.tar
```

Step 2 Export your LD_LIBRARY_PATH and CLASSPATH environment variable:

```
% export LD_LIBRARY_PATH=/cnr-sdk/lib
```

```
% export CLASSPATH=/cnr-sdk/classes/cnr-sdk.jar:.
```

Installing on Windows

To install the Cisco Prime IP Express SDK on a Windows platform:

Step 1 Extract the contents of the distribution .tar file.

a) Create the SDK directory:

```
> md c:\cnr-sdk
```

b) Change to the directory that you just created and extract the .tar file contents:

```
> c:
```

```
> cd \cnr-sdk
```

```
> tar xvf sdk_tar_file_location\cnrsdk.tar
```

You may optionally use Winzip to extract cnrsdk.tar to the C:\cnr-sdk directory.

Step 2 Set your PATH and CLASSPATH variables:

```
> set PATH=%PATH%;c:\cnr-sdk\lib
```

```
> set CLASSPATH=c:\cnr-sdk\classes\cnrsdk.jar;.
```

Testing Your Installation

On Linux, the following test program verifies that you have set your PATH or LD_LIBRARY_PATH correctly:

```
% java -jar /cnr-sdk/classes/cnrsdk.jar
```

On Windows, the following test program verifies that you have set your CLASSPATH correctly:

```
> java -jar c:\cnr-sdk\classes\cnrsdk.jar
```

Compatibility Considerations

For Java SDK client code developed with an earlier version of the SDK, you can simply recompile most code with the latest JAR file to connect to an upgraded server.

But in cases where the client code for versions Cisco Prime Network Registrar 7.1 directly manipulates reservation lists in scopes or prefixes, changes are required. These changes are required because the embedded reservation lists in both scopes and prefixes are no longer used. Beginning with version 7.1, individual reservations are stored separately and reference the parent scope or prefix by name.

The new design provides the following benefits:

- Reservation edits (add/modify/delete) do not require a scope or prefix edit.
- Reservations can be indexed directly to allow quick search and retrieval.

- Edits to scopes or prefixes with a large number of reservations no longer result in large scope or prefix change entry logs.

No changes are required for client code that adds or removes reservations using the `addReservation` or `removeReservation` methods. However, these methods are now deprecated because the edit functionality is replaced and extended by the general `addObject`, `modifyObject`, `removeObject`, `addObjectList`, `modifyObjectList`, and `removeObjectList` methods.



APPENDIX **D**

Enhancing Security for Web UI

This appendix contains the following section:

- [Enhancing Security for Web UI, on page 59](#)

Enhancing Security for Web UI

When connected through the Secured Socket Layer (SSL) protocol using HTTPS, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These ciphers usually include weak cipher session keys and can affect system security. Therefore, you may want to adjust the ciphers to disable the use of weak ciphers in the web UI.

To adjust the ciphers:

-
- Step 1** Open the **server.xml** file in the install-path/tomcat/conf folder in your Cisco Prime IP Express installation folder.
- Step 2** Add a ciphers statement to the HTTPS connector statement and list down the allowed ciphers as described in the following example:

Note The values for **port**, **keystoreFile**, and **keystorePass** must match the values that you have configured in your system.

```
<Connector port="8443"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    maxHttpHeaderSize="8192"
    enableLookups="false"
    disableUploadTimeout="true"
    acceptCount="100" scheme="https" secure="true"
    clientAuth="false"
    ciphers="SSL_RSA_WITH_RC4_128_SHA,
    TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
    TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
    SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
```

