Patching Fundamentals
Avaya Communication Server 1000

Release 7.6
NN43001-407
Issue 04.01
March 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third

parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release

The following sections detail what's new in *Patching Fundamentals*, (NN43001-407) for Avaya Communication Server 1000 (Avaya CS 1000).

Features

There are no updates to the feature descriptions in this document.

Other changes

Revision history

March 2013	Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.6.
May 2012	Standard 03.03. This document is up-issued to add special patching instructions to the Central and Local Patching sections.
May 2011	Standard 03.02. This document is up-issued to add technical information about hard drive space limitations when installing Service Packs on systems using CP PM Co-res as the Primary Server.
November 2010	Standard 03.01. This document is up-issued for Avaya Communication Server 1000 Release 7.5.
June 2010	Standard 02.01. This document is up-issued for Avaya Communication Server 1000 Release 7.0.
June 2009	Standard 01.03. This document is updated for Communication Server 1000 Release 6.0.
May 2009	Standard 01.02. This document is up-issued for Communication Server 1000 Release 6.0.

May 2009	Standard 01.01. This is a new document for Communication Server 1000 Release 6.0.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

This document contains the following topics:

Subject

This document describes how to patch your system using Patching Manager and CLI commands.

Important:

Before patching your system using the Patching Manager, make sure you consider concurrent coordinated patching of your entire system (in particular, with the Call Server).

Legacy products and releases

This document contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 (Avaya CS 1000) software. For more information about legacy products and releases, go to Avaya home page:

WWW.AVAYA.COM

Applicable systems

This document applies to the following systems:

- Avaya Communication Server 1000M Single Group (Avaya CS 1000M SG)
- Avaya Communication Server 1000M Multi Group (Avaya CS 1000M MG)
- Avaya Communication Server 1000E (Avaya CS 1000E)

Intended audience

This document is intended for individuals who administer Avaya Communication Server 1000 systems.

Conventions

Terminology

In this document, the following systems are referred to generically as system:

- Avaya Communication Server 1000E (Avaya CS 1000E)
- Avaya Communication Server 1000M (Avaya CS 1000M)

Unless specifically stated otherwise, the term Element Manager refers to the Avaya Communication Server 1000 Element Manager.

Related information

This section lists information sources that relate to this document.

Technical documentation

This document references the following technical documents:

- *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*
- *Avaya Subscriber Manager Fundamentals, NN43001-120*
- *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Avaya SIP Line Fundamentals, NN43001-508*
- *Avaya Network Routing Service Fundamentals , NN43001-564*
- *Avaya Element Manager System Reference - Administration, NN43001-632*

Online

To access Avaya documentation online, go to Avaya home page:

WWW.AVAYA.COM

Chapter 4: Overview

Patching Manager supports the activation and deactivation of Linux patches, binary patches, deplists, and loadware for VxWorks and Linux-based Call Servers and Media Cards.

Patching Manager supports the following corrective content categories:

- Patch—Patches are used to fix bugs or for diagnostic purposes. In some instances, you can apply this category of patch without a program restart.
- Serviceability update—A serviceability update (SU) is a full-application RPM Package Manager (RPM) package distribution that you apply to a specific application, and replaces previous serviceability updates. An RPM is a Linux software standard for software updates.
- Service pack—A service pack (SP) is a single file that contains a bundle of multiple patches and serviceability updates for a specific product release.
- Deplist—A deplist is a single file containing a bundle of binary patches that are specific to a particular target type and product release.
- Loadware—A loadware file updates a IPMG or PDSL MGC.

This chapter contains the following topics:

Remote broadband connection

To successfully patch your system, you must have a secure remote broadband connection. This remote broadband connection is required to transfer files and to connect to the UCM interface.

Patches, serviceability updates, binary patches, deplists, loadware, and service packs range in file size. Patches are small (a few kilobytes) while service packs can be 100 megabytes (MB)

or greater in size. You need a secure broadband connection to successfully transfer these files to your target system.

Linux patches

Linux patching involves the patching of a specific version of an RPM. The RPM is the base building block of the Linux patching process.

RPM patches are issued only as serviceability updates and each serviceability update can contain only one RPM. Serviceability updates have the same file name as the RPM file that it contains; however, the serviceability update has a different file extension.

Patches are created and distributed against a specific RPM name and release. Patches have unique patch names, which are automatically generated by the patch library. Binary patches are linked to the RPM using the patch header.

All other patches on Linux (such as JAR, WAR, and FRU) are treated in the same manner and each is tied to a specific version or release of an RPM.

As a result, only two types of corrective content distributions exist for Linux:

- Serviceability updates on page 18
- Linux patches on page 20

Important:

In this document, the term patch or patches includes both patches and serviceability updates (SUs) unless explicitly mentioned otherwise because patches and SUs are applied in the same way.

Linux also supports service packs. A service pack is a single file containing multiple patches and serviceability updates for a specific product release. For more information, see Linux service packs on page 21.

Patches cannot cross RPM boundaries. For example, a JAR patch cannot replace files in several RPMs. Patches and serviceability updates do not change the release of applications on the target.

Serviceability updates

Linux serviceability updates (SUs) are used to deliver new and updated RPMs to the target server.

A serviceability update contains the following:

- A header—The header information contains the product releases to which the SU is applicable. When the SU is loaded, the product release of the target is validated. If there is no match, the SU does not load.
- Two optional script files—A pre-patch script file (preScript.pl) and post-patch script file (postScript.pl). These files are predefined and are case sensitive.
- One optional readme file
- One RPM file

After the patch command finishes, if a post-patch script file is included with the patch, it loads and runs. If the post-patching script fails, then an attempt is made to reverse the operation. For example, if the script operation was an installation, then the script attempts to take it out of service.

In some cases, reversing the script may not succeed; for example, trying to remove an SU that is not removable. The SU has identification in the header on whether they are removable. Only kernel RPMs are known not to be removable. If you need to return to a previous state, Avaya must provide another SU to reverse the changes.

Because serviceability updates only replace RPMs, the version of the applications does not change.

Important:

The **swVersionShow** command is not always affected by installing a serviceability update.

Serviceability updates are stored in the Serviceability Updates section of the patch library. (Patches are stored in a different area.) Serviceability updates are linked to the patching section of the patch library as releases of software. Each RPM is treated as its own release so patches can link it. The serviceability update is also linked in patch library to each product release for which it is applicable.

Naming conventions

The file name for a serviceability update is identical to the name of the RPM it contains. The file extension is changed from .rpm to .XXX.ntl (XXX is a unique number assigned by patch library and is the patch library issue of the SU). This naming convention follows the standard for RPM files but also allows for differences for Avaya purposes.

Important:

Do not rename a serviceability update. The patching framework validates the serviceability update file name against the header contents.

The serviceability update file name contains the RPM name and release information for the RPM which, by default, is the name and release of the SU. The SU naming convention can therefore take into account third-party RPMs and Avaya-generated RPMs. Because the SU contains a new version of an RPM, this version replaces the version on the target and appears

in commands that display RPM information. If there is any change (other than a RPM change), then the patch library issue is changed.

For example, the RPM file name for the minicom RPM is minicom-2.1-3.rpm

The first serviceability update issued is called minicom-2.1-3.000.ntl.

If there is a change and the readme file has to be modified, then the SU is upissued in patch library. The new SU is named minicom-2.1-3.001.ntl.

The naming convention identifies the exact contents of the file while preserving the RPM. As a result, an SU can be upissued and all patches still apply to the original minicom RPM with no changes or the need to be re-released.

If the minicom RPM changes release then all the patches are no longer applicable because all patches link to the RPM contained in the serviceability update.

For example, if the minicom RPM was changed to minicom-2.1-4, then the new serviceability update is called minicom-2.1-4.000.ntl.

Linux patches

Three types of Linux patches are available:

- File Replacement Update (FRU)—An FRU is a simple patch type in that no extra packages must be generated for target file updates. An FRU can be used for replace files, but files cannot be removed from the target machine using a FRU patch.
- Java Archive (JAR)—A JAR patch aggregates many files into one. Software developers generally use .jar files to distribute Java classes and associated metadata. Due to the way CS 1000 makes use of the J2EE (JBoss) applications, then it uses hierarchical class loaders. Therefore, the JAR is currently distributed using the FRU mechanism.
- Web Application Archive (WAR)—A WAR patch is a JAR file used to distribute a collection of JavaServer Pages, servlets, Java classes, XML files, tag libraries, and static Web pages (HTML and related files) that together constitute a Web application.

A patch contains the following:

- Header—The patch header contains information about applications and the product release.
- Optional scripts—Patches have optional scripts that function the same as the optional scripts for SUs.

Patches must be created against a specific name and version of an RPM. This information is in the file name of the RPM. The RPM file name is stored in the patch header and links the patch to the specific RPM for which it was created.

Important:

Do not rename patches. The patching framework validates the patch file name against the header contents.

Linux patches are stored in the patch library in the same location as patches for the VxWorks platforms. Patches are stored against the RPM name and release they are linked to. In the patch library, links exist from the RPM to all related patches.

When you load a patch, the version and name of the RPM (which the patch is linked to) is checked. If the RPM name does not exist or if the RPM version does not match, then the patch is not loaded. Patching Manager filters out patches with a patch header product release that does not match the product release of the target.

Linux service packs

A service pack (SP) is a single file containing multiple patches and serviceability updates for a specific product release. The files are bundled in the service pack and a list of files is placed in the header. The service pack can also have optional script files attached that are similar to the scripts attached to an individual patch or serviceability update.

Individual patches and serviceability updates are extracted from the service pack and automatically placed in service. All patches and serviceability updates from the elements which are not in the header of the service pack are removed. The removal occurs automatically without prompting the user for input.

A service pack file has a .ntl file extension.

Important:

Do not change the .ntl file extension. A service pack file name can be renamed to help you keep track of your updates using your preferred naming conventions. However, you must not change the .ntl file extension.

A service pack file can be large if it includes serviceability updates. Use the Meridian ISSP Report and Conflict Checker (MIRCC) to reduce the size of the service pack file. The MIRCC is on the ESPL. Service Packs can be dynamic and tailored to specific installations in the patch library similar to the deplist process by the use of the MIRCC tool. You can use the **`issp`** command on the target to list all installed RPMs, patches, and serviceability updates. MIRCC uses this information to include only the necessary files in the service pack to make the target current. The header file for the service pack contains the list of all serviceability updates and patches that MIRCC determined are needed to be running on the target. However, because the target can already have some of these files installed, only the missing files are included in the service pack. When the service pack reaches the target, the header information is used to determine which patches remain on the target element, which are removed, and which require updating.

Three types of service packs are available:

- Standard service pack—A standard service pack contains the generally available and emergency patches for a specified release.
- Standard + Site-specific service pack—A site-specific service pack contains additional patches or serviceability updates that are not in the standard service pack. These can be debug or limited customer-specific patches. The site-specific service pack may be missing patches or serviceability updates that are in the standard service pack. This can occur,

for example, if an added serviceability updates replaces another serviceability updates that is in the standard service pack. Another case is if an added patch conflicts with another patch that is in the standard service pack.

- Target-specific service pack—A target-specific service pack is generated for a specific element. The service pack is obtained by passing in ISSP command output from the target element to the MIRCC tool. Any debug or limited customer-specific patches that are on the target are retained.

The first two types of service packs contain all the actual patches and serviceability updates for all applications. The target-specific service pack has a header that indicates all the required patches and serviceability updates for the target element. This list depends on the applications installed on the target element. The target-specific service pack only contains actual patches and serviceability updates that are not already present on the target element.

Consider the following when you apply service packs to target elements:

- If a target element has any debug or limited customer-specific patches, then application of a standard service results in removal of these patches. Either a site-specific service pack containing these special patches must be used, or a target-specific service must be generated for the target element.

  Important:

  Applying a service pack will remove customer patches.

- A target-specific service pack is intended for a specific target element. However, you can apply such service packs to other targets but there may be errors. If the other targets do not have the same applications as on the intended target, then patches or serviceability updates may be missing and are not applied. If the other targets do not have the same patches and serviceability updates already installed as on the intended target, and these are still required, there are errors because these items are not in the service pack. This could include debug or limited customer-specific patches that are only on the intended target prior to generating the target-specific service pack. If other targets have other debug or limited customer-specific patches that are not on the intended target, these are removed after you apply the service pack.

Individual patches and serviceability updates contain which applications are stopped and started when they are placed in service. When a service pack is placed in service, the following events occur:

- Applications are stopped as requested by each patch or serviceability update.
- Applications do not start until the entire service pack is loaded.
- A list of applications to restart is maintained as each patch and serviceability update is loaded.
- Applications start automatically at the end of the service pack installation.

A service pack cannot be backed out. To reverse the changes put in by a service pack, you can do the either of the following:

- Reapply a previous service pack for the current release (if available)—If the service pack is updating from a previous service pack, then you can reapply that previous service pack. The previous service pack being reapplied must contain all removed patches.
- Note all the changes made by the service pack—Note the patches and serviceability updates that were added, the patches that were removed, and then reverse the changes. You may need to obtain individual patches from the patch library to complete this process.

VxWorks deplists

Deplists are single files that contain multiple binary patches specific to a particular VxWorks target type and product release. You can manage deplists using the central patch library.

VxWorks patches

The following types of VxWorks patches are available: binary patches, deplists, and MGC loadware. You can manage these patches using the central patch library.

Loadware

There are two types of loadware updates available for MGCs: PSDL and IPMG. You can manage loadware using the central patch library.

Patch loading and unloading sequence

Use the following steps to load a service pack on the target using either the patch command line interface (CLI) commands or the Patching Manager application:

1. Remove all serviceability updates that are no longer needed or will be replaced. (The unload utility removes all patches associated with the RPM contained within the serviceability update which is being removed.)
2. Unload all patches that are no longer needed.
3. Load new serviceability updates.
4. Load new patches.

Note:

Operations such as application stop, start, restart, and system reboot are analyzed for service pack-contained patches and serviceability updates, and they are optimized to be invoked only once.

Obsolete Linux patches

The Patch Management Enhancement Feature provides functionality to automatically remove obsolete Linux patches. The header of the patch contains a list of patches that the current patch makes obsolete. The patches in this header list must be removed before this patch is placed in service. A patch can only obsolete another patch on the same RPM.

Linux patches must be removed manually when you apply individual patches. When using the Patching Manager, you are provided with this information in a service impact. You must manually remove that particular patch by using the Deactivate button within the Central Patching Manager or the Local Patching Manager. For service packs, obsolete patches are automatically removed from the target.

In Patching Manager, you can find patch obsolescence details in two ways:

- You can view individual patch details by clicking the patch name hyperlink. The obsolete patch name is in the Obsolete field on the Patch Details page. If the patch does not make another patch obsolete, then the Obsolete field says None.
- The number of patches which need to become obsolete is indicated after preprocessing the patches selected by the user. You can find the information for the patches that must become obsolete on the Patching Job Details page by clicking the Patching Status Summary hyperlink. Under the Action column, note the patch names that have Deactivate (Obsolete) displayed for the patch name.

Note:

After preprocessing individual patches, the Patching Manager provides the following message: The obsolete patches need to be deactivated before activating the selected patches.

Patch dependencies

Patches are loaded one at a time in a serial fashion. As a result, patches can only have one dependant patch. If the dependant patch (for the patch currently being loaded) is not already loaded, then the current patch is not loaded. A dependent patch must be on the same RPM.

Patching impacts

Patching operations generally require application restarts or reboots. These actions occur automatically when the service pack or patches are applied, or when patches are removed.

If any Linux base application is restarted as the result of patching operations, this results in all Avaya applications being restarted. The Call Server running on a Co-resident Call Server and Signaling Server is included as an Avaya application. Use Base Manager to determine the Avaya applications running on a target.

For Linux-based patching, service impacts are handled automatically. For VxWorks-based patching, Patching Manager indicates whether or not there is a service impact to the target and if the patch requires an administrator to manually perform it.

When the Patching Manager is used for patching, two processing methods are available:

- Review impact for each target and run individually—With this manual processing method, the impact of applying the selected service pack or patch is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) prior to initiating patching to avoid user impact.
- Run all automatically—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

⚠ Warning:

Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

In the manual mode, application restarts or reboots are flagged. Review the potential impacts and take the necessary steps before you start patching.

Important:

Avaya recommends using the manual mode of patching so you can review the impacts. The automatic mode is useful if you are patching during a maintenance window, when service impacts are permitted.

You may need to gracefully idle down the system or transfer operations to other redundant devices prior to patching. Impacts may extend to other systems in cases of network-wide virtual office or branch office scenarios. Some other applications can issue alarms or logs related to applications being restarted.

⚠ Warning:

Special attention is required if a Co-resident Call Server and Signaling Server is being patched. A reboot or restart of any Linux base application results in a restart of the Call Server component, with significant operational impact. Furthermore, any changes that were

made to the Call Server configuration but not saved using an equipment data dump (EDD) would be lost. If required, the EDD must be performed prior to patching.

Chapter 5: Patching Manager overview

The Patching Manager provides a graphical user interface (GUI) to upload and manage patches, deplists, loadware, and service packs on targets within the enterprise network. The Patching Manager facilitates the central deployment of patches to target elements within the Unified Communications Management (UCM) security domain. For more information about UCM, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

This chapter contains the following topics:

Central and Local Patching Managers

You can use Patching Manager on the primary security server to remotely deploy patches from a central location to targets within the same UCM domain (using the Central Patching Manager). You can also install patches locally. Local patching is accessible from the Base Manager of each Linux Element (using the Local Patching Manager) as well as from the local Element Manager logon for VxWorks elements.

Two interfaces support patch management:

- Central Patching Manager—The Central Patching Manager is accessible from the Primary UCM server. Central Patching Manager obtains a list of all elements in the same security domain from the UCM framework and can patch all elements in the same security domain. For more information, see Central Patching Manager on page 39.
- Local Patching Manager—The Local Patching Manager is accessible from the UCM Base Manager of each Linux element. You can access Base Manager using a central UCM logon or a local logon to the element. For more information, see Local Patching Manager on page 97.

⚠ Warning:

If installing a Service Pack on a system using a CP PM Co-res as the Primary Server, then due to hard drive space limitations, you must install the Service Pack on the Backup Server and Member Servers locally, using the Local Patching Manager.

⚠ Warning:

You cannot patch using Central Patching Manager and Local Patching Manager at the same time. You should not use the CLI patching commands while either the Central or Local Patching Manager are in use. Also, do not use Element Manager patching if the Central Patching Manager is used for VxWorks elements.

Applications

Patching Manager is a central patch deployment application used to patch software components. The following table shows the list of software components that you can patch.

Table 1: List of applications

Application	Description
Signaling Server (SS)	The Signaling Server includes the following applications: • UNIStim Line Terminal Proxy Server (UNIStim LTPS) • H.323 Gateway (H.323 GW) • Session Initiation Protocol Gateway (SIP GW) • Failsafe Network Routing Service • MySQL • IP Media Services • SIP Line (SIPL) For more information about the Signaling Server, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*. For more information about SIP Line, see *Avaya SIP Line Fundamentals, NN43001-508*.
Personal Directory (PD)	The Personal Directory allows a user to enter or copy names to a personal directory, and to edit and delete those entries. For more information about the Personal Directory application, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.
Network Routing Service (NRS)	The Network Routing Service includes the following: • SIP Proxy/Redirect Server • Gatekeeper (GK)

Application	Description
	• Network Connection Server (NCS) • NRS Manager (NRSM) • MySQL For more information about the NRS, see *Avaya Network Routing Service Fundamentals , NN43001-130*.
Element Manager (EM)	Element Management includes the following: • Element Manager (EM) with Phone configuration • MySQL For more information about Element Manager, see *Avaya Element Manager System Reference - Administration, NN43001-632*.
Subscriber Manager (SM)	Subscriber Manager provides a central location to manage subscriber information for enterprise services. For more information about Subscriber Manager, see *Avaya Subscriber Manager Fundamentals, NN43001-120*.
All other Linux applications, such as Deployment Manager, Base Manager, Patching Manager, IPSec configuration, SNMP Profile Manager.	Other Linux applications running on UCM elements.
Unified Communications Manager (UCM)	UCM provides an intuitive, common interface to manage and run managed elements. UCM is a container that stores several system management elements in a single repository. You can access all network system management elements in UCM. For more information about UCM, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.
Operating System (Linux Base)	The Avaya CS 1000 Linux base system provides a Linux server platform for applications on a Pentium server. The platform can support Session Initiation Protocol Network Redirect Server (SIP NRS) and Unified Communications Management (UCM). For more information about the Linux base, see *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.
Call Server (CS)	Call Server.
Media Cards	ITG-SA, MC32S.

Patching permissions and roles

Central Patching Manager access is controlled by having access to All Elements of type: Patching Manager for a role assigned to the user. UCM includes two built-in roles that provide this access: NetworkAdminstrator and Patcher.

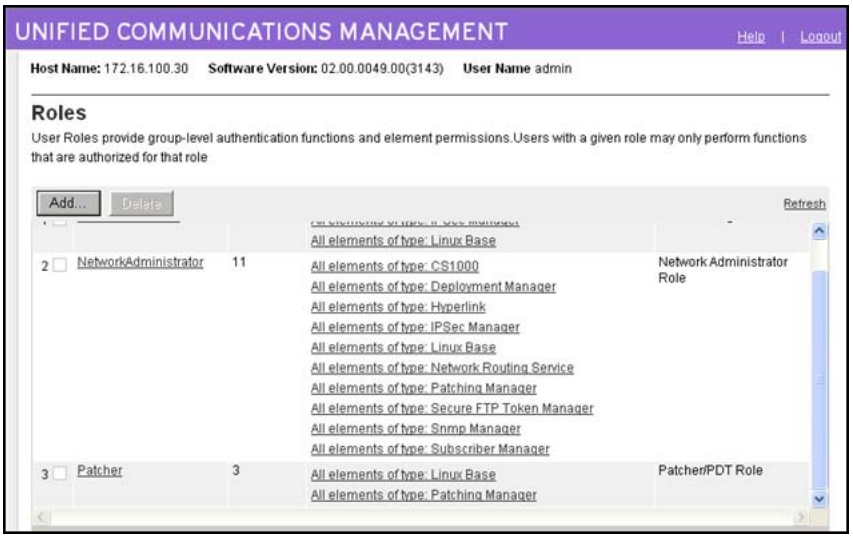

Figure 1: Roles

In the UCM navigation tree, the Patches link does not appear if you do not have a role with this access (All Elements of type: Patching Manager). To view the UCM navigation tree, see Figure 6: UCM navigation tree (Patches selected) on page 41.

