Release Notes for Cisco UCS Central, Release 1.5

First Published: 2016-07-29

Last Modified: 2017-02-28

Introduction

This document describes system requirements, new features, resolved caveats, known caveats, and open caveats with workarounds for Cisco UCS Central software Release 1.5. This document also includes information that became available after the technical documentation was published.

Make sure to review other available documentation on Cisco.com to obtain current information on Cisco UCS Central.

Revision History

Release	Date	Description
1.5(1a)	July 29, 2016	Created release notes for Cisco UCS Central Release 1.5(1a).
—	September 17, 2016	Added Cisco UCS S3260 Storage Server support.
1.5(1b)	September 28, 2016	Created release notes for Cisco UCS Central, release 1.5(1b).
—	October 31, 2016	Added table for supported versions of Cisco UCS Manager.
—	January 03, 2017	Modified supported version of Cisco UCS Manager for Admin Host port for PCI placement.
—	January 17, 2017	Updated supported Cisco UCS Manager version for Maintenance Policy on next reboot.
—	January 18, 2017	Added deprecation announcement for the Statistics Management feature.

Release	Date	Description
—	January 30, 2017	Added guidelines for Cisco UCS Domain Management from Cisco UCS Central.
—	February 01, 2017	Added guidelines for downloading firmware images from Cisco.com.
1.5(1c)	February 28, 2017	Created release notes for Cisco UCS Central, release 1.5(1c).

Guidelines for Cisco UCS Domain Management from UCS Central

Cisco recommends the following guidelines for managing Cisco UCS domains from Cisco UCS Central:

- Cisco recommends that you always register Cisco UCS domains using Cisco UCS Central's Fully Qualified Domain Name (FQDN). If domains are registered with FQDN, any change in the Cisco UCS Central IP address is transparent to the domain.
  - Cisco UCS Central does not support changing Cisco UCS Central's IP address if a Cisco UCS domain is registered with a Cisco UCS Central IP address. For more information about **Changing a Cisco UCS Central IP Address**, see Cisco UCS Central Installation and Upgrade Guide.
- You can migrate a Cisco UCS Central instance to support Data Center migration or disaster recovery scenarios. For more information about migrating a Cisco UCS Central instance, see the **Cisco UCS Central Instance Migration** section in the Cisco UCS Central Installation and Upgrade Guide.
- Unregistering a registered Cisco UCS domain in a production system has serious implications. Do not unregister a Cisco UCS domain unless you choose to permanently not manage it again from Cisco UCS Central. For more information about registering and unregistering a Cisco UCS Domain from Cisco UCS Central, see the **Cisco UCS Domains and Cisco UCS Central** section in the Cisco UCS Central Installation and Upgrade Guide.

  When you unregister any registered Cisco UCS domain from Cisco UCS Central:

  - You can no longer manage the service profiles, policies, and other configuration for the Cisco UCS domain from Cisco UCS Central.
  - All global service profiles and policies become local and continue to operate as local entities. When you re-register the domain, the service profiles, and polices remain local.

Caution Cisco recommends that you contact Cisco Technical Support if you want to unregister any registered Cisco UCS Domain in a production system.

See Related Documentation, on page 16 on Cisco.com for current information on Cisco UCS Central.

System Requirements

Supported Browsers

To access the Cisco UCS Central GUI, your computer must meet or exceed the following minimum system requirements:

- Windows
  - Internet Explorer 11 and above
  - Firefox 45.0.2 and above
  - Chrome 49 and above
- Linux RHEL
  - Firefox 45.0.2 and above
  - Chrome 49 and above
- MacOS
  - Firefox 45.0.2 and above
  - Chrome 49 and above
  - Safari 9.0.3 and above

Supported Operating Systems

The released ISO is supported by the following:

- VMWare ESXi5.0 U3, ESXi5.1, ESXi5.5, and ESXi 6.0 U1b
- Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016
- KVM Hypervisor on Redhat Enterprise Linux 6.5 and 7.2

The released OVA is supported by VMWare ESXi5.0 U3, ESXi5.1, ESXi5.5, and ESXi 6.0 U1b.