```
keystoreFile="conf/.keystore"  
keystorePass="changeit"  
sslProtocol="TLS" />
```

The `ciphers` attribute can carry a comma-separated list of encryption ciphers that this socket is allowed to use. By default, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These contain the weak export-grade ciphers in the list of available ciphers. This results in the web UI supporting weak cipher session keys.

Note The ciphers are specified using the Java Secure Socket Extension (JSSE) cipher naming convention.

Step 3 Restart Cisco Prime IP Express for the changes to take effect.



APPENDIX **E**

Hardening Guidelines

This appendix contains the following section:

- [Hardening Guidelines, on page 61](#)

Hardening Guidelines

Cisco does not recommend any specific set of hardening guidelines. However, if you consider hardening the system, the following hardening guidelines should be considered for each host platform:

- Red Hat 6:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

- Red Hat 7:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Security_Guide/Red_Hat_Enterprise_Linux-7-Security_Guide-en-US.pdf

- Windows Server 2012:

<https://technet.microsoft.com/en-us/security/jj720323.aspx>

- NSA hardening guide collection:

https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml



Note The above links reference external websites and Cisco is not responsible for keeping them up-to-date. They are provided for reference only. If you find that the content is outdated or if you cannot access the links, please contact the website owner for updated information.



APPENDIX **F**

Configuring Network Access on CentOS 7.2 using nmcli

This appendix contains the following section:

- [Configuring Network Access on CentOS 7.2 using nmcli, on page 63](#)

Configuring Network Access on CentOS 7.2 using nmcli

The **NetworkManager** command-line tool (**nmcli**) provides a command line way to configure networking by controlling NetworkManager. This section provides only an overview with some examples to help you learn how to use nmcli to configure network access on the virtual appliance.

In a departure from previous approaches to network interface configuration, NetworkManager deals with both connections and interfaces (also known as devices). Connections are configured with IP addresses, gateways, DNS servers, and then applied to interfaces (devices). This is a critical change from the past way of configuring network access on CentOS Linux, and includes all aspects of nmcli operations.

First, there are two nmcli commands that are of general usefulness:

- The `nmcli d` command lists all available network interfaces (devices).
- The `nmcli c` command lists all available configurations.

Use the above two commands frequently as you are learning to use nmcli.

Follow the steps below to configure a connection for an interface on your virtual appliance. Typically these commands are typed directly into the console of the virtual appliance. If you are already connected through the network (for example, by **ssh**), then making changes to the network interface configuration can be problematic, as you may also lose network connectivity (and thereby your ability to issue nmcli commands) at any point in the process.

Step 1

Make sure that the interface does not block nmcli. The `nmcli d` command lists the existing interfaces. If the interface you want to configure is listed as **unmanaged**, then NetworkManager has been explicitly blocked from configuring this interface. Until you remove this blockage, no `nmcli` command will have any effect on this interface. Note that you may not need to perform this procedure unless the interface is listed as **unmanaged**. Follow the steps below to allow it to be managed by NetworkManager:

- a) Remove the line `NM_CONTROLLED=no` from the file `/etc/sysconfig/network-scripts/ifcfg-<interface>`, where `interface` is the interface name listed in the `nmcli d` command. If there is no file with this name, then you do not need to perform this procedure.
- b) NetworkManager must be told to read the configuration files again. To do this, give the following command:

```
nmcli connection reload
```

Note Manual changes to any `ifcfg` file will not be noticed by NetworkManager until the following command is issued:

```
nmcli connection reload
```

Step 2

Make sure that there is no current configuration for the interface that you want to configure. If you want the configuration that you create to be the default for the interface and there are multiple configurations associated with an interface, it may lead to confusion when the system reboots. The `nmcli c` command lists the existing configurations. If you see any existing configurations, examine them to see if they apply to the interface you want to configure. An easy way to do this is to use the following command:

```
nmcli con show <config> | grep <interface>
```

If you see any output, you should remove the configuration `<config>` with the command:

```
nmcli con delete <config>
```

Note There is often a configuration called "Wired connection 1" which needs to be deleted.

Step 3

Create the configuration and associate it with the interface (device) in one command. This command only creates the configuration, it does not apply it to the interface.