The default account, called Admin, has the default NetworkAdminstrator role. To use the default Patcher role, create an account and assign the Patcher role to that account. You can also create a new role with All Elements of type: Patching Manager access and assign the role to a user.

For more information about accounts and roles, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Patching job queuing

To avoid excessive Primary UCM server resource consumption and network activity, only a limited number of patching operations can run concurrently. The activities are classified as follows:

- preprocessing to analyze the impact of patch application or deactivation, and which patches apply to targets
- actual application or deactivation of patches

Two queues are maintained for these two classes of activities. The queues hold the patching activities of all users and are maintained on a first in, first out (FIFO) basis. There is a limit imposed of three concurrent activities. For example, there can be two targets that are being preprocessed and another target being patched. If there is a mixture of preprocessing and patching activities, at least one patching activity will be running.

The patching sequence is always target preprocessing first followed by target patching:

- For automatic patch application, the activity is first in the preprocessing queue and later in the patching queue.
- For manual processing, the activity enters the patching queue after the user verifies the impact and proceeds with activation or deactivation.

At times, you may experience delays to patching activities. For example, one user may have queued patching activities for several targets. A second user initiating patching may find that activities do not start until the queued activities of the first user are complete. The In Progress tab is used to view all patching activities for all users. Use this view to estimate when activities can be initiated.

Concurrent patching operation from Patching Manager user interfaces

Multiple patch administrators can perform patching operations on various targets through different UCM sessions. Up to five administrators can perform patching operations at a time. However, different administrators are blocked from patching the same target at the same time.

Any administrator with patching permissions can see the current patching operations being performed by any other administrator. An administrator can take over any patching operation initiated by another administrator (for example, clearing completed operations, proceeding with patching). In such cases, a warning is issued that another administrator had control, and if the user proceeds they are designated as the new owner of the activity for that target.

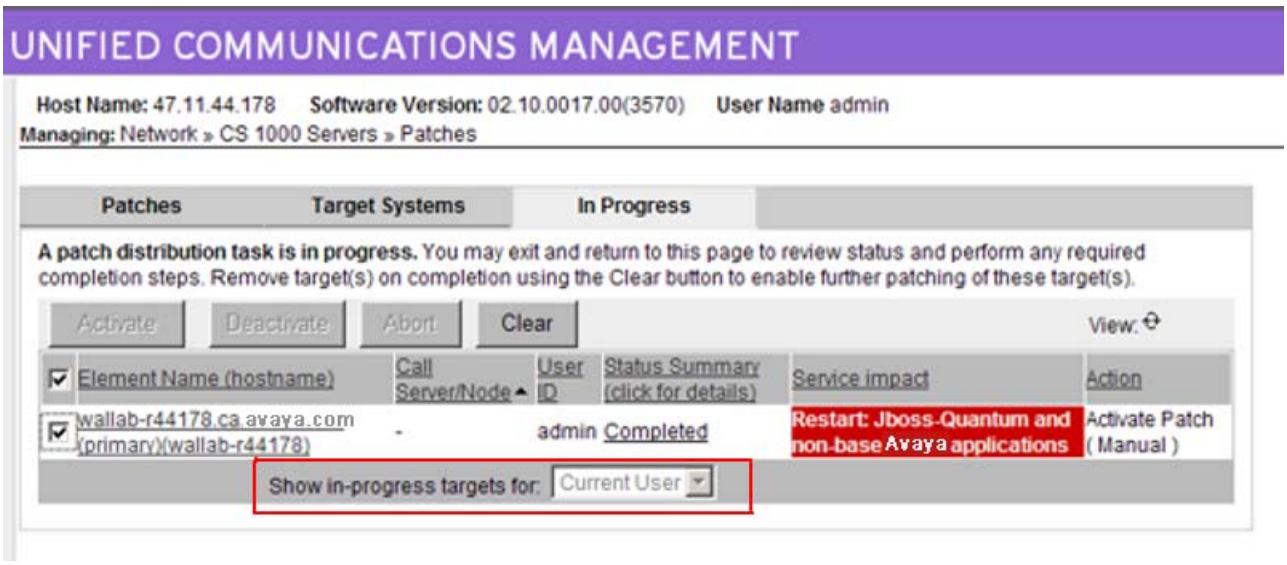

Figure 2: Show in-progress targets list

Patch libraries

Avaya supports the Enterprise Solutions PEP Library (ESPL), which provides online access to Avaya-approved Product Enhancement Package (PEP) solutions for Enterprise products. Use the ESPL Web site to download and save patches, deplists, loadware, serviceability updates, and service packs to your local PC. You must then add the files to the patch libraries using the Central or Local Patching Manager interfaces.

A single UCM security domain typically exists for every customer enterprise network. As a result, a central patch library is on the Primary UCM server for that UCM domain. Use the Central Patching Manager to add patches, deplists, loadware, serviceability updates, and service packs to the central patch library.

The Local Patching Manager supports patches, serviceability updates, and service packs in the normal storage locations as the equivalent CLI patching commands. Element Manager supports deplists and loadware. Neither the Local Patching Manager or Element Manager maintain a patch library. Each target element has a folder in which the files are stored.

In Progress status information

In both the Central and Local Patching Manager, an In Progress tab appears when patching activity occurs. This tab provides status information about the patches, serviceability updates, service impacts, deplists, loadware, and service packs being activated or deactivated on the target elements. In particular, the Status Summary column on this tab provides status information.

The status can appear as a hyperlink. Click the link to obtain additional status information.

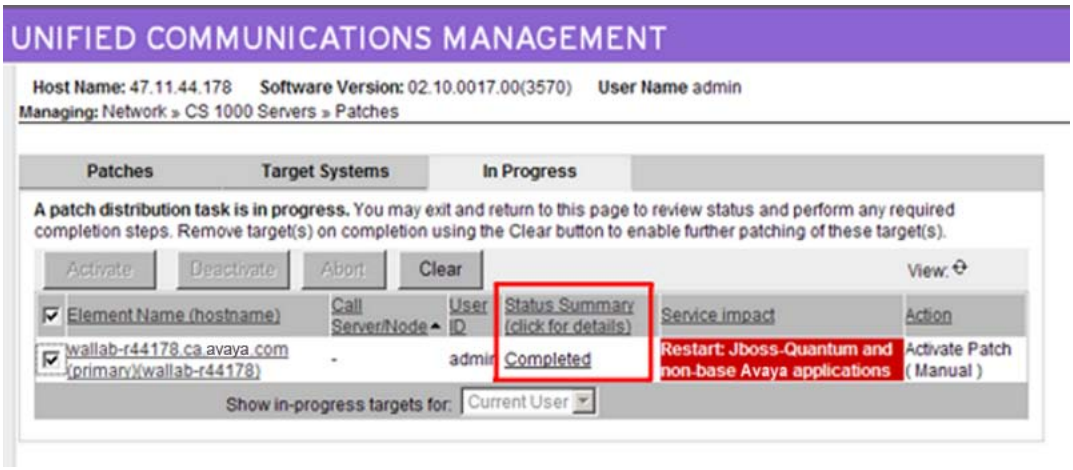

Figure 3: In Progress tab - Status Summary column

The following table lists the status summary and description information.

Table 2: Status information

Status	Description
Queued for Analysis	The target is placed into queue for analysis before preprocessing the selected patches with the target information.
Preprocessing	Currently preprocessing the selected patches with the target information. If activities are queued, it could take several minutes for the preprocessing to complete.
No Impact	This status appears after preprocessing (during patch activation process), if the selected patches are already in service on the target or the patch is not applicable if the required RPM is not installed.
Ready to load	The target is ready for patch activation process; this occurs after the preprocessing completes successfully.
No action required: Patches absent	This status appears after preprocessing (during patch deactivation process), if the selected patches are not already in service.
Ready to deactivate	The target is ready for patch deactivation process. This status appears after the preprocessing completes successfully.
Queued for patching	The target is placed into queue either for patch activation or deactivation process.
In progress	Either patch activation or deactivation is in progress on the target.
Completed	Either patch activation or deactivation completed successfully.

Status	Description
Partially Completed	Either patch activation or deactivation completed with partial success.
Failed	Either patch activation or deactivation failed.

Service impact

The Service Impact column provides a color-coded message to indicate the severity of service impacts, such as required restarts, during Linux patch activation and deactivation.

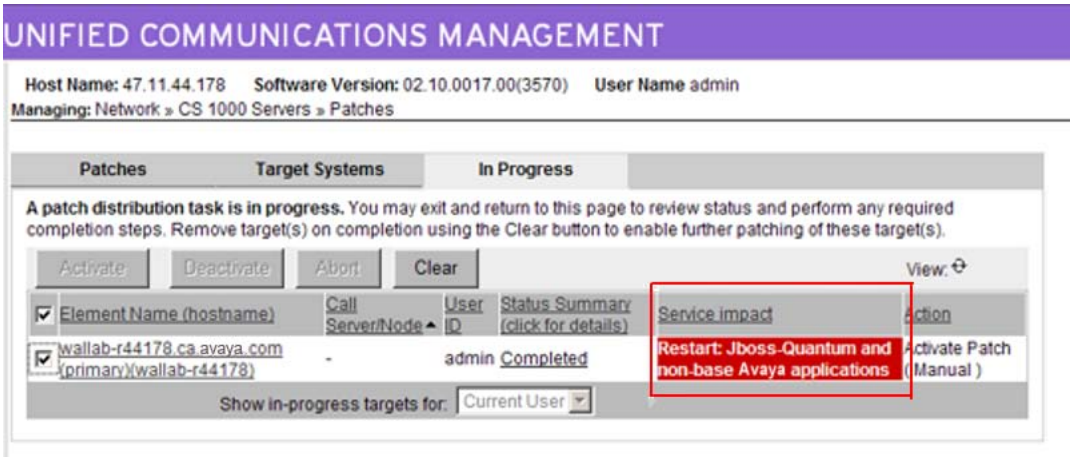

Figure 4: Service impact column

Table 3: Service impact color coding

Color	Severity
Red	Major service impact. Restart required.
Orange	Moderate service impact. Application restart only required.
White (clear)	No service impact. No restart or application restart required.

Clearing patch activities

All patching activities on a target element must be cleared on the element before further patching activities can start (such as patch activation or deactivation). Use the **Clear** button to end the patching activities for a selected target element.

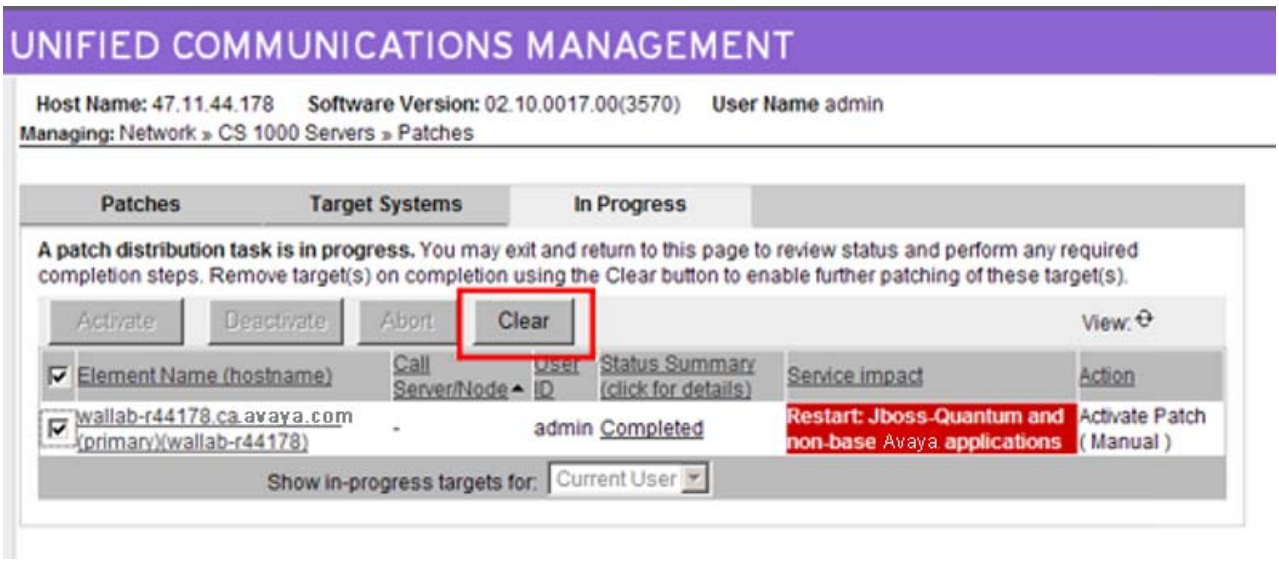

Figure 5: Clear button

Patching activation and deactivation operations cannot occur on an element if the element is cleared; that is, the target element should not appear on the **In Progress** tab.

If anyone is patching a target element, you cannot initiate new patching activities on that element. You must clear the patching before you attempt to perform patching activities.

If patching activities are in progress that are not cleared, then the **In Progress** tab appears when you log on to UCM (in addition to the Patches and Target Systems tabs). The **In Progress** tab shows the active patching activities on the elements (for you or for any other patching administrator).

The **Clear** button must not be used for targets unless the patching operation is finished. If a patching operation is taking excessively long, there could be rare cases that some internal error occurred and the patching status will never be updated. In this case, the Clear button may be used to clear out the information for the operation. A warning appears indicating that patching may still be in progress. The patching operation may have been completed or there could have been failures. After the clear, review the patching status on the target using Base Manager or the CLI, and perform the required actions.

Failure recovery

When patching activities fail, you may need to perform manual clean up activities on the patching targets. The following situations require such cleanup:

- failure of service pack activations
- failure of patch or serviceability updates activation or deactivation

These operations have several stages, such as a patch first being placed into a loaded state and then installed. If the failure occurs at a specific point, patches may move to a particular stage and have to be cleaned up. If a service pack is being activated, a failure at the loading

stage can result in some patches being loaded. The service pack does not move to the installation stage if there are loading errors, so the patches are left in that state. Similarly, there can be deactivation failures that result in patches being left in a loaded state or not deleted. Patches that are being activated, can also be left in a loaded state if installation fails.

The following are related clean up activities. These relate to activities done using a service pack (if applicable) or individual patches:

- Patches or serviceability updates that are to be activated, deactivated, or obsoleted could be left in a loaded state. These patches or serviceability updates would have to be installed or unloaded as required.
- Some patches can be transferred and show up as Unloaded, but not loaded. Cleanup or activation would be required as appropriate.
- Patches to be deactivated may be in Unloaded state and have to be removed.
- When a service pack is applied, some installed patches may have been automatically removed because they were rendered obsolete. If the service pack installation fails it is necessary to reapply the patches that were removed.

Many of these activities may be accomplished using Local Patching Manager. For more information, see Local Patching Manager on page 97.

Recommended order of patching operations

Due to interactions that can occur during patching, such as potential restarting, there are restrictions on elements and applications that you can patch concurrently. Multiple patching operations often must be performed on the same targets to apply all patching content.

Important:

VxWorks elements must be running Avaya Communication Server 1000 Release 7.0 or later software. Patching Manager does not support the patching of VxWorks elements running earlier versions of Avaya Communication Server 1000 software.

You can select multiple Avaya CS 1000 High Scalability systems, CS 1000 systems, or individual elements in Patching Manager by performing the steps described below. You can select the same target selections for each successive patching operation, with the patching option selections varying to indicate the item to patch during each pass. This automatically restricts the actual elements and patching content in the workflow.

Note:

The Special Instructions must be followed for the first time installation of LinuxBase, BaseWeb or PatchWeb Application SU's (when applicable); and whenever a newer version of these SU's are available. This requires using command line interface (CLI) to apply the Linux base serviceability update (SU) to all Linux elements. You must also apply the Base Web SU to the UCM Primary Security Server using the CLI (and Patchweb). The reason behind these instructions are due to the fixes that may be required to the Linux operating system (OS), Patch Deployment Manager or the underlying base patching framework to

allow the Service pack installation to function correctly. If these instructions are not followed, this may result in a Patch activation failed error message.

The following steps are recommended for sequence patching operations using multiple passes. You must complete each step (including restarts) in the order shown before you proceed with the next step. Not all steps may be applicable, depending on the patching operations being performed. For example, if there is no loadware to be patched, then that step may be skipped.

1. Patch the UCM Primary Security server first and separately from the other elements. Patch the UCM Primary Security Server in the following sequence:
    - Apply service packs or individual Linux patches.
    - If the UCM Primary Security Server is a Co-resident Call Server and Signaling Server, apply a deplist or Call Server patches.
    - If the UCM Primary Security Server is a Co-resident Call Server and Signaling Server, apply loadware.
2. Select all other required targets, excluding the Primary UCM Security Server. This includes the UCM Backup and Member servers. Patch them in the following sequence:
    - Apply a service pack and deplists or individual patches to Linux and VxWorks elements. This does not patch any Co-resident Call Server and Signaling Servers.
    - If you need to patch any Co-resident Call Server and Signaling Servers, apply a deplist or patches to those Call Servers.
    - Apply loadware.

Limitations

The following limitations exist for the Central Patching Manager and Local Patching Manager:

- You cannot use Central and Local Patching Manager at the same time. You should not use CLI patching commands while using either the Central or Local Patching Manager.
- You can only patch the Primary UCM only. If patching activities on other target elements are in progress, you cannot select or patch the primary UCM server.
- You must clear all patching activities on all targets before you can patch the Primary UCM server. That is, you must select an element and then click the Clear button.
- In Central Patching Manager, if you select the Primary UCM server on the Target Systems tab, then you can select no other element at the same time.
- If another user is currently patching an element, you cannot select that element (check box is dimmed) until activities for the element are cleared.

- If another user is registering or deploying new elements in Deployment Manager, these elements do not automatically show up in Central Patching Manager. Use the Refresh icon to display the list of active elements in the Central Patching Manager.
- Patching Manager only supports the patching of VxWorks elements that are running Avaya Communication Server 1000 Release 7.0 or later software.

Chapter 6: Central Patching Manager

The Central Patching Manager interface runs on the Primary UCM Security server and is accessible by logging on to UCM. A central patch library is available to which patches, deplists, loadware, and service packs can be uploaded to the library and centrally deployed to elements in the security domain. The central patch library consists of patches, serviceability updates, loadware, deplists, and service packs on the Primary UCM Security server. You can add and remove these items from the central patch library.

Important:

In this document, unless explicitly mentioned otherwise, the term patch or patches includes both patches and serviceability updates (SUs) because patches and serviceability updates are applied in the same way.

This chapter provides procedures to perform the following in the Central Patching Manager:

- Add, activate, deactivate, and delete Linux and binary patches.
- Add, activate, deactivate, and delete loadware and serviceability updates.
- Add, activate, deactivate, and delete deplists. (Deplists cannot be deactivated; however, individual patches that are part of a deplist can be deactivated.)
- Add, activate, and delete service packs. (Service packs cannot be deactivated; however, individual patches that are part of a service pack can be deactivated.)

You must have patching permissions to access the Central Patching Manager. For more information, see Patching permissions and roles on page 30.

Important:

VxWorks elements must be running Avaya Communication Server 1000 Release 7.0 or later software. Patching Manager does not support the patching of VxWorks elements running earlier versions of Avaya Communication Server 1000 software.

Note:

The Special Instructions must be followed for the first time installation of LinuxBase, BaseWeb or PatchWeb Application SU's (when applicable); and whenever a newer version of these SU’s are available. This requires using command line interface (CLI) to apply the Linux base serviceability update (SU) to all Linux elements. You must also apply the Base Web SU to the UCM Primary Security Server using the CLI (and Patchweb). The reason behind these instructions are due to the fixes that may be required to the Linux operating system (OS), Patch Deployment Manager or the underlying base patching framework to allow the Service pack installation to function correctly. If these instructions are not followed, this may result in a Patch activation failed error message.

Download and save patches, serviceability updates, and service packs

The Enterprise Solutions PEP Library (ESPL) provides online access to Avaya-approved Product Enhancement Package (PEP) solutions for Enterprise products.

- Patches are stored in the Communication 1000 /Meridian 1 Patch Tools section of the ESPL.
- Serviceability updates are stored in the Serviceability Updates and Loadware/Firmware Distribution Tools (Avaya CS 1000) section of the patch library.
- Service packs are stored in the PEP Dependency Tools section of the ESPL.
- Loadware is stored in the Serviceability Updates and Loadware/Firmware Distribution Tools (CS 1000) section of the patch library.
- Deplists are stored in the PEP Dependency Tools section of the ESPL.

Access the Central Patching Manager

Users must have patch administrator permissions (the patchAdmin permissions) to access Central Patching Manager. For more information, see Patching permissions and roles on page 30.

Use the following procedure to access the Central Patching Manager.

Accessing the Central Patching Manager from the Primary UCM Server

1. Start your browser.
2. In the **Address** field of the browser, enter the Fully Qualified Domain Name (FQDN) of the server (or if the FQDN is not known then enter then IP address).
   - If the FQDN is entered, go to 4 on page 40.
   - If the IP address is entered, go to 3 on page 40.
3. Click the **Go to central login for Single Sign-On** link (on the left side of the Unified Communications Management (UCM) page).
4. Log on to UCM using an account with patching privileges.

   The UCM interface appears.
5. In the UCM navigation tree, select **Network > CS 1000 Services > Patches**.

Figure 6: UCM navigation tree (Patches selected)

The Central Patching Manager appears. See Figure 7: Central Patching Manager on page 42.