Changes in Cisco UCS Central, Release 1.5

New Software Features in Release 1.5(1a)

This release includes full support for the HTML5-based user interface, which is now the default user interface. The previous flash-based user interface is available at `http://UCSCentral_IP/flex.html`.

Note The flash-based user interface is being deprecated, and will not be supported after Cisco UCS Central release 1.5.

Release 1.5(1a) supports the following new features in the HTML 5-based user interface:

Feature	Functions
Support for 160 LDAP group maps	Allows 160 LDAP group maps to be managed from Cisco UCS Central.
vNIC/vHBA pairing	Allows you to create redundancy pairs for vNICs and vHBAs.
Traffic monitoring	Allows you to use Switched Port Analyzer (SPAN) to monitor network traffic.
UUID sync	Enables syncing of UUIDs to match operating systems on M3 and above servers.
Admin host port for PCI placement	Allows you to select an admin host port for vNICs or vHBAs attached to vCONs.
Object tagging	Allows you to create tags to organize objects, run infrastructure firmware updates, and run the hardware compatibility report.
Infrastructure firmware updates with tags	Allows you to run infrastructure firmware updates outside of domain groups.
Hardware compatibility report	Allows you to check interoperability information for Cisco UCS components and configurations.
Domain registration from Cisco UCS Central.	Allows you to register domains directly from Cisco UCS Central instead of Cisco UCS Manager.
Local service profile views	Service profiles created in Cisco UCS Manager can now be viewed in Cisco UCS Central.
Enhanced error messaging	Added additional text to clarify error messages.

Feature	Functions
UI localization	Added UI support for the following languages: • Spanish • German • Italian • Japanese • Korean • Chinese (mainland China)
Tech support enhancements	Allows you to generate a tech support file for servers, chassis, FEX, and other options.

Behavior Changes in Release 1.5

Deprecation Announcements

- Cisco UCS M-Series Modular Servers have been deprecated and will not be supported in Cisco UCS Central release 1.5.
- The Statistics Management feature is being deprecated and will not be supported after Cisco UCS Central release 1.5.
- After March 3, 2017, Cisco UCS Central version 1.4 or earlier will be unable to fetch the updated firmware image list from Cisco.com. If you are running Cisco UCS Central version 1.4 or earlier, you can manually download firmware images directly from Cisco.com and import them to Cisco UCS Central. To continue to have Cisco UCS Central fetch the available image data from Cisco.com and place the firmware image in the **Image Library**, Cisco recommends that you upgrade to Cisco UCS Central release 1.5 or later.

Feature Support

RDM-based shared storage for Cisco UCS Central HA configurations is no longer supported with Cisco UCS Central release 1.5.

The following features that are available in the older flash-based user interface are not supported in the HTML5 user interface at this time:

- Policy Import
- Threshold Policy
- Statistics

Note Any functionality introduced in Cisco UCS Central release 1.4(1a) and newer releases will be available in the HTML 5 user interface only.

Behavior Changes Based on Design

- You must create the global service profile template before you can create a service profile.
- vNIC and vHBA Placement is now referred to as Interface Placement.
- Registration Policy is now referred to as Domain Group Qualification Policy.
- ID Range Qualification Policy is now referred to as ID Range Access Control Policy.
- There are no qualified IP addresses for ID Range Access Control Policy.
- Only the configuration export (all-config) and backup (full-state) options are used in Cisco UCS Central. Other backup types such as config logical and config system are not supported.

Feature Support Matrix

Cisco UCS Central 1.5(1b) supports Cisco UCS Manager versions 2.1 and later, up to and including 3.1(2). The following table lists the compatible versions of Cisco UCS Central and Cisco UCS Manager.

Cisco UCS Central	Supported versions of Cisco UCS Manager
1.5	2.1, 2.2, 3.0, 3.1 up to 3.1(2)
1.4	2.1, 2.2 up to 2.2(8), 3.0, 3.1 up to 3.1(1)
1.3	2.1, 2.2 up to 2.2(6)

The following tables provides a list of specific features in Cisco UCS Central, and the Cisco UCS Manager release versions in which these features are supported:

Note Some features are built in Cisco UCS Central to be compatible with upcoming Cisco UCS Manager releases.