```
nmcli con add type ethernet con-name <config> ifname <interface> ip4 <ip>/<netmaskwidth> gw4 <gateway>
```

where `<config>` is the name of the configuration, which can be anything (including the name of the interface), `<interface>` is the name of the interface (device), `<ip>` is the IPv4 address, `<netmaskwidth>` is the network mask width, and `<gateway>` is the IPv4 gateway address.

Example (type all in one line):

```
nmcli con add type ethernet con-name my-office ifname ens160 ip4 10.10.24.25/24 gw4 10.10.20.174
```

Step 4

Add the DNS server to the interface (device):

```
nmcli con mod <config> ipv4.dns <dnsip>
```

where `<dnsip>` is the IPv4 address of the DNS server and `<config>` is the name of the configuration.

Example:

```
nmcli con mod my-office ipv4.dns 72.63.128.140
```

You can add two DNS addresses as given below:

```
nmcli con mod my-office ipv4.dns "72.63.128.140 72.63.111.120"
```

Note This will replace any previously set DNS servers. To add to an previously set DNS entry, use the + before `ipv4.dns` as shown below:

```
nmcli con mod test-lab +ipv4.dns "72.63.128.140 72.63.111.120"
```

Step 5 Bring up the interface:

```
nmcli con up <config>
```

where `<config>` is the name of the configuration.

Step 6 Use the following command to examine information about a connection. You may examine information about a connection by using this command:

```
nmcli -p con show <config>
```

This will typically scroll off of the console screen, leaving the beginning unreadable. To allow you to move back and forth and examine the output easily, use this command:

```
nmcli -p con show <config> | less
```

From this, you can see the entire configuration. You can modify things in the configuration with:

```
nmcli con mod <config> <something>.<other> <new-value>
```

Example:

```
nmcli con mod my-office wifi-min.key-cntl wpa-psk
```

Step 7 Use the command `set-hostname` to set the hostname for the system:

```
hostnamectl set-hostname <hostname>.<domain>
```

Note This must be done before registering the local to the regional, otherwise an error will result about "localhost" already existing.

where `<hostname>` is the hostname you want to use and `<domain>` is the domain name, ending with `.com`, `.org`, and so on. It is important to include the domain name (along with the `.com`, `.org`, or whatever ending is appropriate), since this is used as the default for DNS lookups.

Example:

```
hostnamectl set-hostname my-server.gooddomain.com
```

Step 8 After you configure the networking you must restart CPIPE (`/etc/init.d/nwreglocal stop`, followed by `/etc/init.d/nwreglocal start`) in order for the interfaces to be properly discovered. If you fail to restart, it will result in a misconfigured registration at the regional.

To develop a complete understanding of the usage of nmcli, search for the online resources on nmcli and CentOS 7.2.



INDEX

;installation:log files:install_cnr_log;install_cnr_log file;log files [27](#)
;installation:log files:lease_upgrade_log;lease_upgrade_log file; [27](#)

A

Add License page [32](#)
 web UI;Web UI:Add License page [32](#)
archive directories;upgrade:archive directories;Regional.sav
 directory;Local.sav directory [21](#)
archiving;upgrade:archiving [21](#)

C

certificate file [18](#)
 importing;keytool utility [18](#)
ciphers:adjusting [59](#)
cnr_status utility;cnr_status;Linux:cnr_status [23](#)
cnr_status utility:cnr_status;Linux:cnr_status; [33](#)
command line interface;CLI; [1](#)
connection type;installation:connection type;upgrade:connection
 type;HTTP connection;HTTPS connection [22](#)

D

database status;upgrade:database status [21](#)
debug_install script [28](#)
disk space requirements [8](#)

E

error logging;logging:server events;servers:logging
 events;starting:logging when;viewing server
 logs;logging:startups [16, 36](#)

G

gzip utility;gzip;Linux:gzip;uncompressing the media [19](#)

I

install_cnr utility;Linux:install_cnr [19, 52](#)
installation [13, 17](#)
 checklist [13](#)
 system privileges [17](#)

installation (*continued*)
 upgrade [13](#)
 license keys [13](#)
 upgrade process [17](#)
installation;upgrade [17](#)
installation:CD;upgrade:CD;installation:network
 distribution;upgrade:network distribution [18](#)
installation:cluster mode;clusters:modes;upgrade:cluster mode;local
 mode;regional mode;clusters:local;clusters:regional; [19](#)
installation:directory;Local directory;Regional directory [20](#)
installation:modes:new;installation:modes:upgrade with data
 migration;installation:modes:upgrade without data
 migration [9](#)
installation:types;upgrade:types;server-client installation;client-only
 installation [21](#)

J

Java Runtime Environment (JRE);Java Development Kit
 (JDK);installation:JRE/JDK requirements;upgrade:JRE/JDK
 requirements [17](#)
JAVA_HOME setting;installation:JAVA_HOME
 setting;upgrade:JAVA_HOME setting [17](#)
Java:directory;installation:Java directory;upgrade:Java directory [22](#)
Java:requirements [7](#)

K

keystore file;self-signed certificates;keytool utility [18](#)

L

lab evaluation installations;installation:lab evaluation;upgrade:lab
 evaluation [53](#)
license keys [9, 31](#)
license set key command (CLI);CLI:license set key command [32](#)
license types [9](#)
license; market segment specific [10](#)
Linux [17](#)
 superuser/root accounts [17](#)
Linux:requirements [8](#)
Linux:variable declaration file [49](#)

N

Network Registrar [1](#)
 about; [1](#)
 nwreglocal utility;nwregregion utility;nwreglocal and nwregregion [33](#)

O

operating system:requirements [7](#)
 operating system:versions [8](#)
 OVA [37](#)
 overview;installation:overview;upgrade:overview; [1](#)

P

processing messages;installation:processing
 messages;upgrade:processing messages [23](#)

R

RAM requirements [8](#)
 root accounts [17](#)

S

sdk [55](#)
 sdk:compatibility considerations [56](#)
 sdk:installing [55](#)
 secure login;installation:secure login;upgrade:secure login [17](#)
 self-extracting executable;Windows:self-extracting executable [18](#)
 servers:DHCP;DHCP servers; [2](#)
 servers:DNS;DNS servers; [2](#)
 servers:running with other [15](#)
 servers:starting/stopping;starting:servers;stopping servers [32](#)
 setup.exe file;Windows:setup.exe file [18](#)
 silent installations;installation:silent;upgrade:silent;noninteractive [49](#)
 Start menu:access;Windows:Start menu [31](#)
 starting:Web UI;starting:CLI;Web UI: starting;CLI:starting [31](#)
 status of server agents;server agents [23](#)
 checking status [23](#)
 superuser accounts [17](#)

T

tail command [16](#)
 troubleshooting;installation:troubleshooting [27](#)

U

uninst.exe utility;Windows:uninst.exe [52](#)
 uninstallation [35](#)
 uninstallation:lab evaluation [54](#)
 uninstallation:Linux;uninstall_cnr
 utility;Linux:uninstall_cnr;Linux:uninstallation [36](#)
 uninstallation:Windows;Windows:uninstallation programs [35](#)
 unpacking the media;gtar utility;gtar;Linux:gtar [19](#)
 unpacking the media;gtar utility;Linux:gtar [19](#)
 upgrade [17](#)
 system privileges [17](#)

V

virtual appliance: booting and configuring [40](#)
 virtual appliance: installing and configuring [38](#)
 virtual appliance: managing [43](#)
 virtual appliance: upgrading [43](#)
 virtual appliance:deploying [39, 41, 42](#)
 virus scanning [15](#)
 excluding directories;excluding directories for virus scanning [15](#)
 VMWare vCenter [39](#)
 VMWare vSphere [39](#)

W

Web UI;web-based user interface; [1](#)
 Web UI:ciphers [59, 63](#)
 Web UI:ports;installation:Web UI port;upgrade:Web UI port [22](#)
 Web UI:requirements;CLI:requirements; [7](#)
 Windows:logging;logging:Windows [16](#)
 Windows:program run location;Windows:Start menu;Start
 menu:setup [19](#)
 Windows:requirements [8](#)