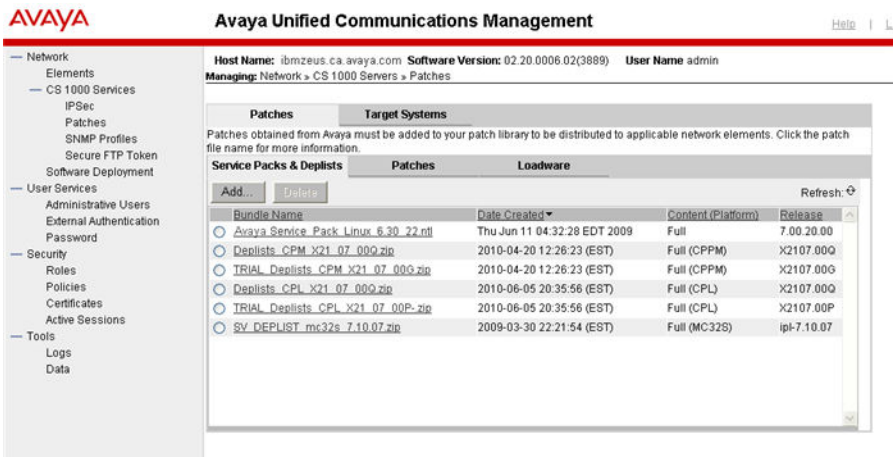

Figure 7: Central Patching Manager

The Central Patching Manager has two main tabs at the top of the page: Patches and Target Systems.

Important:

If any patching activities are active (not cleared), a third tab called In Progress appears when you log on to UCM. This tab shows the active patching activities on the elements for all patch administrators. The In Progress tab appears only when patch distribution is in progress and is active by default.

The Patches tab has three tabs: Service Packs & Deplists, Patches, and Loadware.

- On the Service Packs & Deplists tab, you can add service packs and deplists to the central patch library or delete them from the central patch library. You can also view details for added service packs and deplists. You can perform the following procedures from the Service Packs & Deplists tab:
  - Adding a service pack or deplist to the central patch library on page 43
  - Viewing service pack details on page 45
  - Viewing deplist details on page 47
  - Deleting a service pack or deplist from the central patch library on page 48
- On the Patches tab, you can add patches or serviceability updates to the central patch library or you can delete them. You can also view patch details for added patches. You can perform the following procedures from the Patches tab:
  - Adding a patch to the central patch library on page 49
  - Viewing patch details on page 50
  - Deleting a patch from the central patch library on page 51
- On the Loadware tab, you can add loadware updates for MGC and PSDL to the central patch library or you can delete them. You can also view the

loadware details. You can perform the following procedures from the Loadware tab:

- Adding loadware to the central patch library on page 52
- Viewing loadware details on page 53
- Deleting loadware from the central patch library on page 54

The Target Systems tab shows a list of elements that you can patch. The top level Network nodes are shown in a tree view that you can expand to show the elements assigned to each node. Select the node check boxes to indicate which elements to patch.

When you select or expand a branch, all other open branches at the same level collapse. However, selections within collapsed branches are retained.

The next page provides a list of patchable targets with Call Server and Node association, applications, release details, and type for each target element.

You can click an Element Name to open Base Manager and display information about currently deployed patches. You can perform the following procedures from the Target Systems tab:

- Activating patches on page 61
- Activating a service pack on page 55
- Activating a Call Server patch or deplist on page 67
- Deactivating a patch on page 84

Add a service pack or deplist to the central patch library

Use the following procedure to add a service pack or deplist to the central patch library. The file name of a service pack is similar to Avaya_Service_Pack_Linux_6.00_12.ntl. You must have downloaded and saved the file to a location accessible from your local PC before you can add it to the central patch library.

Note:

Uploading a large service pack or deplist can take a significant amount of time (15 to 30 minutes or longer) depending on the size of the service pack.

Adding a service pack or deplist to the central patch library

1. In the Patching Manager, ensure the **Patches** tab is selected.
2. Select the **Service Packs & Deplists** tab.

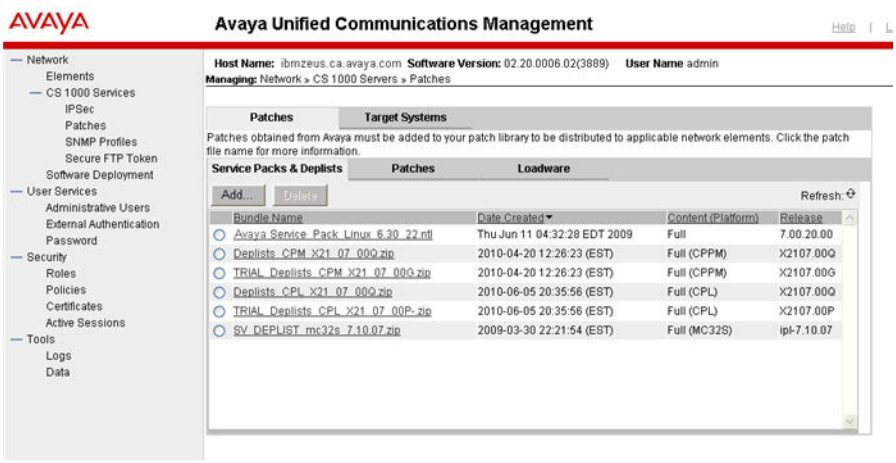

Figure 8: Patches tab - Service Packs and Deplists tab

3. Click **Add**.

   The New Service Pack or Deplist page appears.

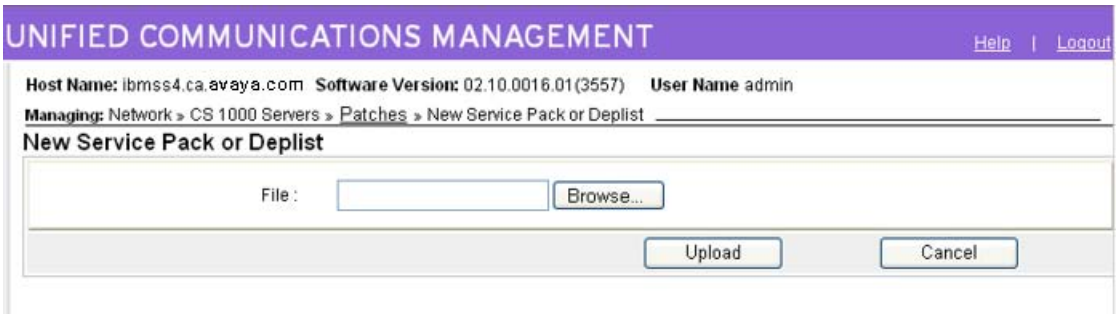

Figure 9: New Service Pack or Deplist

4. Click **Browse**.

   The Choose File dialog box appears.

5. In the Choose File dialog box, browse to the find the service pack or deplist on your client PC.

6. Select the service pack or deplist file, and click **Open**.

   The file appears in the File field.

7. Click **Upload**.

   The upload progress is indicated by a status bar at the bottom of the window. The Central Patching Manager validates the file and then the file appears on the Service Pack & Deplist tab. The Service Pack & Deplist tab displays the new file and its details. For more information, see View service pack details on page 45 or View deplist details on page 46.

View service pack details

Use the following procedure to view the details about a service pack and the individual patches and serviceability updates that it contains. The Service Pack Details page displays important details about a service pack and patches such as header information.

Viewing service pack details

1. In the Central Patching Manager, select the **Patches** tab.
2. Select the **Service Packs & Deplists** tab.
3. To view details of the service pack, under the **Name** column, click the name of the service pack file.

   The Service Pack Details (sp_name) page appears; sp_name is the name of the service pack.

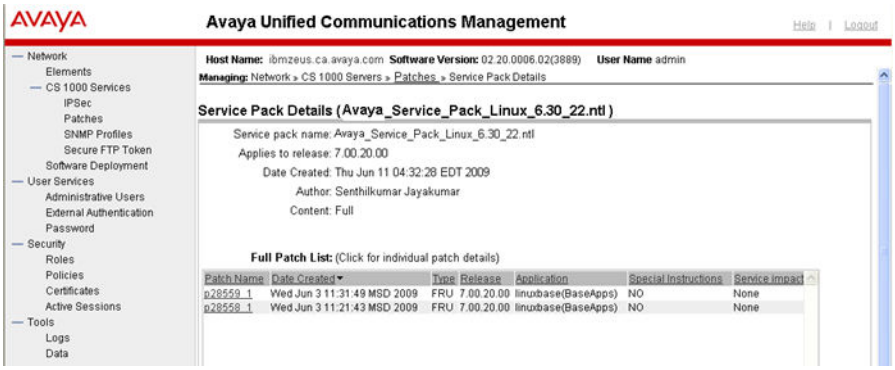

Figure 10: Service Pack Details page

4. On the **Service Pack Details (sp_name)** page, review the detailed information about the service pack.

   The page provides the following information about the service pack:

   - Patch Name—The name of the patches or serviceability updates within the service pack.
   - Date Created—The date the patch or serviceability update was created.
   - Type—The patch or SU type.
   - Release—The software release that the patch or serviceability update is applies to.
   - Application—The applications affected by the patch
   - Special Instructions—Whether there are special instructions. YES appears if the patch has special instructions and NO appears if the patch has no instructions.

- Service impact— Whether or not there is an impact to service. NONE indicates no impact to service.

5. To review an individual patch in the service pack, under **Patch Name**, click the name of the patch.

   The Patch Details (patch_name) page appears; patch_name is a name of a patch in the service pack. The Patch Details page provides information such as patch name, type and sub-type, general patch information, service impacts, dependent patches, obsolete patches, special instructions, and other details from the patch header.

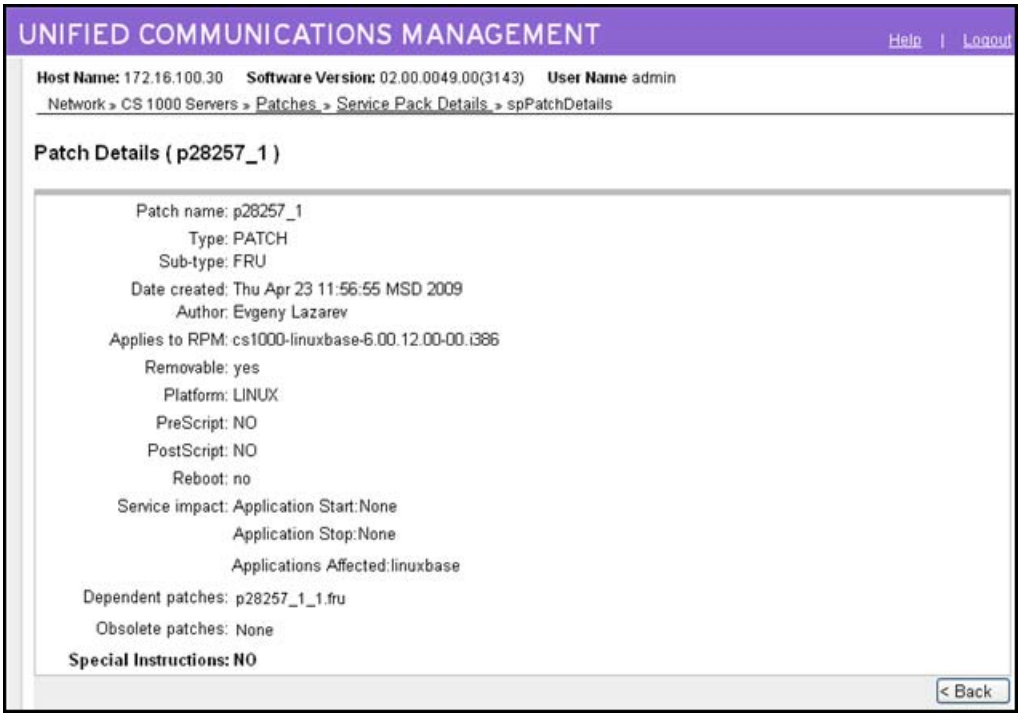

Figure 11: Patch Details

6. To return to the Service Pack Details page, click **Back** on the Patch Details page.
7. To return to the Service Packs & Deplists tab, click **Back** on the Service Pack Details page.

View deplist details

Use the following procedure to view the details about a specific deplist that is in the central patch library. The Deplist Details page displays important details about the loadware, such as header information.

Viewing deplist details

1. In the Central Patching Manager, select the **Patches** tab.
2. Select the **Service Packs & Deplists** tab.
3. To view details of the deplist, under the **Bundle Name** column, click the name of the deplist file.

   The Deplist Details (deplist_name) page appears; deplist_name is the name of the deplist.

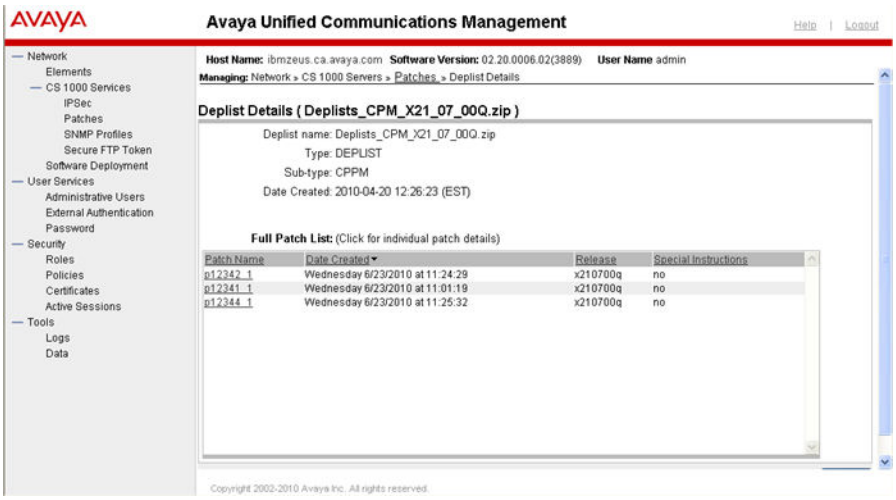

Figure 12: Deplist details (deplist name)

4. On the **Deplist Details (deplist_name)** page, review the detailed information about the deplist.

   The page provides the following information about the deplist:

   - Patch Name—The name of the deplist.
   - Type—Deplist.
   - Sub-type —The sub-type the deplist belongs to.
   - Date Created—The date the deplist was created.
   - Release—The software release the patch applies to.
   - Special instructions—Whether there are special instructions. YES appears if the patch has special instructions and NO appears if the patch has no instructions.

5. To review an individual patch in the deplist, under **Patch Name**, click the name of the file.

   The Patch Details (patch_name) page appears; patch_name is a name of a patch in the deplist. The Patch Details page provides information such as patch name, type and sub-type, general patch information, service impacts, dependent patches, obsolete patches, special instructions, and other details from the patch header.

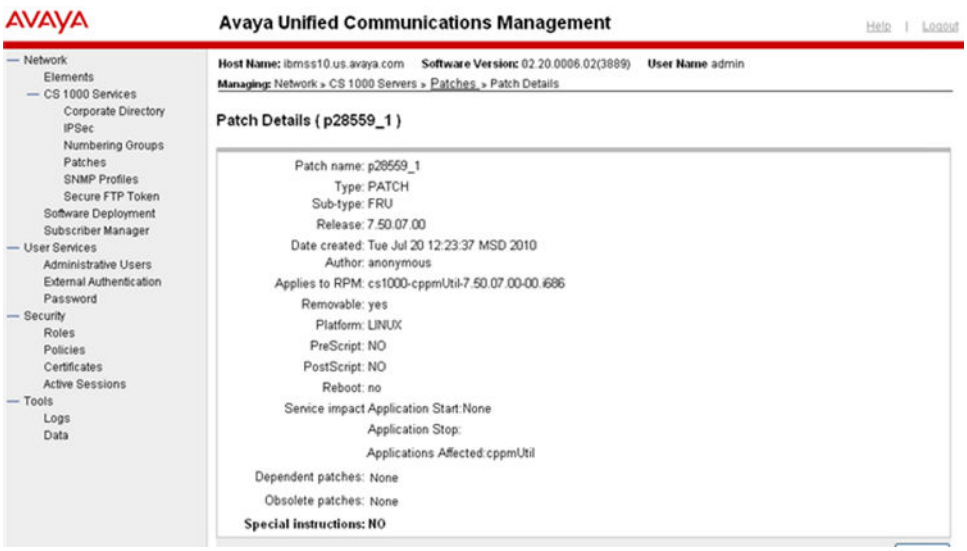

Figure 13: Patch Details

6. To return to the Deplist Details page, click **Back** .
7. To return to the Service Packs & Deplists tab, click **Back** on the Service Pack Details page.

Delete a service pack or deplist from the central patch library

Use this procedure to delete a service pack or deplist from the central patch library. Deleting a service pack or deplist from the central patch library does not delete it from any target.

Important:

You cannot recover a deleted service pack.

Deleting a service pack or deplist from the central patch library

1. In the Patching Manager, ensure the **Patches** tab is selected.
2. Select the **Service Packs & Deplists** tab.
3. Select the service packs to delete.
4. Click **Delete**.

   A dialog box appears prompting you to confirm the deletion.
5. Click **OK** to confirm the deletion.

   The service pack or deplist is removed from the list on the Service Packs & Deplists tab.

Add a patch to the central patch library

Use the following procedure to add a patch to the central patch library. You must have downloaded and saved the patch that you need to your local PC before you can add it to the central patch library.

Adding a patch to the central patch library

1. In the Central Patching Manager, select the **Patches** tab.
2. Select the **Patches** tab.
3. Click **Add**.

   The New Patch page appears.
4. Click **Browse**.

   The Choose File dialog box appears.
5. In the Choose File dialog box, browse to the find the downloaded patch on your client PC. Linux patch files have an .ntl file extension. Binary patches have a .cpl, .cpm, or .pp4 extension.
6. Select the patch file, and click **Open**.

   The file appears in the File field.
7. Click **Upload**.

   The upload progress is indicated by a status bar at the bottom of the window. The Central Patching Manager validates the file and then the patch file appears on the Patches tab.

   The Patches tab displays the new patch and its details:

   - Patch Name—The name of the patch or serviceability update.
   - Date Created—The date and time the patch was created. Patches are sorted based on the Date Release column.
   - Type—The type of patch. A patch appears as type FRU or WAR. A serviceability update appears as type RPM.
   - Release—The software release number.
   - Application—The application for which the patch applies.
   - Special Instructions—Whether there are special instructions. YES appears if the patch has special instructions and NO appears if the patch has no instructions.
   - Service Impact—Information about service impacts, such as system or device restarts.

For more information about viewing the patch details, see View patch details on page 50.

View patch details

Use the following procedure to view the details about a specific patch that is in the central patch library. The Patch Details page displays important details about the patch such as header information.

Viewing patch details

1. In the Patching Manager, select the **Patches**.
2. Select the **Patches** tab.
3. To view details for a patch, under the **Patch Name** column, click the patch name.

   The Patch Details (patch_name) page appears; patch_name is the name of the patch.

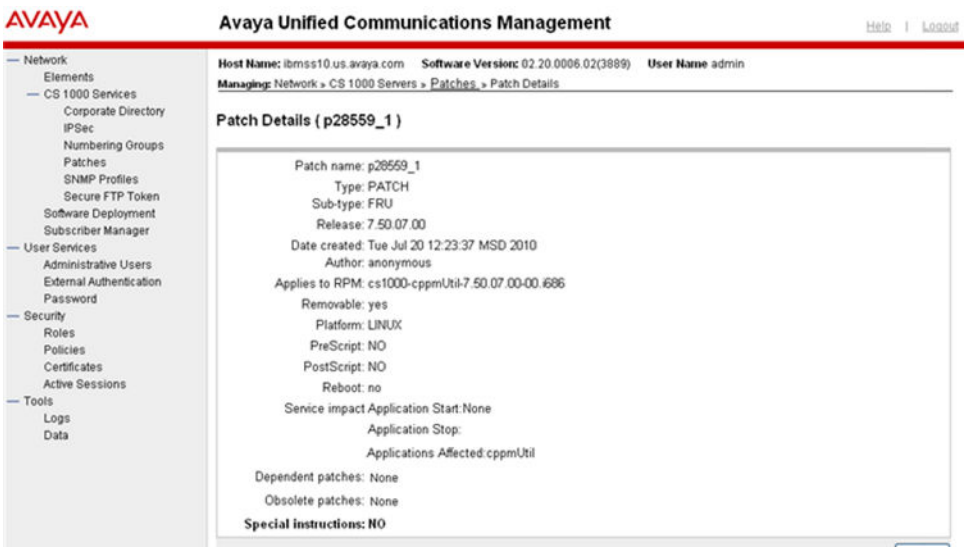

Figure 14: Patch Details (patch_name)

4. On the **Patch Details (patch_name)** page, review the detailed information about the patch.

   The Patch Details page provides the following information:

   - Patch name—The name of the patch.
   - Type—Patch or SU (Serviceability Update)
   - Sub-type— If the type is patch, then the subtype is FRU or WAR. If the type is SU, then the subtype is RPM.

- Release— (Binary patches only) Specifies the release number.
- Date created—The date and time the patch was created.
- Author—(Linux patches only) The patch author.
- Applies to RPM—(Linux patches only) Provides the RPM name and version to which the patch applies. For a serviceability update, the field provides the new version of the RPM that is contained in the serviceability update.
- Removable—(Linux patches only) Whether the patch is removable.
- Platform—The platform appears.
- PreScript—(Linux patches only) Whether there is a prepatch script file.
- PostScript—(Linux patches only) Whether there is a postpatch script file.
- Reboot—(Linux patches only) Whether a system restart is required.
- Service impact—Provides a list of service impacts. For example, if an application must stop or start. The impacts are color-coded according to severity. Red indicates a high service impact (such as a system restart), orange indicates a medium impact (such as an application restart), and no color indicates that there is no service impact.
- Dependent patches—Because patches are loaded one at a time in a serial fashion, patches can have only one dependant patch. If the dependant patch (for the patch being loaded) is not already loaded then the patch will not load. A dependent patch can only be on the same RPM.
- Obsolete patches—The most recently uploaded patch makes any listed patch obsolete.
- Special instructions—Lists any special instructions or considerations for the patch; otherwise, NO is displayed.

5. To return to the Patches tab, click **Back** on the Patch Details page.

Delete a patch from the central patch library

Use this procedure to delete a patch from the central patch library. Deleting a patch or serviceability update from the central patch library does not deactivate or delete it from any target.

Important:

Patches and serviceability updates cannot be recovered after they are deleted.

Deleting a patch from the central patch library

1. In the Patching Manager, select the **Patches** tab.
2. Select the **Patches** tab.
3. Select the check box for the patch or serviceability update to delete.

4. Click **Delete**.

   A dialog box appears prompting you to confirm the patch deletion.

5. Click **OK** to confirm the deletion of the patch.

   The patch is removed from the list.

Add loadware to the central patch library

Use this procedure to add loadware to the central patch library.