Feature Support for Release 1.5

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1
Cisco UCS S3260 Storage Server support	1.5(1a)	No	No	No	3.1(2) and later
vNIC/vHBA pairing	1.5(1a)	No	2.2(7) and later	No	3.1(2) and later
Traffic monitoring	1.5(1a)	No	2.2(7) and later	No	3.1(1) and later
UUID sync	1.5(1a)	No	2.2(7) and later	No	3.1(2) and later
Admin host port for PCI placement	1.5(1a)	No	No	No	3.1(1e) and later
Support for 160 LDAP group maps	1.5(1a)	No	2.2(8) and later	No	3.1(2) and later

Feature Support for Release 1.4

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Port Configuration	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later
Advanced Local Storage Configuration	1.4(1a)	No	2.2(7) and later	2.5(1) and later	No	3.1(1) and later
Multiple LUNs in Boot Policy	1.4(1a)	No	2.2(7) and later	2.5(1) and later	No	3.1(1) and later
Consistent Device Naming	1.4(1a)	No	2.2(4) and later	2.5(1) and later	3.0(1) and later	3.1(1) and later
Direct-Attached Storage/FC Zoning	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Advanced Host Firmware Pack	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
usNIC Connection Policy	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
VMQ Connection Policy	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
Equipment Policies	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later
Maintenance Policy on Next Reboot	1.4(1a)	No	No	No	No	3.1(1) and later

Feature Support for Release 1.3 and earlier

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Multi-version management support and viewing supported Cisco UCS Manager features	1.1(2a)	No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Importing policy/policy component and resources		No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Specifying remote location for backup image files		No	2.2(2b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
3rd party certificate		No	2.2(2c) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
IPv6 inband management support		No	2.2(2c) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Estimate Impact on Reconnect	1.2(1a)	No	2.2(3a) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Precision Boot Order Control		No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Scriptable vMedia	1.2(1e) and later	No	2.2(2c) and later	2.5(1a) and later	3.0(2c) and later	3.1(1a) and later

Note

- Searching for policy/policy components or resources is supported in Cisco UCS Manager, releases 2.1(2x) and 2.1(3x). To import policies, you must have Cisco UCS Manager, releases 2.2(1b) or higher.
- For precision boot order control, the blade server must have CIMC version 2.2(1b) or above.

Upgrade Paths

You can upgrade Cisco UCS Central to release 1.5(1a) from any of the following releases:

- From 1.3 to 1.5(1a)
- From 1.4 to 1.5(1a)

Note For information about how to upgrade to previous releases of Cisco UCS Central, see the installation and upgrade guide for that release.

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Defect ID	Symptom	Workaround
CSCus21388	In a cluster set up, when the RDM shared storage link goes down on the primary node, DMEs cannot write to the database. This causes a crash on the primary node and failover to the subordinate node. The subordinate node takes over as the primary node. The database is then mounted in read-write mode on the new primary node. Because the RDM link is down, umount fails on the old primary node. When the RDM link comes up, the database is mounted on the old primary (current subordinate) node in read-only mode.	Restart pmon services on the current subordinate node or restart the node itself. Either of these processes will unmount the read-only partition and enable proper cleanup.

CSCuy37428
CSCuv32055
	When registering a Cisco UCS domain immediately after installation, you may see one of the following issues:
	• After installing Cisco UCS Central on RHEL 7.2 KVM, domain registration fails.
	• After installing Cisco UCS Central on VMware using the ISO image, domain registration may fail due to a time sync issue between Cisco UCS Manager and Cisco UCS Central.
		If this issue occurs, regenerate the certificate manually from the CLI in Cisco UCS Central using the following commands:
		`# connect policy-mgr`
		`# scope org`
		`# scope device-profile`
		`# scope security`
		`# scope keyring default`
		`# set regenerate yes`
		`# commit-buffer`

—	When using the Cisco UCS Central HTML5 GUI, you may experience display issues such as missing icons or unclear fonts.	Clear your browser cache and restart the Cisco UCS Central HTML5 GUI.