Adding loadware to the central patch library

1. In the Central Patching Manager, select the **Patches** tab.
2. Select the **Loadware** tab.
3. Click **Add**.

   The New Patch page appears.

4. Select the Patch category.
5. Click **Browse**.

   The Choose File dialog box appears.

6. In the Choose File dialog box, browse to the find the downloaded loadware on your client PC.
7. Select the loadware file, and click **Open**.

   The file appears in the File field.

8. Click **Upload**.

   The upload progress is indicated by a status bar at the bottom of the window. The Central Patching Manager validates the file and then the loadware file appears on the Loadware tab.

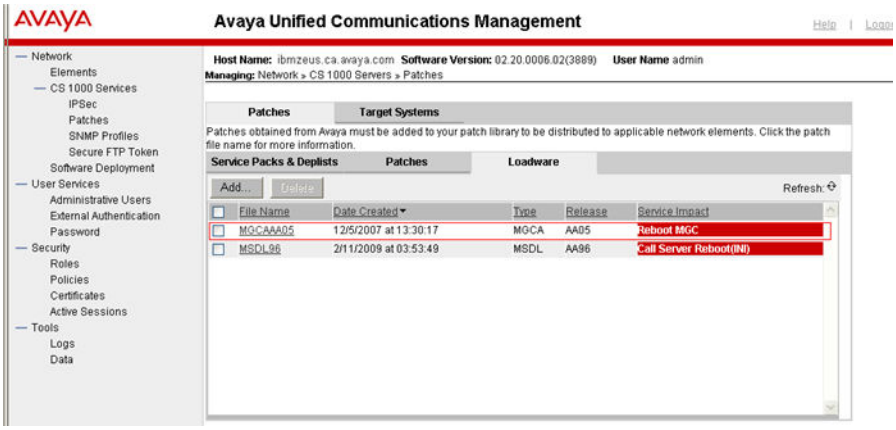

Figure 15: Loadware tab showing loadware details

The Loadware tab displays the new loadware and its details:

- File name—The name of the loadware.
- Date created—The date and time the loadware was created.
- Type— The first four letters of the loadware file name.
- Release — The loadware release.
- Service impact—Any impacts to service, such as a device or application restart.

View loadware details

Use the following procedure to view the details about specific loadware that is in the central patch library. The Loadware Details page displays important details about the loadware, such as header information.

Viewing loadware details

1. In the Patching Manager, select **Patches**.
2. Select the **Loadware** tab.
3. To view details for a loadware, under the **File Name** column, click the loadware name.

   The Loadware Details (loadware_name) page appears; loadware_name is the name of the loadware file.

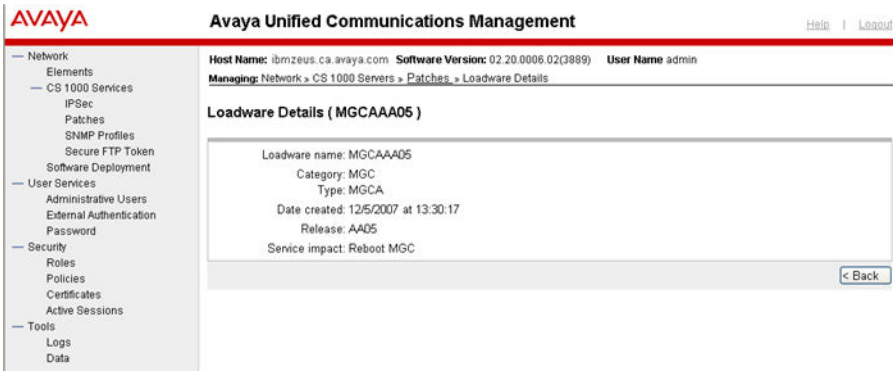

Figure 16: Loadware details (loadware name)

4. On the **Loadware Details (loadware_name)** page, review the detailed information about the loadware.

   The Loadware Details page provides the following information:

   - Loadware name—The name of the loadware.
   - Category—The loadware category.
   - Type— The first four letters of the loadware file name.
   - Date created—The date and time the loadware was created.
   - Release — The loadware release.
   - Service impact—Any impacts to service, such as a device or application restart.

5. To return to the Loadware tab, click **Back** on the Loadware Details page.

Delete loadware from the central patch library

Use this procedure to delete loadware from the central patch library.

Deleting loadware from the central patch library

1. In the Patching Manager, select the **Patches** tab.
2. Select the **Loadware** tab.
3. Select the check box for the loadware to delete.
4. Click **Delete**.

   A dialog box appears prompting you to confirm the loadware deletion.

5. Click **OK** to confirm the deletion of the loadware.

   The loadware is removed from the list.

Activation workflow

Before you begin patching activation operations, see Recommended order of patching operations on page 36.

- Activating a service pack on page 55
- Activating patches on page 61
- Activating a Call Server patch or deplist on page 67
- Activating a Media Card patch on page 71
- Activating a MGC loadware patch on page 75
- Activating a PSDL loadware patch on page 80

Activate a service pack

Use the following procedure to apply a service pack to one or multiple elements. The service pack must be in the Central Patching Library. This procedure is specific to service packs; however, you can patch more than one type of element during a patching session. Before you begin patching activation operations, see Recommended order of patching operations on page 36.

Activating a service pack

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 17: Target Systems tab showing Network tree view

When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to activate patches.
3. Click **Next**.
4. From the list of elements, select the check box for one or more elements for which to apply the service pack.

Important:

If you select the Primary UCM server on the Target Systems tab, no other element can be selected at the same time.

If an element is being patched by another user, you cannot select that element (check box is dimmed) until all patching activities for that element are cleared.

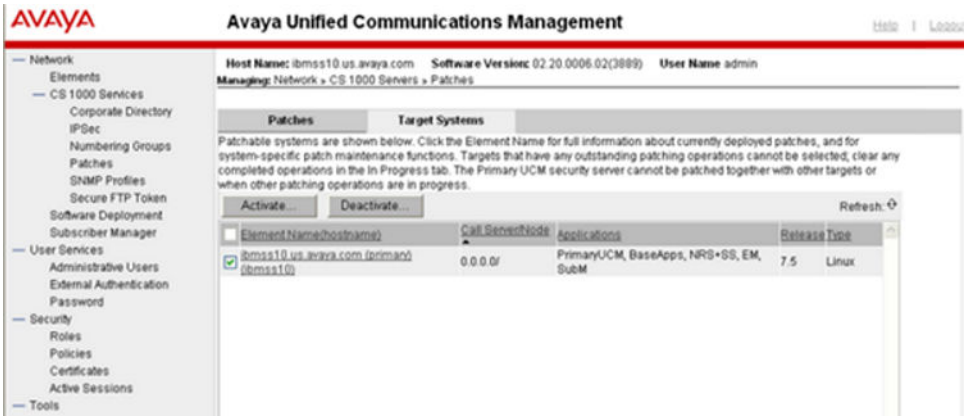

Figure 18: Select element to receive service pack

The Activate button is enabled.

5. Click **Activate**.

The Patching Options page appears.

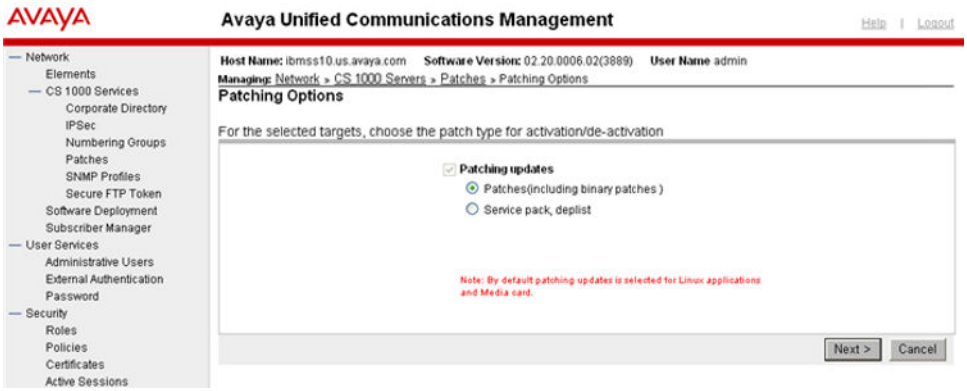

Figure 19: Patching Options page

6. Select the patching type and click **Next**.

   The Distribute Patches Step 1 page appears. Applicable service packs are displayed on the Service Pack & Deplists tab (based on the release of the selected elements and the applications installed on them).

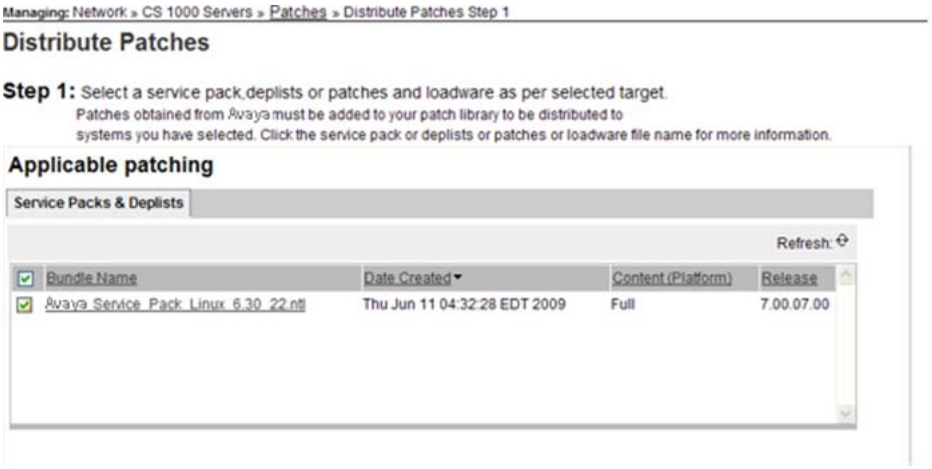

Figure 20: Distribute Patches Step 1 page

7. Select the applicable service pack to apply on the elements.

   Important:

   You can select only one of the following to activate at any one time:

   - A single service pack
   - Multiple patches and serviceability updates

   You cannot mix activation of service packs with patches and serviceability updates.

8. Click **Next**.

The Distribute Patches Step 2 page appears.

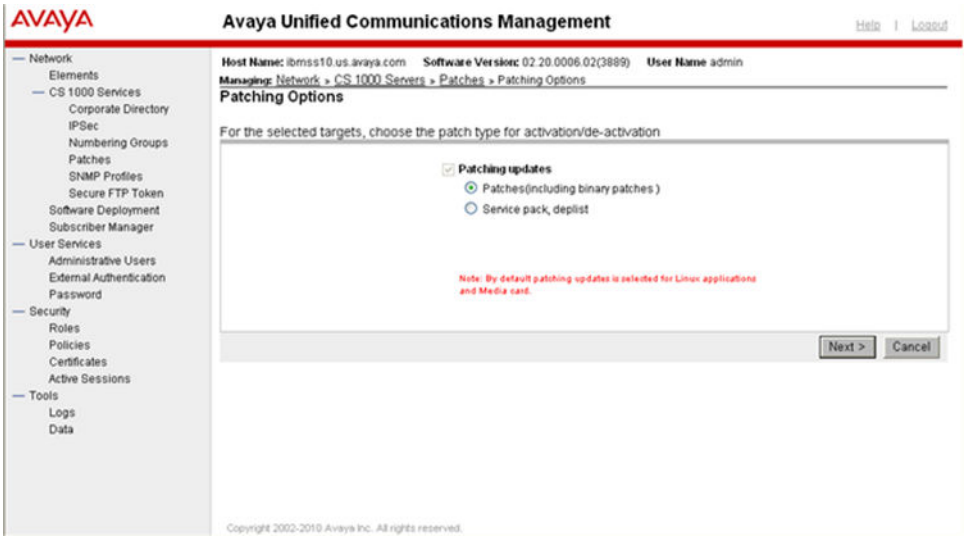

Figure 21: Distribute Patches Step 2

9. On the Distribute Patches Step 2 page, select the **Processing method**:

   - **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected service pack or patch is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.

     ⚠ Warning:

     If you are patching the Primary UCM server then this is the only option. Avaya strongly advises that you review the impact of patching the Primary UCM server and be aware of any application restart. If there is an indication of a JBoss restart during the patching operation, then the Web session will be dropped. You must then log on again.

     ⚠ Warning:

     When you review the impacts for a given target, if there is an indication of a reboot or JBoss-Quantum restart during the patching operation, be aware that all Avaya applications will also be restarted.

   - **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

     ⚠ Warning:

     Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

10. Click **Continue**.

    The In Progress tab appears and shows the number of patches which are ready to load (under the Status Summary column).

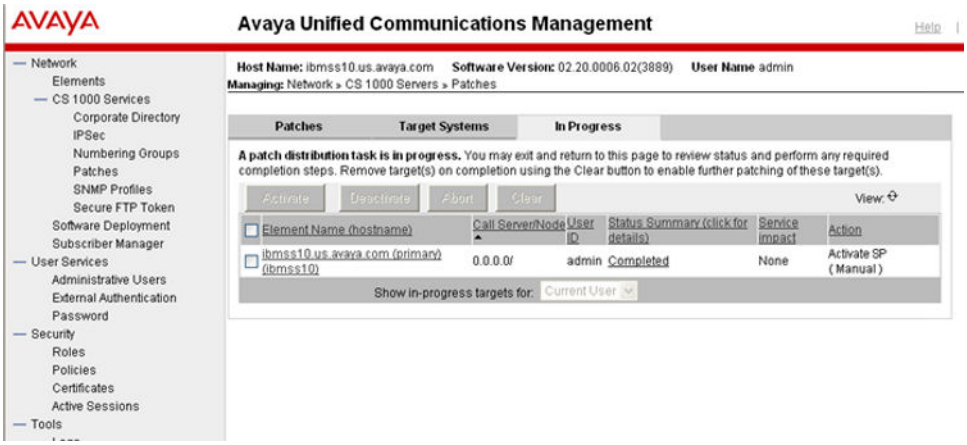

Figure 22: In Progress tab

Important:

Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

11. If you selected the **Review impact for each target and run individually** option in 9 on page 58, the targets are analyzed based on the current patch information obtained from the target and the service pack to be applied. Complete 12 on page 59 to 15 on page 60 and then proceed to 16 on page 60.

    OR

    If you selected the **Run all automatically** option in 9 on page 58, the targets are analyzed based on the current patch information obtained from the target and the service pack to be applied. Unless there are errors detected, the patch application proceeds automatically without waiting for your user input. Proceed to 16 on page 60.

12. Wait for the status to change in the **Status Summary** column. The Status Summary provides information about the patch activation progress. For more information about the statuses displayed, see Table 2: Status information on page 33.

    Use the Refresh icon to see the progress updates.

13. Under the **Status Summary** column, click the **Ready to Load** link for each target element to view the patching plan details for that target.

    The Patching Job Details page appears for the selected element and displays the list of patches and serviceability updates within the service pack.

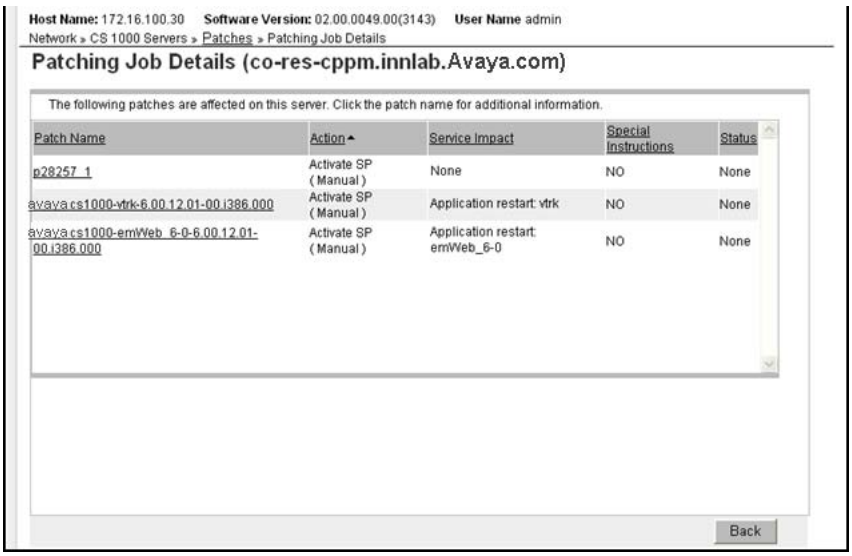

Figure 23: Patching Job Details page

To view details for a specific patch, click the link under the **Patch Name** column. The Patch Details page appears.

14. After you review the identified service impacts in the patching plan, click **Back** on the **Patch Details** page, and then click **Back** again on the **Patching Job Details** page to return to the **In Progress** tab.
15. Select the check box for the target element and then click **Activate** to apply patches within the service pack.
16. Wait while the updates are applied to the target element.

    Note:

    Depending on the size of the service pack, it can take some time to activate a service pack.

17. Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.
18. Wait until the updates are completed on the target. The **Status Summary** column indicates when the service pack activation is **Completed**.
19. To view the results, under the **Status Summary** column, click the **Completed** link.

    The Patching Job Details (target_name) page appears and the Status column indicates that the patch succeeded. For a service pack, the underlying operations and an overall result is provided.
20. On the Patching Job Details (target_name) page, click Back.
21. After you review your patching results and are satisfied with the results, select the check box for the target element, and then click **Clear** to end the patching process for the target element. You must click Clear before you can perform any other patch operations for this target element.

Further patching activation and deactivation operations cannot be performed on the element until it is cleared.

The In Progress tab disappears when all activities for all elements are cleared.

Activate patches

Use the following procedure to apply a patch to one or more target elements. This procedure is specific to patches; however, you can patch more than one type of element during a patching session. Before you begin patching activation operations, see Recommended order of patching operations on page 36.

Activating patches

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 24: Target Systems tab showing Network tree view

   When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to activate patches.
3. Click **Next**.
4. From the list of elements, select the check boxes for one or more elements for which to apply the patches.

   Important:

   If you select the Primary UCM server on the Target Systems tab, no other element can be selected at the same time.

If an element is currently being patched by another user, you cannot select that element (check box is dimmed) until all patching activities for that element have been cleared.

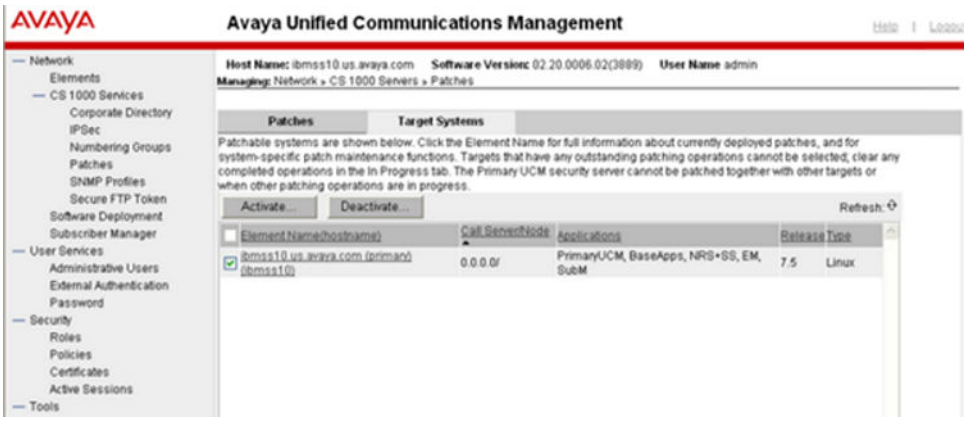

Figure 25: Select target element

5. Click **Activate**.

   The Distribute Patches Step 1 page appears. This page displays the applicable patches and serviceability updates (based on the release of the selected elements).

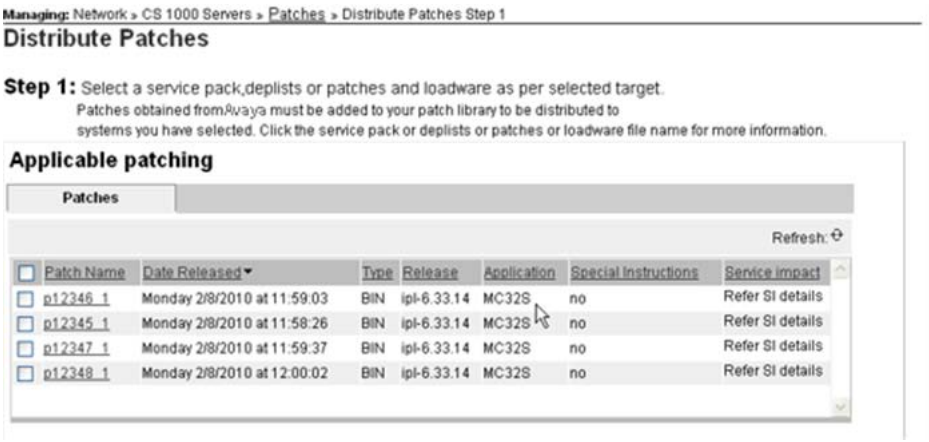

Figure 26: Distribute Patches Step 1 page

6. Select the check boxes for the patches to apply on the elements.

Important:

You can select only one of the following to activate at any one time.

- A single service pack.
- Multiple patches and serviceability updates

You cannot mix activation of service packs with patches and serviceability updates.

7. Click **Next**.

   The Distribute Patches Step 2 page appears.

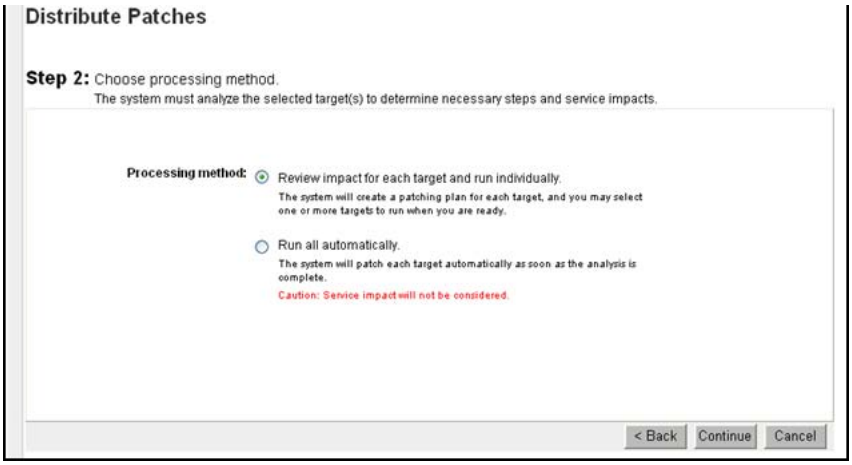

Figure 27: Distribute Patches Step 2

8. On the Distribute Patches Step 2 page, select the **Processing method**:

   - **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected patch or serviceability update is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.
   - **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

     ⚠ Warning:

     Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

9. Click **Continue**.

   The In Progress tab appears.

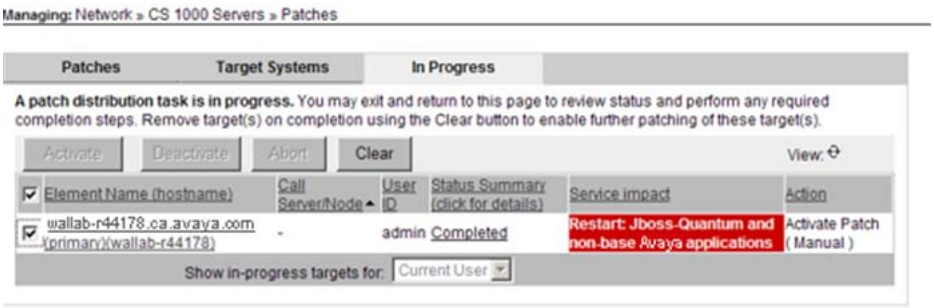

Figure 28: In Progress tab

Important:

Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

10. If you selected the **Review impact for each target and run individually** option, the targets are analyzed based on the current patch information obtained from the target and the new patches to be applied. Continue with the next steps.

    OR

    If you selected the **Run all automatically** option, the targets are analyzed based on the current patch information obtained from the target and the new patches to be applied. Unless there are errors detected, the patch application proceeds automatically without waiting for your user input. Proceed to step 14.

11. Wait for the status to change in the **Status Summary** column. The Status Summary provides information about the patch activation progress. For more information about the statuses displayed, see Table 2: Status information on page 33.

    Use the Refresh icon to see the progress updates.

12. Under the **Status Summary** column, click the **Ready to Load** link for each target element to view the patching plan details for that target.

    The Patching Job Details page appears.

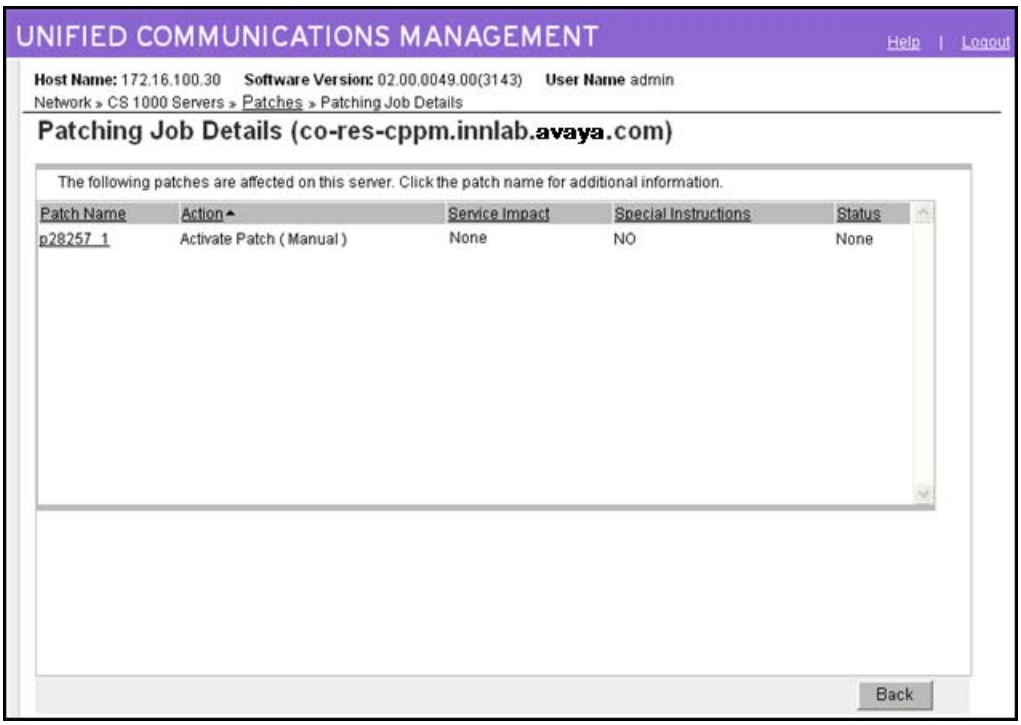

Figure 29: Patching Job Details

To view the patch details, click the link under the **Patch Name** column. The Patch Details page appears.

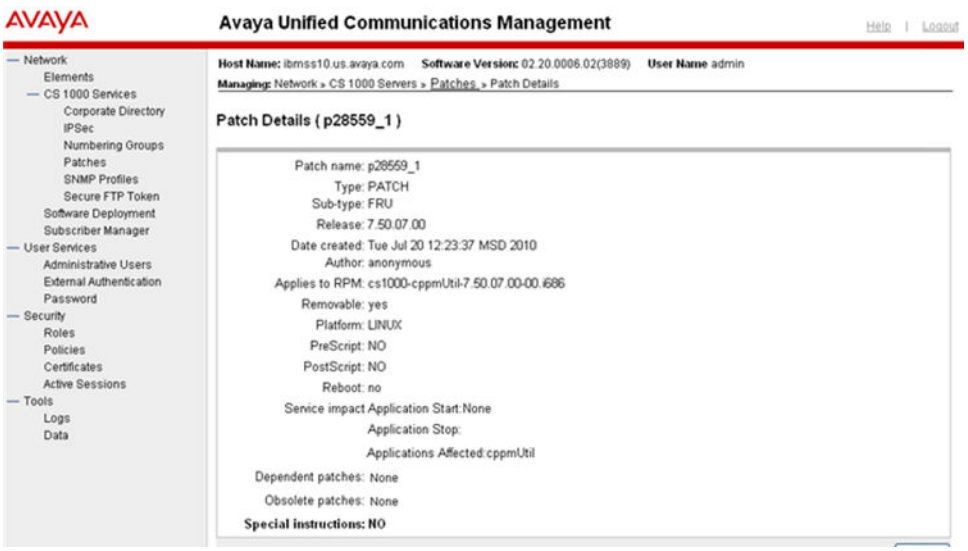

Figure 30: Patch Details

13. After you review the identified service impacts in the patching plan, click **Back** on the **Patch Details** page, and then click **Back** again on the **Patching Job Details** page to return to the **In Progress** tab.
14. Select the check box for the target element.

The Activate button is enabled.

15. Click **Activate** to start applying patches.
16. Wait while the updates are applied to the target. The **Status Summary** column provides information about the patch activation progress. For more information about the statuses displayed, see Table 2: Status information on page 33.
17. Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.
18. Wait for the process to complete.
19. To view the results, under the **Status Summary** column, click the **Completed** link.

    The Patching Job Details (target_name) page appears and the Status column indicates that the patch succeeded.

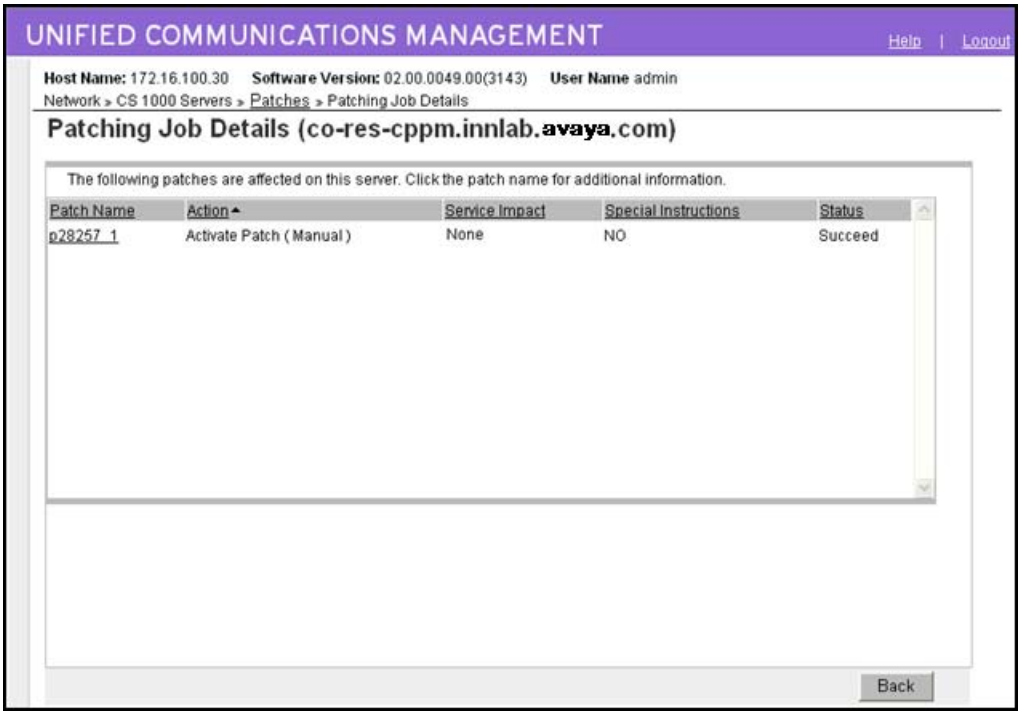

Figure 31: Patching Job Details

20. On the Patching Job Details (target_name) page, click Back.
21. After you review your patching results and are satisfied with the results, select the element and then click **Clear** to end the patching process for the select target. You must click Clear before you can perform any other patch operations for this target element.

    Further patching activation and deactivation operations cannot be performed on the element until it is cleared.

    The In Progress tab disappears when all activities for all elements are cleared.

Activate a Call Server binary patch or deplist

Use the following procedure to activate a deplist or binary patches for Call Server (VxWorks and Linux) targets. You can select either multiple individual patches or a deplist, but not both. This procedure is specific to Call Server binary patches and deplists; however, you can patch more than one type of element during a patching session. Before you begin patching activation operations, see Recommended order of patching operations on page 36.

For information about PEP settings for Call Server and Media Card, see Figure 35: Call Server and Media Card PEP settings page on page 69.

Activating a Call Server patch or deplist

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 32: Target Systems tab showing Network tree view

Note:

When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to activate patches.
3. Click **Next**.
4. From the list of elements, select the check boxes for one or more elements for which to apply the patches.

Important:

If you select the Primary UCM server on the Target Systems tab, no other element can be selected at the same time.

If an element is currently being patched by another user, you cannot select that element (check box is dimmed) until all patching activities for that element have been cleared.

5. Click **Activate**.

   The Patching Options page appears.

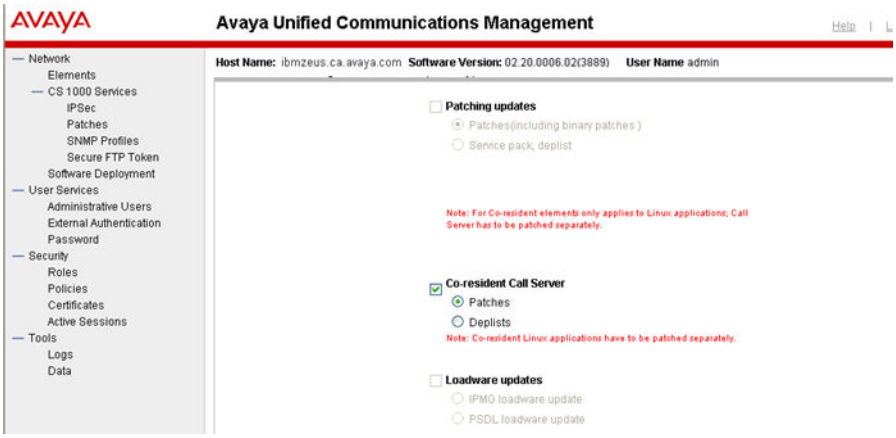

Figure 33: Patching Options page

6. Select the appropriate patch type. You can only select one check box.
7. For the patch type selected, select the appropriate radio button.
8. Click **Next**.

   The Distribute Patches Step 1 page appears.

Figure 34: Distribute Patches Step 1 page

9. Select a deplist or individual patch files.

   You can select either a deplist or individual patch files, but not both. For individual patches, applicability depends on the application and version installed.

You can also select the **Modify PEP settings** box if you wish to make changes to the default patch settings.

10. Click **Next**.

    If you selected the **Modify PEP settings** box, the Patch Settings Step 2 page appears with the Call Server and Media Card PEP settings.

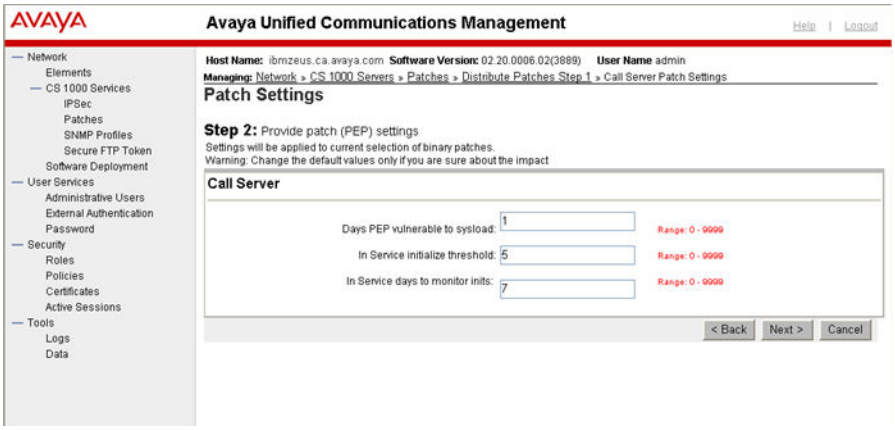

Figure 35: Call Server and Media Card PEP settings page

Note:

The Media Card section is only enabled if at least one selected element is a Media Card and you are applying patches. This option is not available for deplists.

11. Make any desired changes and click **Next**.

    The Distribute Patches page appears.

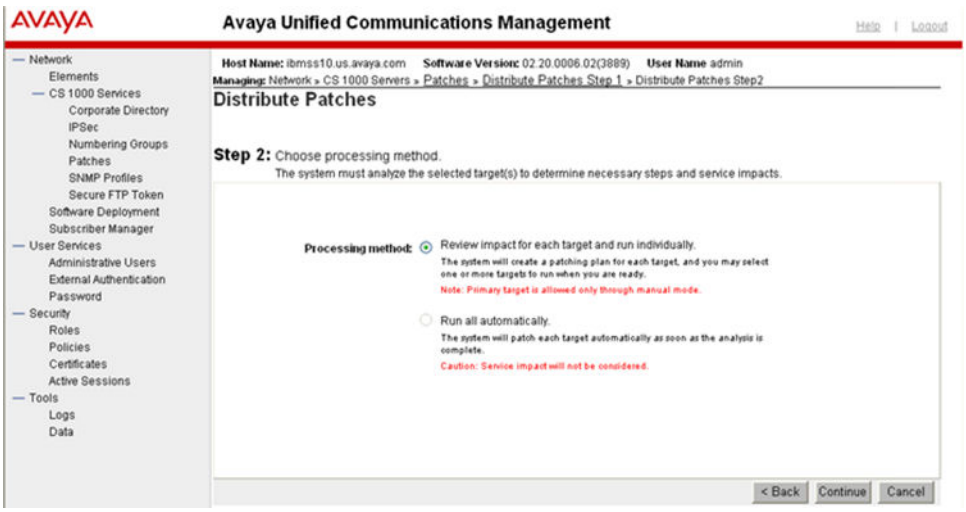

Figure 36: Distribute Patches page

12. On the Distribute Patches page, select the **Processing method**:

    - **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected patch or serviceability update is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.
    - **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

    ⚠ Warning:

    Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

13. Click **Continue**.

    The **In Progress** tab appears.

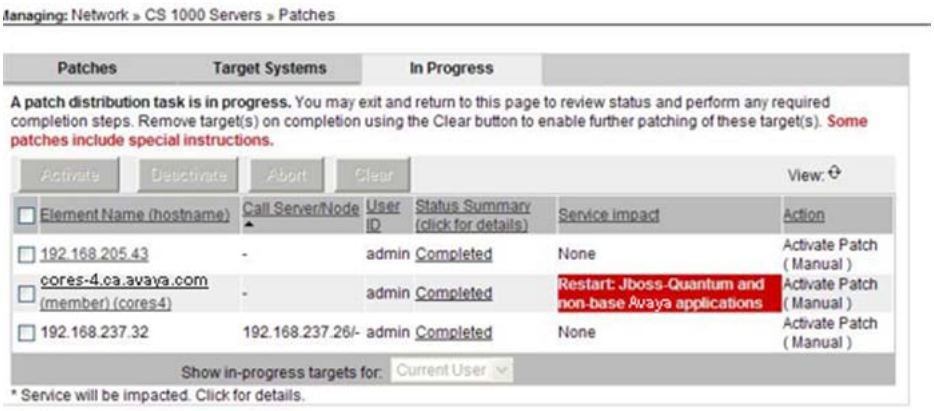

Figure 37: In Progress tab

Important:

Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

After a patch completes, aborts, or fails, the status appears in the Status Summary column. You can click the link under the Status Summary column to view the details.

14. When the patching for a target element completes (or fails or aborts), click **Clear** to clear the summary report.
15. Repeat the patching process for each target, as required.

Activate a Media Card patch

Use the following procedure to activate Media Card (MC32S, VGMC) patches. This procedure is specific to media cards; however, you can patch more than one type of element during a patching session. Before you begin patching activation operations, see Recommended order of patching operations on page 36.

Activating a Media Card patch

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 38: Target Systems tab showing Network tree view

Note:

When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the media cards for which to activate patches.
3. Click **Next**.
4. From the list of elements, select the check boxes for one or more elements for which to apply the patches.
5. Click **Activate**.

   The Patching Options page appears, as shown in the following figure.

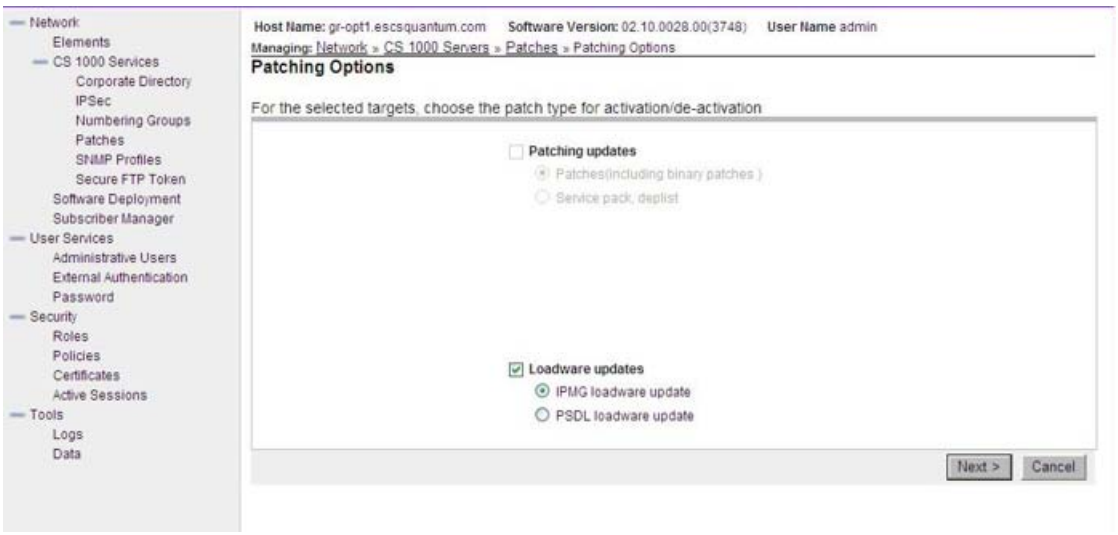

Figure 39: Patching Options page

6. In the Patching updates section, select the appropriate patching type.
7. Click **Next**.

   The Distribute Patches Step 1 page appears.

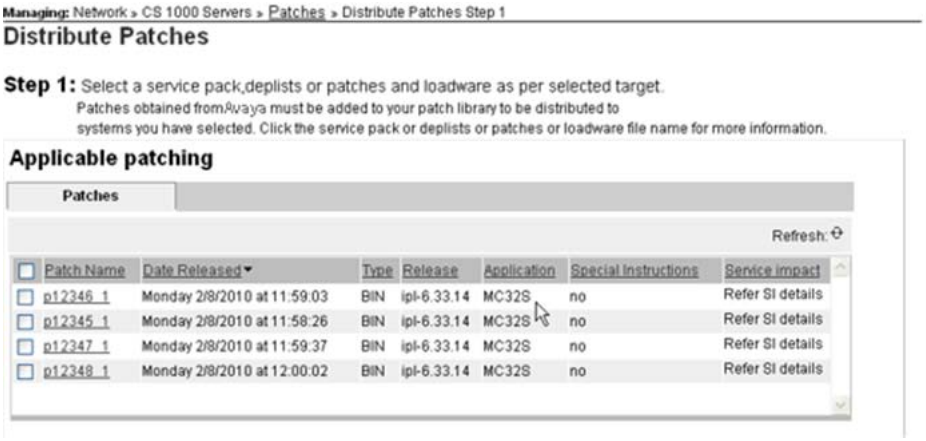

Figure 40: Distribute Patches Step 1 page

8. Select a deplist or individual patch files.

   You can select either a deplist or individual patch files, but not both. For individual patches, applicability depends on the application and version installed.

   You can also select the **Modify PEP settings** box if you wish to make changes to the default patch settings.

9. Click **Next**.

   If you selected the **Modify PEP settings** box, the Patch Settings Step 2 page appears, as shown in the following figure.

Figure 41: Patch Settings Step 2 page

10. Make any desired changes and click **Next**.

    The Activate Patches Step 3 page appears.