Defect ID	Symptom	Workaround
CSCux75985 CSCuy07572	Excluding components from the host firmware package policy is supported in Cisco UCS Manager release 2.2.7 and above. When excluding components, you should be aware of the following: • The global-default host firmware package policy includes all components, but if you create a new custom host firmware package policy, the local disk component is automatically excluded. • Host firmware package policies created in Cisco UCS Central 1.3 or previous do not support excluding components. These policies are not changed when you upgrade to Cisco UCS Central release 1.5. • If you create your own custom host firmware package policy with excluded components, including the local disk component that is excluded by default, you cannot include that host firmware package policy in a service profile associated with a server running a Cisco UCS Manager version prior to 2.2.7. If you do, you will see the following error during service profile association: `ucs domain does not have the matching server capabilities for this service-profile`	If you have issues with your custom host firmware package policies that include excluded components, you can either remove all excluded components in the host firmware package policy, or upgrade your version of Cisco UCS Manager to release 2.2.7 or above.

Security Fixes

The following security fixes are resolved:

Release	Defect ID	CVE ID	Symptom
1.5(1a)	CSCuy54500	CVE-2016-0800, CVE-2016-0705, CVE-2016-0798, CVE-2016-0797, CVE-2016-0799, CVE-2016-0702, CVE-2016-0703, CVE-2016-0704	A vulnerability in OpenSSL and the TLS protocol has been addressed.
	CSCuz52405	CVE-2016-2108, CVE-2016-2107, CVE-2016-2105, CVE-2016-2106, CVE-2016-2109, CVE-2016-2176	A vulnerability in OpenSSL has been addressed.
	CSCuz92669	CVE-2016-4957, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956	A vulnerability in NTPd has been addressed.

Resolved Caveats for Release 1.5(1c)

Resolved Caveats in Release 1.5(1c)

The following caveats are resolved in Release 1.5(1c):

Defect ID	Symptom
CSCvc34642	Cisco UCS Central now displays the availability status of Cisco S3260 chassis, and displays only the available chassis during manual association to a chassis profile.
CSCva04178	A service profile in Cisco UCS Central no longer displays a different association status as that in Cisco UCS Manager.
CSCvc34656	Certain remote operations on the LUNs, such as bringing a LUN online, no longer fail when initiated from Cisco UCS Central when global service profiles are configured using a storage profile.
CSCvb59957	Cisco UCS Central HTML UI dashboard now displays Faults, Events, and Audit logs. These were not displayed in Cisco UCS Central releases 1.5(1a) and 1.5(1b) because of incorrect file permissions.

Resolved Caveats for Release 1.5(1b)

Resolved Caveats in Release 1.5(1b)

The following caveats are resolved in Release 1.5(1b):

Defect ID	Symptom
CSCuz25412	Legacy licensing expired faults no longer show up after enabling Smart Licensing.
CSCuz81757	Service profile association no longer fails with the FSM config error `identpoolDomain already attached`.
CSCva67779	Undeployed LUN becomes Online causing GSP config failure.
CSCva74219	In the Global BIOS Policy, **Power Management** and **Energy Performance** property values can now be set to Performance.
CSCva74326	Cisco UCS Central 1.5 HTML GUI accepts bind password when the password contains special characters such as + - ; | / \ ~ `
CSCva76835	Cisco UCS Central 1.5 HTML GUI is responsive after httpd gets restarted.
CSCva78188	Domain registration and hardware compatibility tables now refresh status automatically.
CSCva78997	Cisco UCS Central 1.5 HTML GUI setup with FQDN name is now accessible when the `mgmt IP` of the network interface on Cisco UCS Central is changed.
CSCva89609	When **user-ack** is triggered for the Chassis Profile changes in the Cisco UCS Central 1.5 HTML GUI, global 'pending activities' does not refresh after acknowledgment.
CSCva90596	HFP Policy with some excluded components does not resolve in 3.1(1) Cisco UCS Manager, when storage bridge device and sas expander regular firmware options are selected.
CSCva93540	vMedia policy with filename generated by SPName option is now resolved.
CSCva95505	Cisco UCS Central GUI now supports the use of special character (**"**) in the password for a LDAP user or a local user.
CSCvb05938	Cisco UCS Central certificate now maintains the name fields **organization name (O) and (OU)** uniformly from both the GUI and CLI.
CSCvb17347	Core dme no longer crashes due to SNMP query.
CSCvb19428	Cisco UCS Central does not lock user account during external authentication like LDAP.