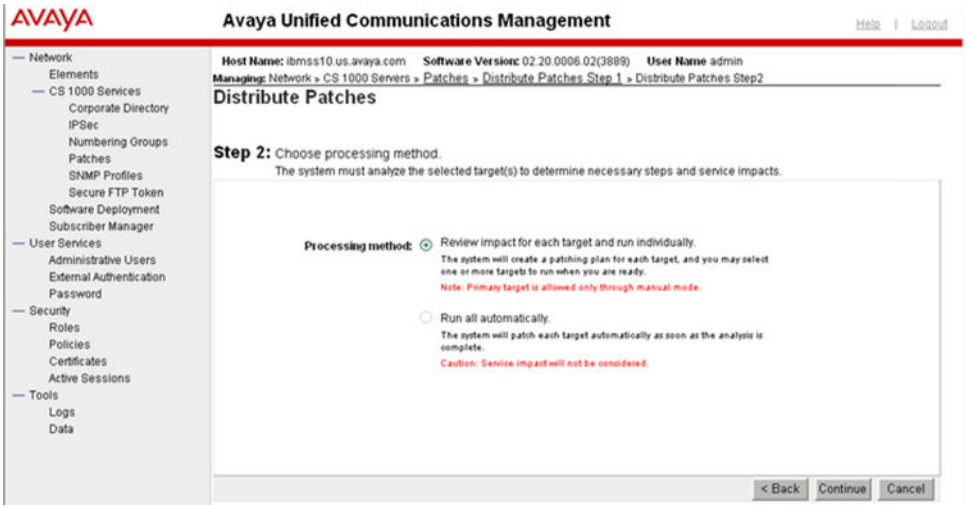

Figure 42: Activate Patches Step 3 page

11. On the Activate Patches Step 3 page, select the **Processing method**:

    - **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected patch or serviceability update is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.
    - **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

Warning:

Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

12. Click **Continue**.

    The In Progress tab appears.

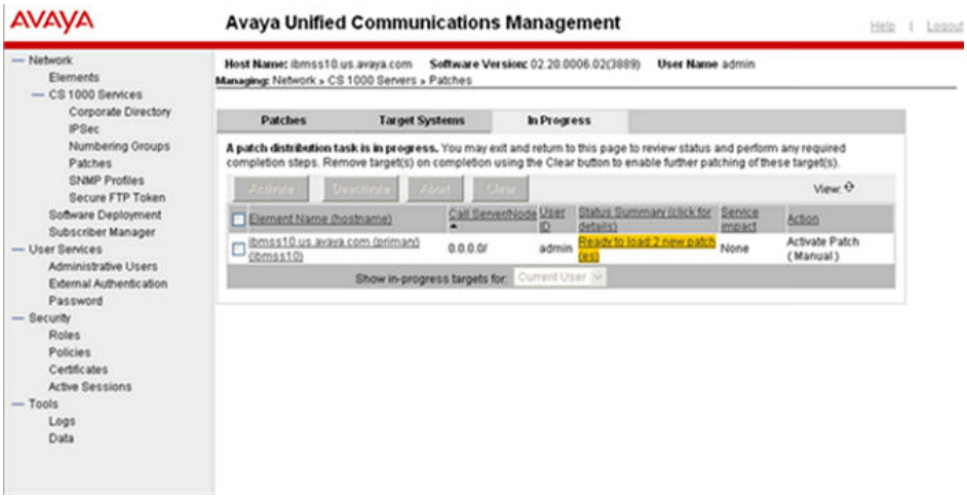

Figure 43: In Progress tab

Important:

Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

After a patch completes, aborts, or fails, the status appears in the Status Summary column. You can click the link under the Status Summary column to view the details.

13. When the patching for a target element completes (or fails or aborts), click **Clear** to clear the summary report.
14. Repeat the patching process for each target, as required.

Activate a MGC loadware patch

Use this procedure to activate a MGC loadware patch. This procedure is specific to MGC loadware; however, you can patch more than one type of element during a patching session. Before you begin patching activation operations, see Recommended order of patching operations on page 36.

For information about upgrading multiple Call Server elements, see Figure 46: Associated MGC Upgrade page on page 76.

Activating a MGC loadware patch

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 44: Target Systems tab showing Network tree view

Note:

When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to activate patches. You must select at least one Call Server element.
3. Click **Next**.
4. From the list of elements, select the check boxes for one or more elements for which to apply the patches.

   Important:

   If you select the Primary UCM server on the Target Systems tab, no other element can be selected at the same time.

   If an element is currently being patched by another user, you cannot select that element (check box is dimmed) until all patching activities for that element have been cleared.

5. Click **Next**.

   The list of element names is shown.

6. Select the elements to activate and click **Activate**.

   The Patching Options page appears.

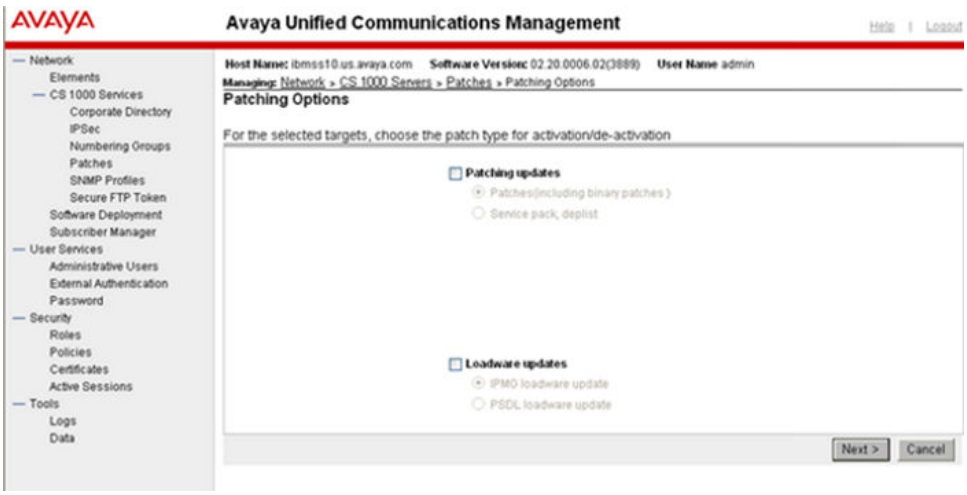

Figure 45: Patching Options page

Note:

The Co-resident Call Server section only displays if there are any Co-resident Call Server and Signaling Server systems.

7. In the Loadware updates section, select IPMG loadware update.
8. Click **Next**.

   The Associated MGC Upgrade page appears. This page shows all MGCs registered with the Call Server.

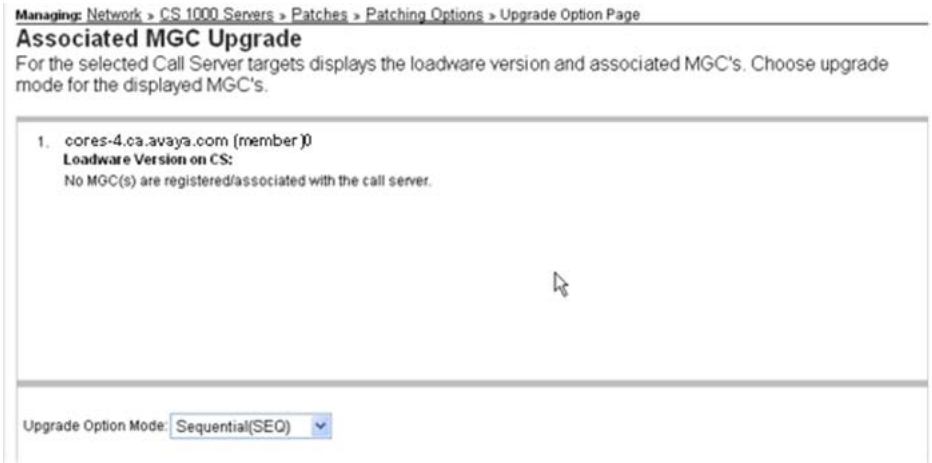

Figure 46: Associated MGC Upgrade page

9. Select the Upgrade Option Mode. The choices are:
   - Sequential (SEQ)—upgrade each selected element one at a time
   - Simultaneous (SIM)—upgrade all elements at once
10. Click **Continue**.

The Distribute Patches Step 1 page appears.

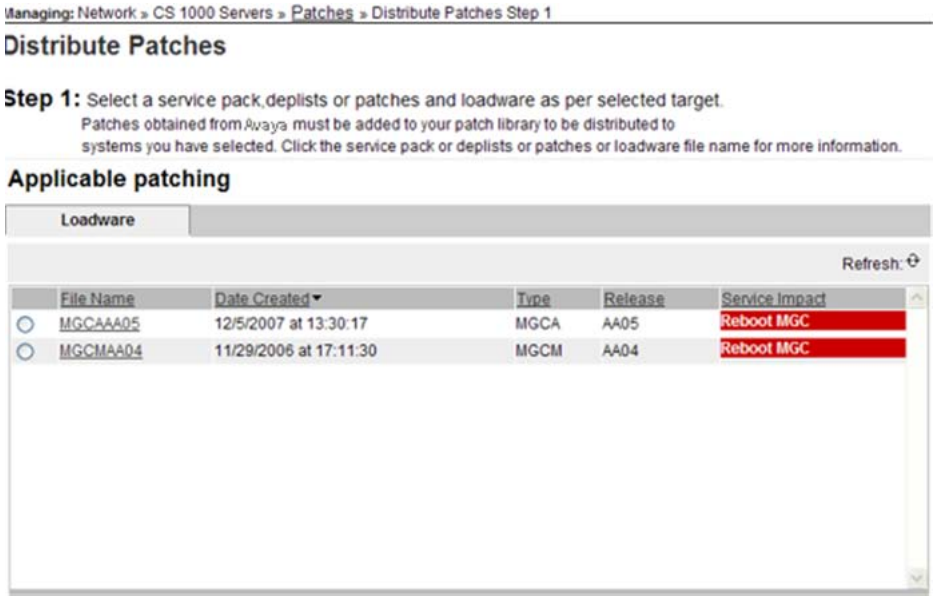

Figure 47: Distribute Patches Step 1 page

11. In the Applicable patching section, select the loadware to apply.

    For loadware, the applicable patches include all MGC Loadware versions available in the Central Patching Manager Library.

    Note:

    If selecting multiple loadware, you cannot select two loadware of the same type.

12. Click **Next**.

    The Activate Patches Step 3 page appears.

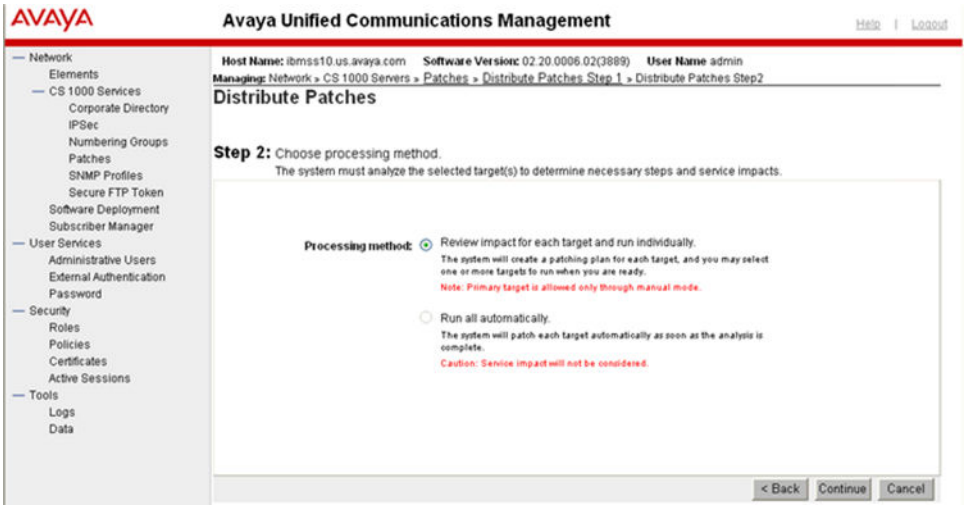

Figure 48: Activate Patches Step 3 page

13. On the Activate Patches Step 3 page, select the **Processing method**:

    - **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected patch or serviceability update is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.
    - **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

      ⚠ Warning:

      Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

14. Click **Continue**.

    The In Progress tab appears.

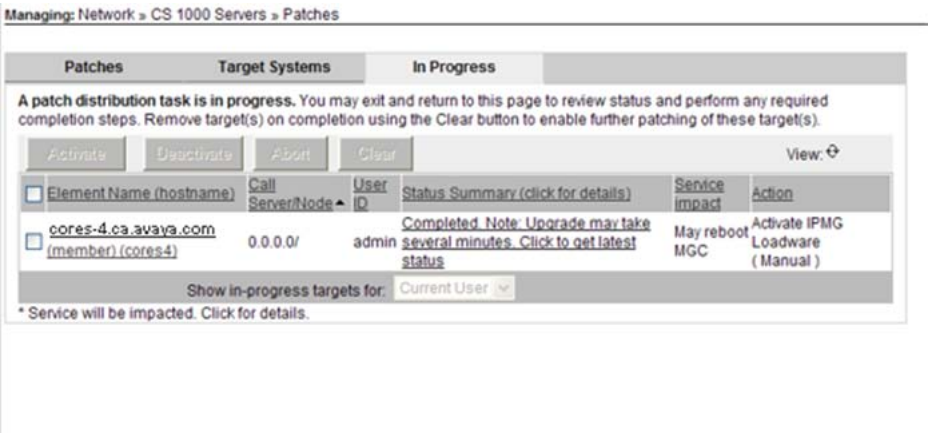

Figure 49: In Progress tab

Important:

Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

After a loadware completes, aborts, or fails, the status appears in the Status Summary column. You can click the link under the Status Summary column to view the details. When you click the status link, the Loadware Patching Status page appears, as shown in the following figure.

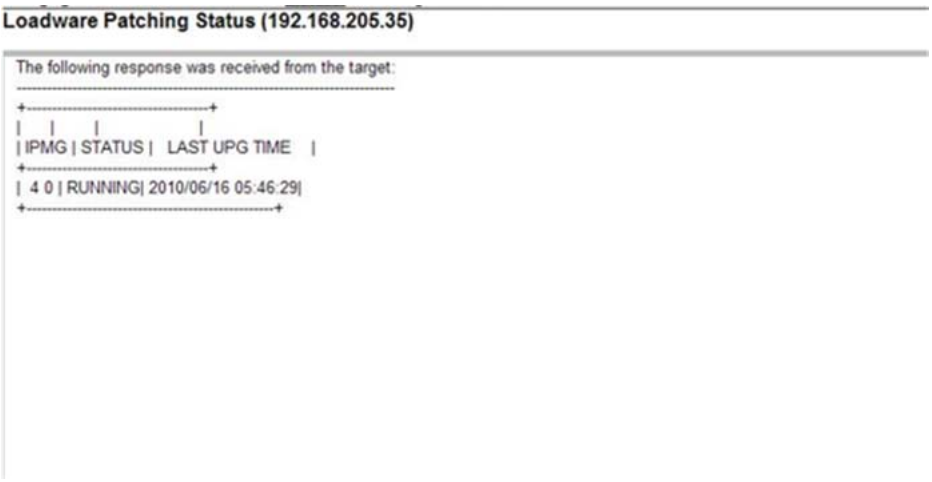

Figure 50: Loadware Patching Status page

Click **Back** to return to the previous page.

15. When the patching for a target element completes (or fails or aborts), click **Clear** to clear the summary report.
16. Repeat the patching process for each target, as required.

Activate a PSDL loadware patch

Use this procedure to activate a PSDL type loadware patch. This procedure is specific to PSDL loadware; however, you can patch more than one type of element during a patching session. Before you begin patching activation operations, see Recommended order of patching operations on page 36.

Activating a PSDL loadware patch

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 51: Target Systems tab showing Network tree view

   When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to activate patches. You must select at least one Call Server element.
3. Click **Next**.
4. From the list of elements, select the check boxes for one or more elements for which to apply the patches.

   Important:

   If you select the Primary UCM server on the Target Systems tab, no other element can be selected at the same time.

   If an element is currently being patched by another user, you cannot select that element (check box is dimmed) until all patching activities for that element have been cleared.

5. Click **Activate**.

   The Patching Options page appears, as shown in the following figure.

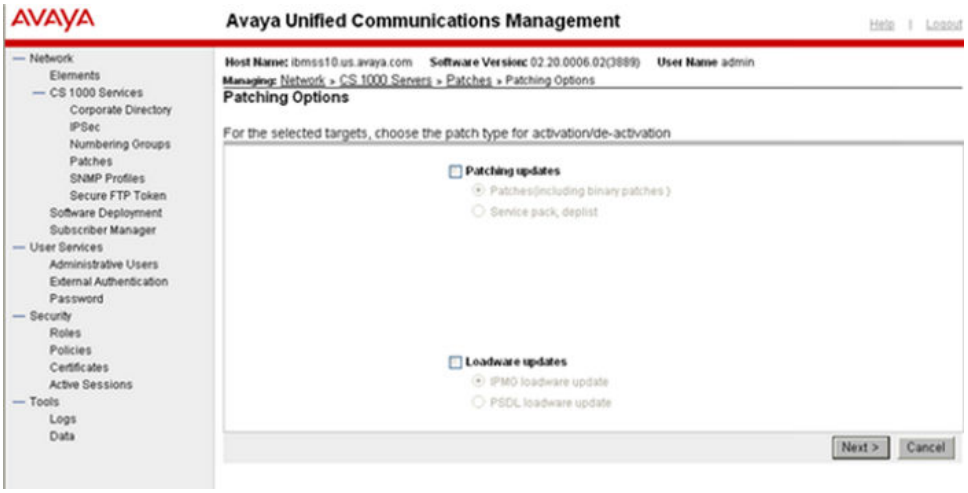

Figure 52: Patching Options page

Note:

The Co-resident Call Server section only displays if there are any Co-resident Call Server and Signaling Server systems.

6. In the Loadware updates section, select PSDL loadware update.
7. Click **Next**.

   The Distribute Patches Step 1 page appears.

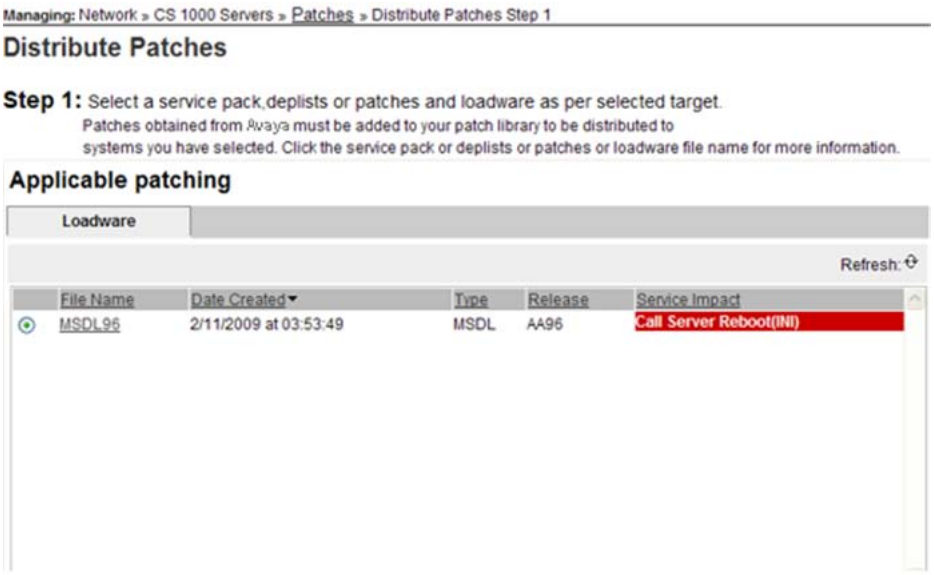

Figure 53: Distribute Patches Step 1 page

8. In the Applicable Loadware section, select the loadware to apply.

For loadware, applicable patches include all Loadware PEP available in the Central Patching Manager Library, excluding binary patches, Linux patches, and MGC loadware.

9. Click **Next**.

   The Activate Patches Step 3 page appears.

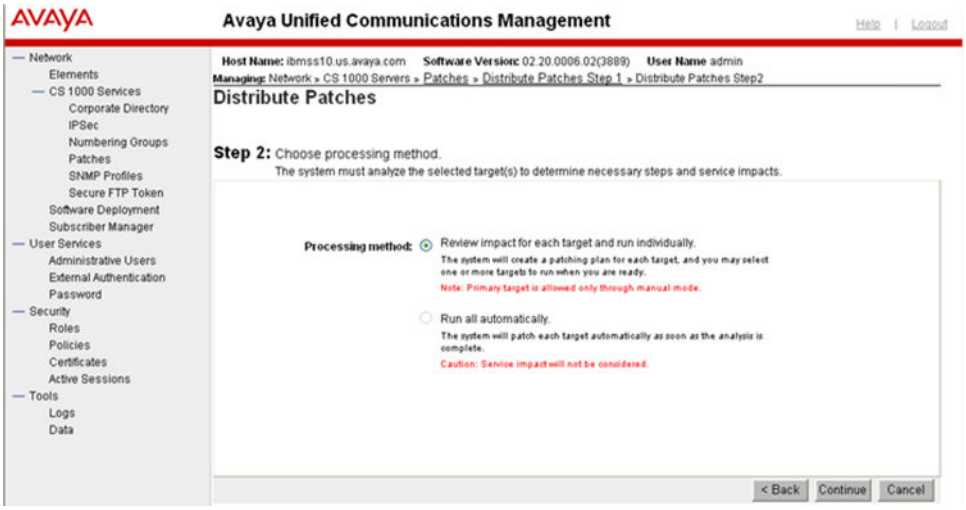

Figure 54: Activate Patches Step 3 page

10. On the Activate Patches Step 3 page, select the **Processing method**:

    - **Review impact for each target and run individually**—With this manual processing method, the impact of applying the selected patch or serviceability update is analyzed. This is the default method. A patching plan is created and presented for each selected target element. After you review the patching plan, you must manually initiate the patching operation for each element. You must take appropriate steps (such as idling down) before you start patching to avoid user impact.
    - **Run all automatically**—With this automatic processing method, each target element is patched automatically as soon as the analysis is complete.

      ⚠ Warning:

      Service impacts are not considered with the automatic method. For example, applications can restart as part of this operation.

11. Click **Continue**.

    The In Progress tab appears.

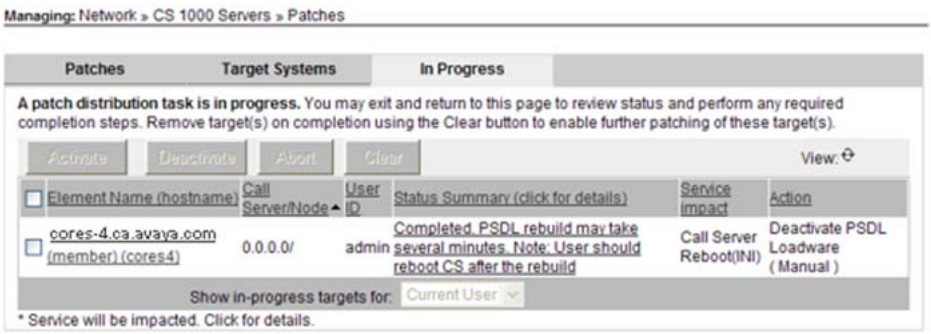

Figure 55: In Progress tab

Important:

Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

After a loadware completes, aborts, or fails, the status appears in the Status Summary column. You can click the link under the Status Summary column to view the details. When you click the status link, the Loadware Patching Status page appears.

Click **Back** to return to the previous page.

12. When the patching for a target element completes (or fails or aborts), click **Clear** to clear the summary report.
13. Repeat the patching process for each target, as required.

Deactivation workflow

Before you start patching deactivation operations, see Recommended order of patching operations on page 36.

- Deactivating a patch on page 84
- Deactivating a Call Server or Media Card patch on page 88
- Deactivating a MGC loadware patch on page 91
- Deactivating a PSDL loadware patch on page 93

Deactivate a patch

Use the following procedure to deactivate a patch or serviceability update. Service packs cannot be deactivated; however, you can deactivate items that were installed using a service

pack. This procedure is specific to patches; however, you can deactivate more than one type of patch during a patching session. Before you start patching deactivation operations, see Recommended order of patching operations on page 36.

Deactivating a patch

1. In the Patching Manager, select the **Target Systems** tab.
2. From the list of elements, select the check box for one or more elements for which to deactivate patches.

Figure 56: Elements to deactivate

3. Click **Next**.

   The Target Systems tab displays the selected elements. The Activate and Deactivate buttons are active.

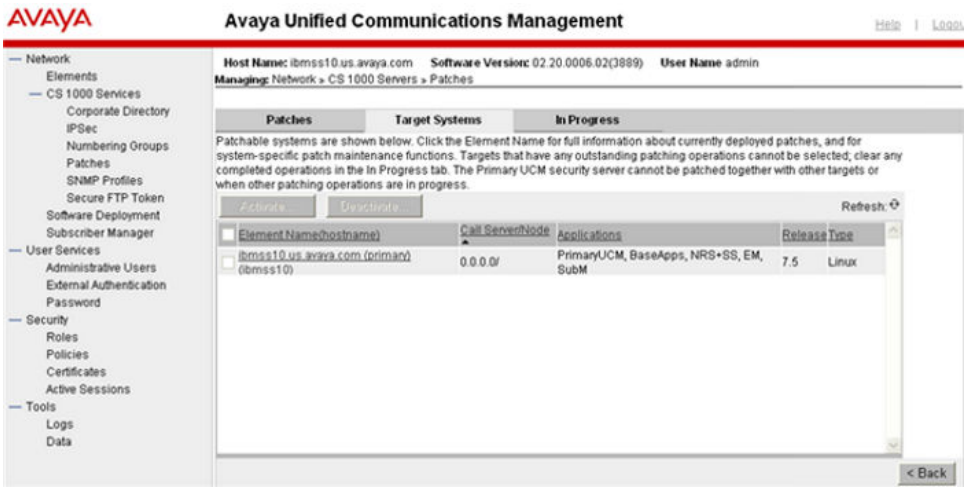

Figure 57: Target systems with selected elements

4. Click **Deactivate**.

   The Deactivate Patches Step 1 page appears. This page displays a list of all patches or serviceability updates (that are available for deactivation) that have been applied

by Central Patching Manager. These patches or serviceability updates may have been applied individually or using a service pack.

If the patch or serviceability update was never processed using Patching Manager, then the names of such patches (separated by commas) may be entered in the box at the bottom. Only patches applicable to the selected elements are displayed based on release and installed applications. However, some patches may not be in service on the selected elements; there will be an indication of no operation to be performed for these elements.

Figure 58: Deactivate Patches Step 1

5. On the Deactivate Patches Step 1 page, from the **Applied Patches** list, select the patches to deactivate.

   If applicable, you can also enter an additional patch to deactivate in the Additional Patch File name field.

6. Click **Next**.

   The Deactivate Patches Step 2 appears.

Figure 59: Deactivate Patches Step 2

7. On the Deactivate Patches Step 2 page, select the **Processing method**:

   - **Review impact for each target and run individually**—With this manual processing method, a patch deactivation plan is presented for each target. Review the patch deactivation plan. You must select each target and manually initiate the patch deactivation.
   - **Run all automatically**—With this automatic processing method, the patch deactivation occurs automatically as soon as the analysis is complete. In Automatic mode patch deactivation on each target occurs automatically as soon as the analysis is complete.

   Warning:

   Service impacts are not considered with the automatic method.

8. Click **Continue**.

   A dialog box appears prompting you to confirm the patch deactivation.

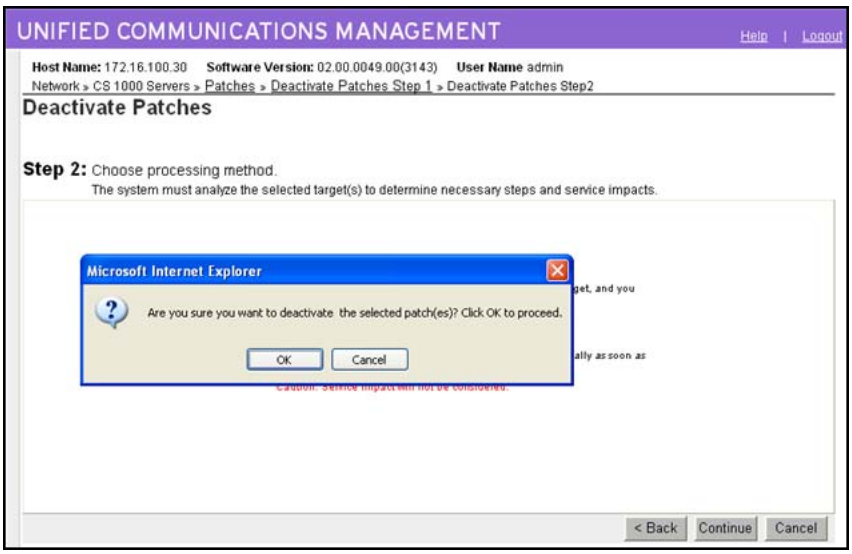

Figure 60: Confirmation dialog box

9. Click **OK** to confirm the patch deactivation.

   The In Progress tab appears.

   Important:

   Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.

10. If you selected the **Review impact for each target and run individually** option in 7 on page 86, the targets are analyzed based on the current patch information obtained from the target. Complete 11 on page 87 to 15 on page 88, and then proceed to 16 on page 88.

    OR

    If you selected the **Run all automatically** option in 7 on page 86, the targets are analyzed based on the current patch information obtained from the target. Unless there are errors detected, the patch deactivation proceeds automatically without waiting for your input. Wait while the patches are deactivated on the target. Proceed to 16 on page 88.

11. Under the **Status Summary** column, click the **Ready to Deactivate** link for each target to view the patching deactivation plan details for that target.

    The Patching Job Details page appears for the patch.

12. After you review the identified service impacts in the patching deactivation plan, click **Back**.

13. Select the check box for the target element.

    The Deactivate button is enabled.

14. Click **Deactivate** to start the patch deactivation.

    A dialog box appears prompting you to confirm the patch deactivation.

15. Click **OK** to confirm the patch deactivation.
16. Wait while the patch is deactivated on the target. The **Status Summary** column provides information about the patch deactivation progress.
17. Click the **Refresh** icon (in the upper-right corner of the View area) at regular intervals to obtain a progress update.
18. Wait for the process to complete. The Status Summary column indicates the process is **Completed**.
19. After you review your patching results and are satisfied with the results, select the check box for the target element and then click **Clear** to end the patching process for the selected target. You must click Clear before you can perform any other patch operations for this target element.

    Further patching activation and deactivation operations cannot be performed on the element until it is cleared.

    The In Progress tab disappears when all activities for all elements are cleared.

Deactivate a Call Server or Media Card patch

Use this procedureto deactivate patches for Call Server elements and Media Cards. Thisprocedure is specific to Call Server and Media Card patches; however,you can deactivate more than one type of patch during a patching session.Before you start patching deactivation operations, see Recommended order of patching operations on page 36.

Deactivating a Call Server or Media Card patch

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 61: Target Systems tab showing Network tree view

When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to deactivate patches.
3. Click **Next**.
4. From the list of elements, select the check box for one or more elements for which to deactivate patches.
5. Click **Deactivate**.

   The Patching Options page appears.

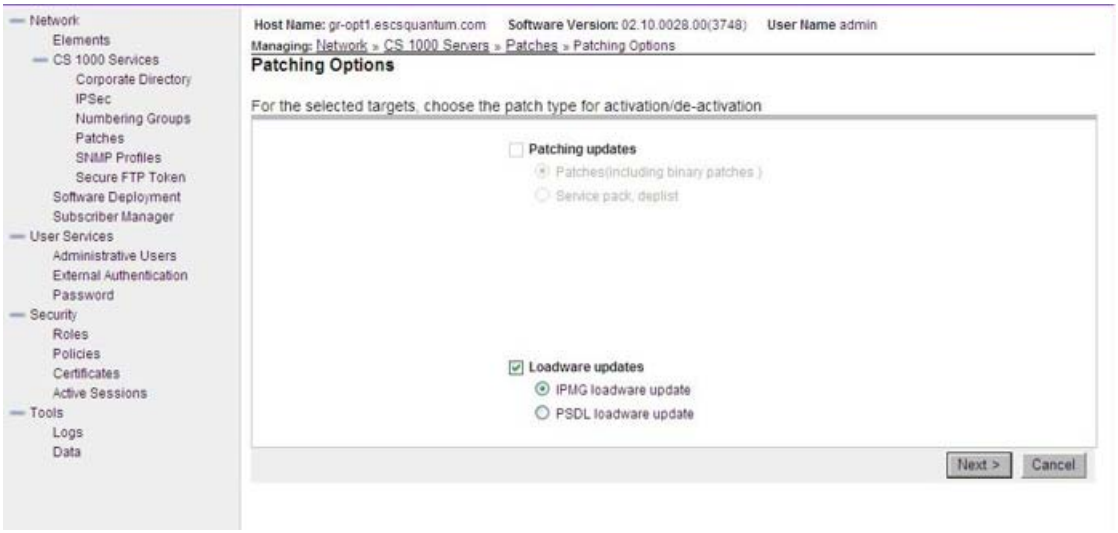

Figure 62: Patching Options page

6. Select the patch type for deactivation.
7. Click **Next**.

   The Deactivate Patches Step 1 page appears.

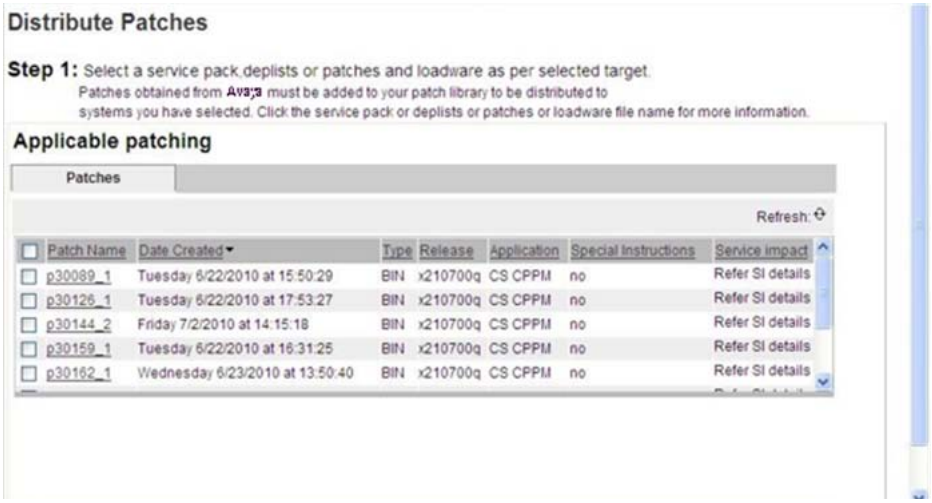

Figure 63: Deactivate Patches Step 1 page

The Applicable Patches are filtered and listed based on the targets selected on the Target Systems tab.

8. From the list of patches, select the patches to deactivate.
9. Click **Next**.

   The **Deactivate Patches Step 2** page appears.
10. On the Deactivate Patches Step 2 page, select the **Processing method**:

    - **Review impact for each target and run individually**—With this manual processing method, a patch deactivation plan is presented for each target. Review the patch deactivation plan. You must select each target and manually initiate the patch deactivation. This is the default option.
    - **Run all automatically**—With this automatic processing method, the patch deactivation occurs automatically as soon as the analysis is complete. In Automatic mode patch deactivation on each target occurs automatically as soon as the analysis is complete.

      ⚠ Warning:

      Service impacts are not considered with the automatic method.
11. Click **Continue**.

    A dialog box appears prompting you to confirm the patch deactivation.
12. Click **OK** to confirm the patch deactivation.

    The In Progress tab appears.

    If you selected the Run all automatically option, the targets are analyzed based on the current patch information obtained from the target. Unless there are errors detected, the patch deactivation proceeds automatically without waiting for your input. Wait while the patches are deactivated on the target.

When each target completes (or fails or aborts), select it and click **Clear** to clear the summary report.

You can click the link under the Status Summary column to view the deactivation details.

Deactivate a MGC loadware patch

Use this procedure to deactivate a MGC loadware patch. This procedure is specific to MGC loadware; however, you can deactivate more than one type of patch during a patching session. Before you start patching deactivation operations, see Recommended order of patching operations on page 36.

Note:

After deactivation, a MGC is updated with the GA version of its loadware type.

Deactivating a MGC loadware patch

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

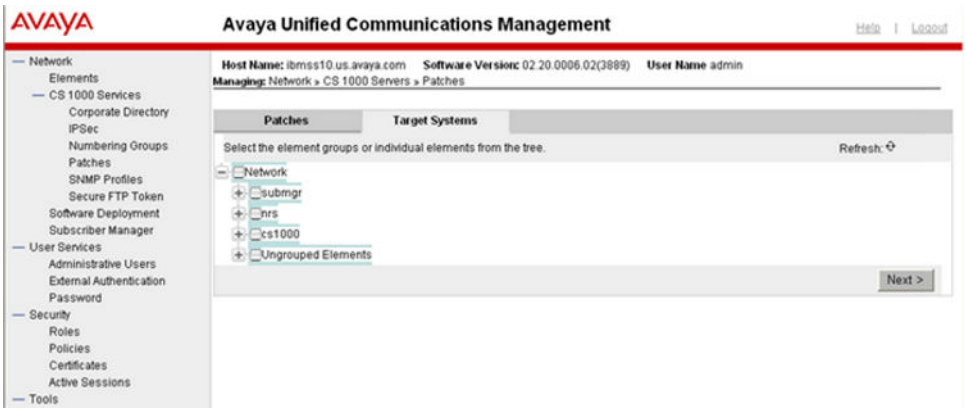

Figure 64: Target Systems tab showing Network tree view

   When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to deactivate patches.
3. Click **Next**.
4. From the list of elements, select the check box for one or more elements for which to deactivate patches.
5. Click **Deactivate**.

The Patching Options page appears.

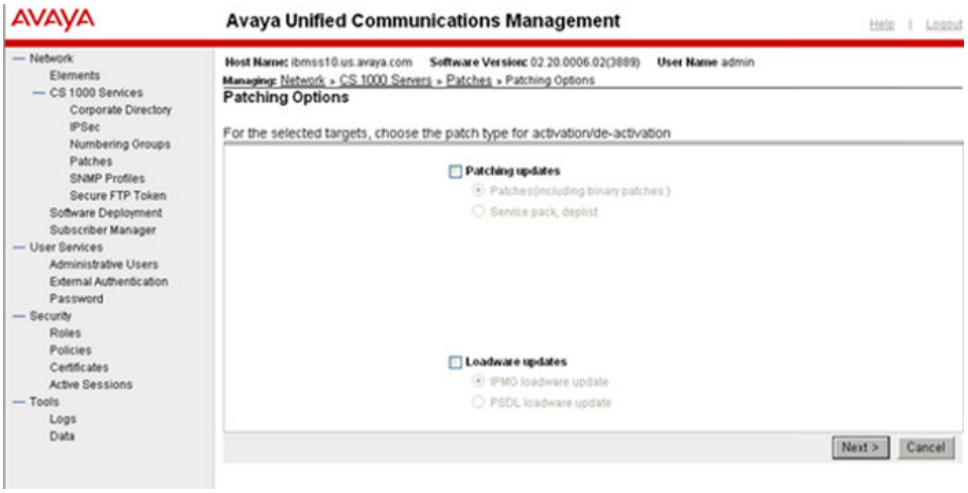

Figure 65: Patching Options page

If at least one Call Server element was selected, the Loadware type option is enabled.

6. Select the Loadware type.
7. Click **Next**.

   The Deactivate Patches Step 1 page appears.

   The Applicable Patches are filtered and listed based on the targets selected on the Target Systems tab.
8. From the list of patches, select the patches to deactivate.
9. Click **Next**.

   The **Deactivate Patches Step 2** page appears.
10. On the Deactivate Patches Step 2 page, select the **Processing method**:

    - **Review impact for each target and run individually**—With this manual processing method, a patch deactivation plan is presented for each target. Review the patch deactivation plan. You must select each target and manually initiate the patch deactivation. This is the default option.
    - **Run all automatically**—With this automatic processing method, the patch deactivation occurs automatically as soon as the analysis is complete. In Automatic mode patch deactivation on each target occurs automatically as soon as the analysis is complete.

      ⚠ Warning:

      Service impacts are not considered with the automatic method.
11. Click **Continue**.

A dialog box appears prompting you to confirm the patch deactivation.

12. Click **OK** to confirm the patch deactivation.

    The In Progress tab appears.

    If you selected the Run all automatically option, the targets are analyzed based on the current patch information obtained from the target. Unless there are errors detected, the patch deactivation proceeds automatically without waiting for your input. Wait while the patches are deactivated on the target.

    When each target completes (or fails or aborts), select it and click **Clear** to clear the summary report.

    You can click the link under the Status Summary column to view the deactivation details.

Deactivate a PSDL loadware patch

Use this procedure to deactivate a PSDL loadware patch. This procedure is specific to PSDL loadware; however, you can deactivate more than one type of patch during a patching session. Before you start patching deactivation operations, see Recommended order of patching operations on page 36.

Deactivating a PSDL loadware patch

1. In the Patching Manager, select the **Target Systems** tab.

   The Target Systems tree view displays the network nodes.

Figure 66: Target Systems tab showing Network tree view

   When you select or expand a branch, all other open branches at the same level collapse. However, any selections made within collapsed branches are retained.

2. From the Network navigation tree, select the check boxes of the nodes for which to deactivate patches.

3. Click **Next**.
4. From the list of elements, select the check box for one or more elements for which to deactivate patches.
5. Click **Deactivate**.

   The Patching Options page appears.

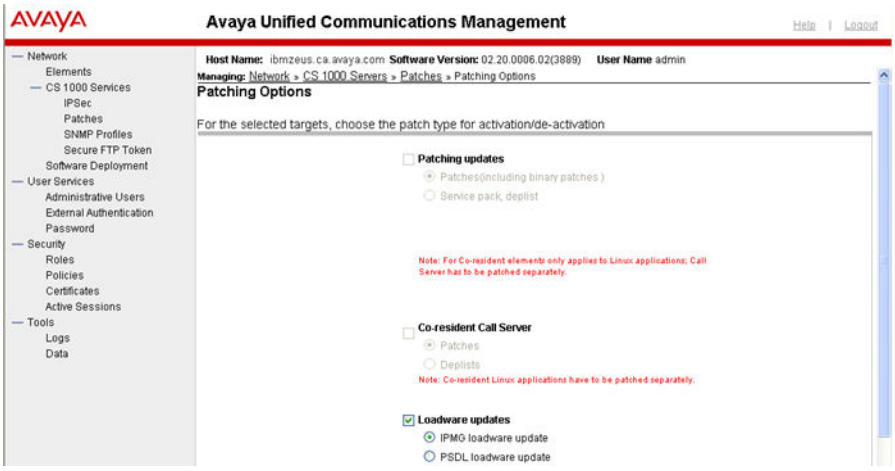

Figure 67: Patching options page

6. Under Loadware updates, select PSDL loadware update.
7. Click **Next**.

   The Deactivate Patches Step 1 page appears.

   The Applicable Patches are filtered and listed based on the targets selected on the Target Systems tab.
8. From the list of patches, select the patches to deactivate.
9. Click **Next**.

   The **Deactivate Patches Step 2** page appears.
10. On the Deactivate Patches Step 2 page, select the **Processing method**:

    - **Review impact for each target and run individually**—With this manual processing method, a patch deactivation plan is presented for each target. Review the patch deactivation plan. You must select each target and manually initiate the patch deactivation. This is the default option.
    - **Run all automatically**—With this automatic processing method, the patch deactivation occurs automatically as soon as the analysis is complete. In Automatic mode patch deactivation on each target occurs automatically as soon as the analysis is complete.

      ⚠ Warning:

      Service impacts are not considered with the automatic method.

11. Click **Continue**.

    A dialog box appears prompting you to confirm the patch deactivation.

12. Click **OK** to confirm the patch deactivation.

    The In Progress tab appears.

    If you selected the Run all automatically option, the targets are analyzed based on the current patch information obtained from the target. Unless there are errors detected, the patch deactivation proceeds automatically without waiting for your input. Wait while the patches are deactivated on the target.

    When each target completes (or fails or aborts), select it and click **Clear** to clear the summary report.

    You can click the link under the Status Summary column to view the deactivation details.

Chapter 7: Local Patching Manager

The Local Patching Manager interface runs directly on each Linux element and supports patching only for that specific element. The Local Patching Manager provides a list of patches on the server with the status (such as Unloaded, Loaded, and In-Service). It also provides storage space management for patches.