Open and Resolved Caveats for Release 1.5(1a)

Open Caveats in Release 1.5(1a)

The following caveats are open in Release 1.5(1a):

Defect ID	Symptom	Workaround
CSCuz88613	In HA mode, the VIP fails to come up and the DB fails to load after admin failover is triggered and the primary node reboots immediately.	Restart pmon on the primary node.
CSCva56392	If you register a Cisco UCS immediately after installing Cisco UCS Central, then take a full state backup and restore the backup on a new VM, you may experience core dumps.	Contact Cisco TAC. To avoid this issue, after you install Cisco UCS Central, wait at least 5 minutes before registering a domain. At that point, you can take a full state backup.

CSCux06188	After decommissioning a server, the server slot number cannot be recognized.	Acknowledge the slot using the CLI. For example:
		`UCSC# connect resource-mgr`
		`ucsc(resource-mgr) # scope domain-mgmt`
		`ucsc(resource-mgr) /domain-mgmt # scope ucs-domain 1008`
		`ucsc(resource-mgr) /domain-mgmt/ucs-domain # acknowledge slot 1/8`
		`ucsc(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer`
		`ucsc(resource-mgr) /domain-mgmt/ucs-domain #`

CSCuz65590	If you change a WWXN pool to a static ID on an associated global service profile, Cisco UCS Manager will assign IDs to the vHBAs that are different from the IDs in Cisco UCS Central.	Assign new IDs to the vHBAs in Cisco UCS Central.
CSCuz67168	If you change a static IP in a service profile to pool, the global service profile may get a different IP.	Either leave the IP set to static ID, or use a pool with a static ID inside it.

Resolved Caveats in Release 1.5(1a)

The following caveats are resolved in Release 1.5(1a):

Defect ID	Symptom
CSCva11498	Cisco UCS Central messages file no longer grows extremely large.
CSCva42074	Cisco UCS Central in an HA pair no longer fails to receive the inventory update from the domain if a failover happens during upgrade.
CSCuy09692	Remote backups using FTP/TFTP no longer use an incorrect transfer mode.
CSCuy30580	Launching Cisco UCS Manager from Cisco UCS Central no longer fails when the certificate is installed using FQDN.
CSCuz22744	Cisco UCS Central no longer fails to check for duplicate VSAN IDs before deploying a global service profile.
CSCuz50941	Entering a SAN boot target no longer fails with certain WWNs or WWN blocks.
CSCuz72748	Renaming service profiles when config FSM is running no longer generates new IDs.
CSCuz74516	Service profiles no longer fail to associate with Cisco UCS Mini.
CSCva08192	Smart licensing no longer temporarily reverts to showing traditional licensing in the GUI.
CSCva08213	Smart Licensing no longer displays the incorrect time.
CSCva17240	Upgrading Cisco UCS Central with Smart Call Home enabled no longer causes a core dump.
CSCva24775	Adding a FC adapter policy to a vHBA no longer fails when it is created using a template.
CSCva40791	Using the estimate impact tool when creating a new organization no longer causes a core dump.
CSCva45134	Scheduled backups no longer after upgrading a Cisco UCS domain if the IP address is changed before the upgrade.
CSCuz09943	The backup/restore widget no longer fails to display the correct information.
CSCva05601	When you use the domain qualification policy to add IP IDs to a service profile, the IDs are now released back to the IP pool when the service profile is disassociated.
CSCup18781	Global service profile template names are now pushed to global service profiles on a Cisco UCS domain.
CSCva37187	Firmware image catalogs no longer fail to download when using an authenticated proxy.

Related Documentation

In addition to these release notes, you can find documentation for Cisco UCS Central in the following locations on Cisco.com:

- Cisco UCS Documentation Roadmap
- Cisco UCS Central Install and Upgrade Guides
- Cisco UCS Central Configuration Guides
- Cisco UCS Central Videos
- Cisco UCS Central CLI Reference Manual
- Cisco UCS Central Best Practices and Operations

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 NONINFRINGEMENT 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: 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. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.