Patching can occur on a single-target basis using the Local Patching Manager (within Base Manager). The Local Patching Manager can be used to augment the Central Patching Manager in the following ways:

- To view the current state of a patch.
- To remove existing patches to avoid conflicts (if necessary).
- To remove patches in failure scenarios.

Base Manager can be used for related activities, such as the following:

- Application maintenance for starting, stopping, and restarting before and after patching. (This process depends on the instructions in each patch.)
- To restart the server (if necessary).

When patching finishes, generally all application restarts or reboots occur automatically. It is necessary to take manual action only if indicated in the special instructions for the patch. Manual actions may be necessary in case of patching errors. For example, if a patch deactivation fails, then an application may be stopped and not restarted. The patch details show applications to restart and the status of these applications can be checked to see if action is required.

Important:

In this document, the term patch or patches includes both patches and serviceability updates (SUs) unless explicitly mentioned otherwise because patches and SUs are applied in the same way.

This chapter provides procedures to perform the following in the Local Patching Manager:

- Add, activate, deactivate, and delete patches.
- Add, activate, and delete service pack. (Service packs cannot be deactivated; however, patches that are part of a service pack can be deactivated.)

Note:

The Special Instructions must be followed for the first time installation of LinuxBase, BaseWeb or PatchWeb Application SU's (when applicable); and whenever a newer version of these SU’s are available. This requires using command line interface (CLI) to apply the Linux base serviceability update (SU) to all Linux elements. You must also apply the Base Web SU to the UCM Primary Security Server using the CLI (and Patchweb). The reason behind these instructions are due to the fixes that may be required to the Linux operating system (OS), Patch Deployment Manager or the underlying base patching framework to allow the Service pack installation to function correctly. If these instructions are not followed, this may result in a Patch activation failed error message.

Download and save patches, serviceability updates, and service packs

The Enterprise Solutions PEP Library (ESPL) provides online access to Avaya-approved Product Enhancement Package (PEP) solutions for Enterprise products. To download the required patches, serviceability updates, and service packs and save them on your client PC, see Download and save patches, serviceability updates, and service packs on page 40.

Access the Local Patching Manager

You can access Local Patching Manager by being redirected from the UCM network level or from Element Manager (using a log in to the UCM framework). For these cases, the role of the user governs whether access is permitted to local patching capabilities. Access to the Local Patching Manager is controlled by the permission for the element. The patchAdmin permission must be assigned for the element (either individually or in All elements of type: Linux Base). This element-level permission is allocated to a role, which in turn is assigned to a user.

You can also access the Local Patching Manager using local login to Base Manager. When a local log on is performed (this could be with an emergency account), you have complete access to all Base Manager functionality, including patching

Use the following procedure to access the Local Patching Manager.

Accessing the Local Patching Manager from the Base Manager

1. Log on to UCM.
2. In the Elements pane, under the **Element Name** column, select the element to patch.

   Base Manager appears for the element.
3. In the Base Manager navigation tree, select **Software > Patches**.

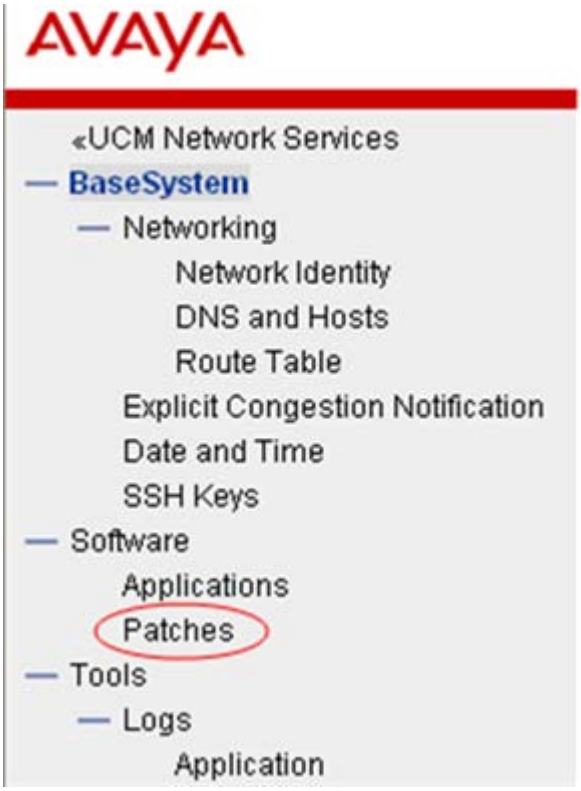

Figure 68: Base Manager navigation tree: Patches

You can also access the Local Patching Manager in the following ways:

- In the UCM Central Patching Manager, select the Targets Systems (Linux only) tab, and then select an element name to open the Local Patching Manager for that element.
- When Base Manager is accessed with a local logon (using local or emergency account).

The Local Patching Manager (within Base Manager) appears for the element. The page is called Patches (element host name) where element host name is the name of the server.

Figure 69: Local Patching Manager

The Local Patching Manager has two main tabs: Service Packs and Patches.

On the Service Packs tab, you can add or delete service packs. After you add service pack, you can view details for the service pack. Service packs can also be activated on the Service Packs tab but cannot be deactivated. You can perform the following procedures on the Service Packs tab:

- Adding a service pack on page 100
- Viewing service pack details on page 102
- Deleting a service pack on page 103
- Activating a service pack on page 105

On the Patches tab, you can add or delete patches or serviceability updates. You can also view details for the patches you have added on the element. Patches and serviceability updates can be both activated and deactivated. (This tab is selected by default.) You can perform the following procedures on the Patches tab:

- Adding a patch on page 109
- Viewing patch details on page 110
- Activating patches on page 111
- Deactivating a patch on page 114
- Deleting a patch on page 115

Add a service pack

Use the following procedure to add a service pack to the element.

Adding a service pack

1. In the Local Patching Manager, select the **Service Packs** tab.

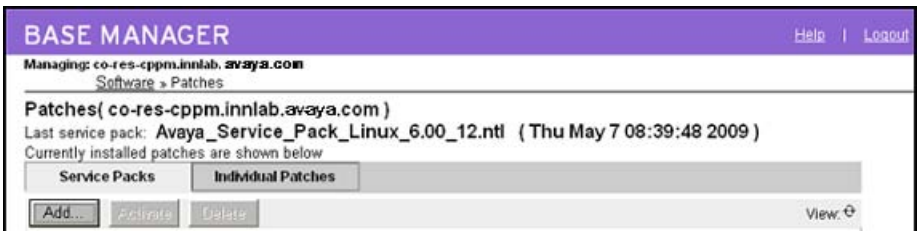

Figure 70: Service Packs tab

2. Click **Add**.

   The New Service Pack page appears.

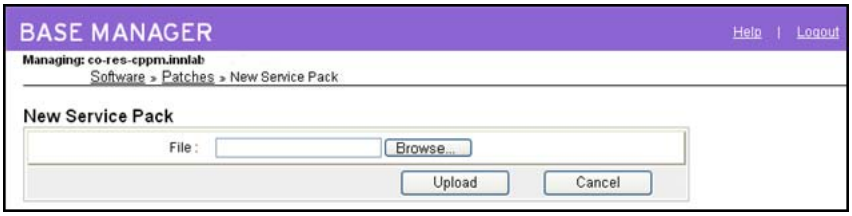

Figure 71: New Service Pack

3. Click **Browse**.

   The Choose File dialog box appears.

4. In the Choose File dialog box, browse to the find the service pack on your client PC.

5. Select the service pack file, and click **Open**.

   The file appears in the File field.

6. Click **Upload**.

   The Local Patching Manager validates the file. The service patch file appears on the Service Pack tab. The Service Pack tab displays the new service pack and it details.

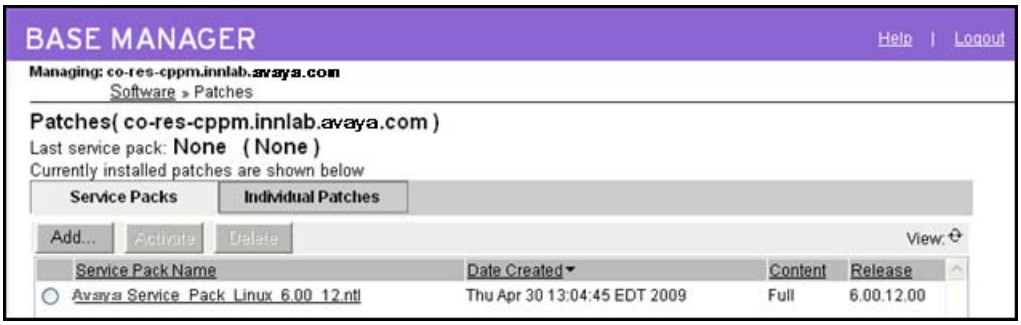

Figure 72: Added service pack

For more information, see View service pack details on page 102.

View service pack details

Use the following procedure to view the details about a service pack and the individual patches that it contains. The Service Pack Details page displays important details about a service pack and patches such as header information.

Viewing service pack details

1. In the Local Patching Manager, select the **Service Packs** tab.
2. To view details of the service pack, under the **Service Pack Name** column, click the name of the service pack file.

   The Service Pack Details (sp_name) page appears; sp_name is the name of the service pack.

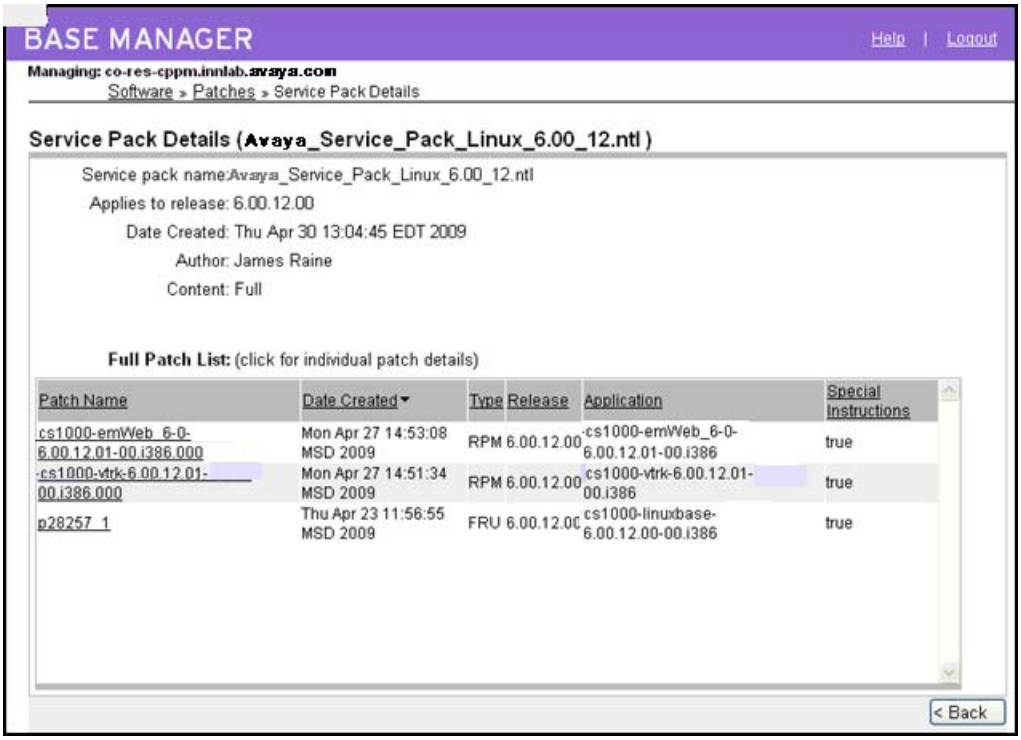

Figure 73: Service Pack Details

3. On the **Service Pack Details (sp_name)** page, review the detailed information about the service pack.
4. To review an individual patch in the service pack, under **Full Patch List**, click the name of the patch.

The Patch Details (patch_name) page appears. This page provides details such as patch file name, service impact, dependent patches, obsolete patches special instructions, and other details from the patch header.

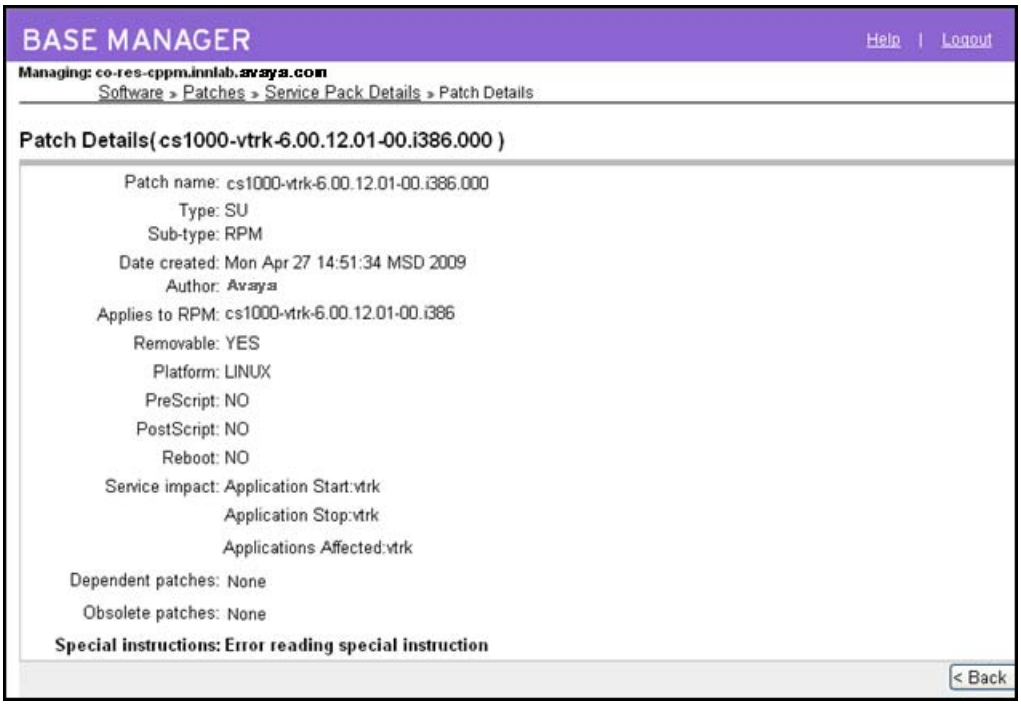

Figure 74: Patch Details

5. To return to the Service Pack Details page, click **Back** on the Patch Details page.
6. To return to the Service Packs tab, click **Back** on the Service Pack Details page.

Delete a service pack

Use this procedure to delete a service pack from the element. Service packs stay on the target element until you manually remove them. Deleting a service pack does not delete or deactivate the patches or serviceability updates that were included within service pack.

Deleting a service pack

1. In the Local Patching Manager, select the **Service Pack** tab.
2. Select the option button for the service pack to delete.

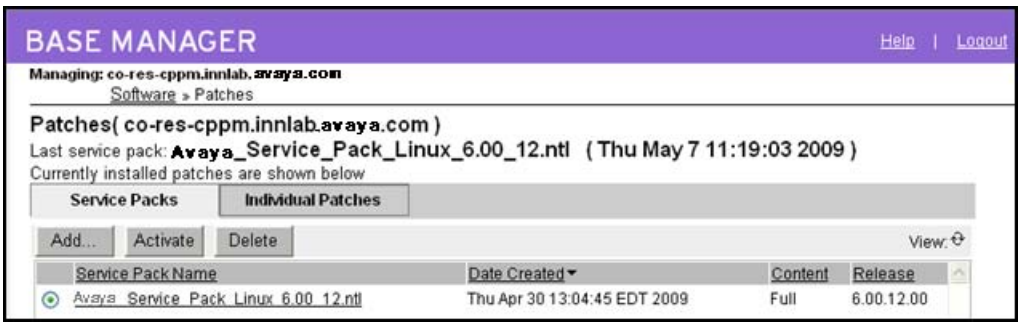

Figure 75: Select service pack

3. Click **Delete**.

   A dialog box appears prompting you to confirm the service pack deletion.

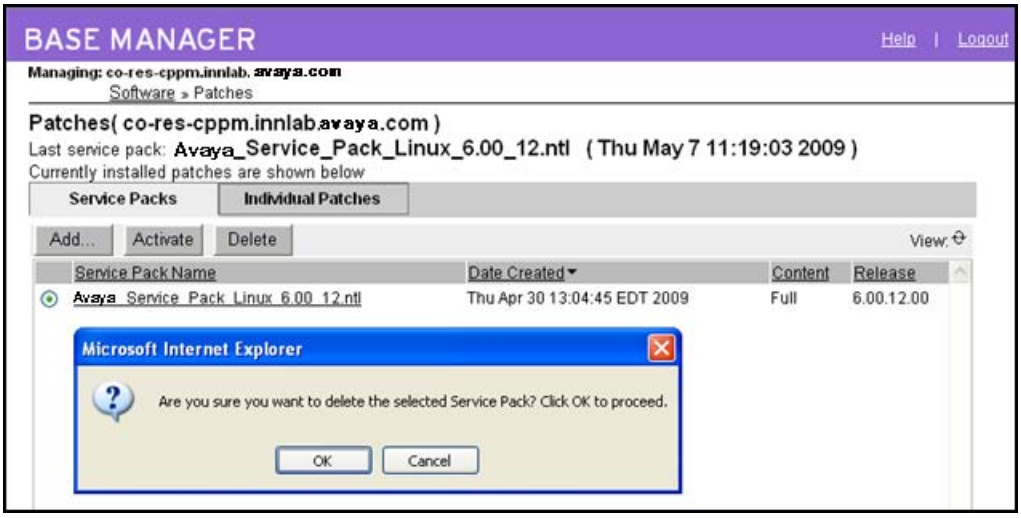

Figure 76: Confirm service pack deletion

4. Click **OK** to confirm the deletion of the service pack.

   The service pack is removed from the list on the Service Packs tab.

Activate a service pack

Use the following procedure to apply a service pack to the element. When you activate a service pack, all the applicable patches and serviceability updates within the service pack are loaded and placed in service.

Note:

You can activate only one service pack at a time. You cannot activate a service pack together with patches or serviceability updates.

Activating a service pack

1. In the Local Patching Manager, select the **Service Packs** tab.
2. From the list of service packs, select the option button for the service pack to activate on the element.

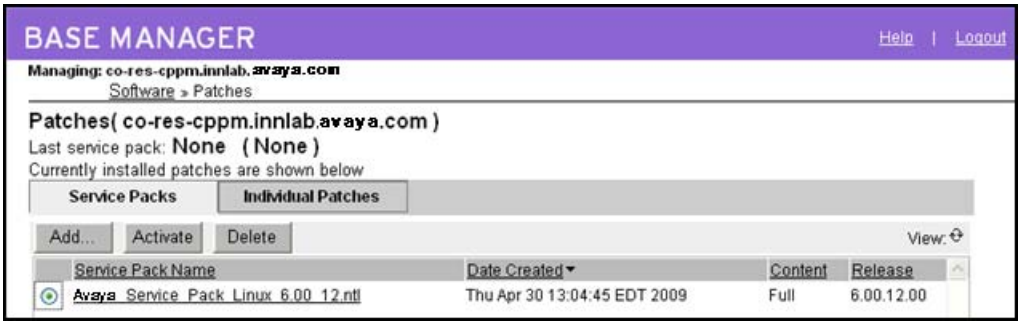

Figure 77: Select the service pack

3. Click **Activate**.

   The Patching Job Details page appears. The status changes from Queued for Patching to Ready to Load: x new patches (x is the number of patches in the service pack).

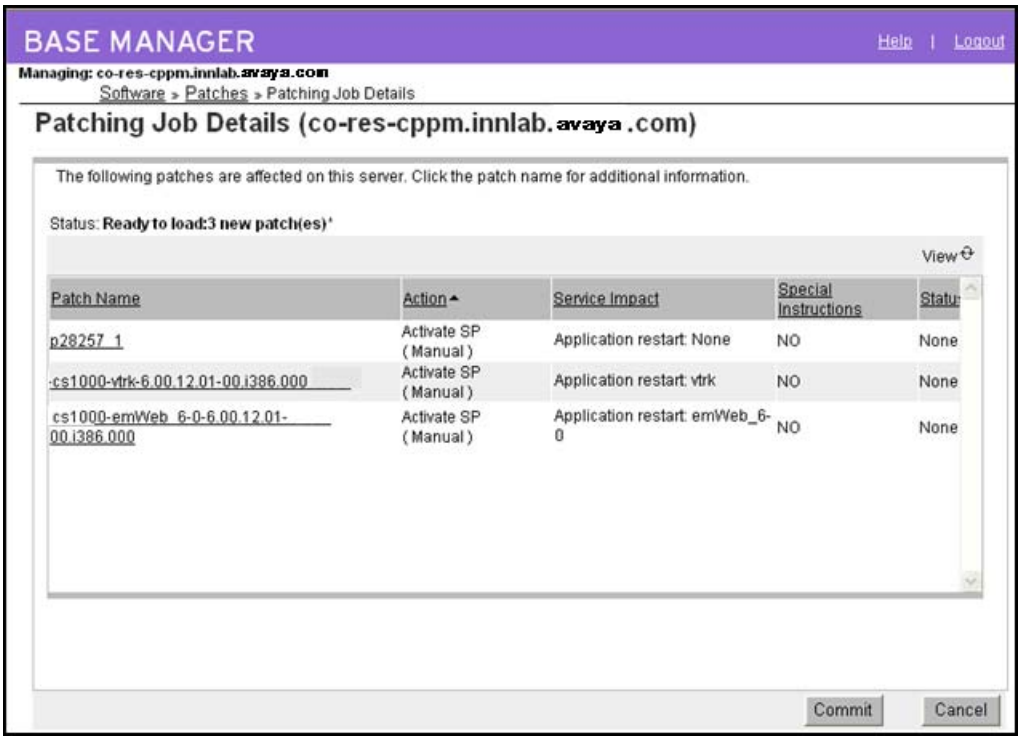

Figure 78: Patching Job Details - Ready to load

4. In the **Service Impact** column, review the service impacts for the patches and serviceability updates.
5. In the **Special Instructions** column, verify whether any patches have Special Instructions equal to **YES**. Review the patch if there are special instructions.
6. To review the details for a specific patch, under the **Patch Name** column, click the link for the patch.

   The Patch Detail (patch_name) page appears.

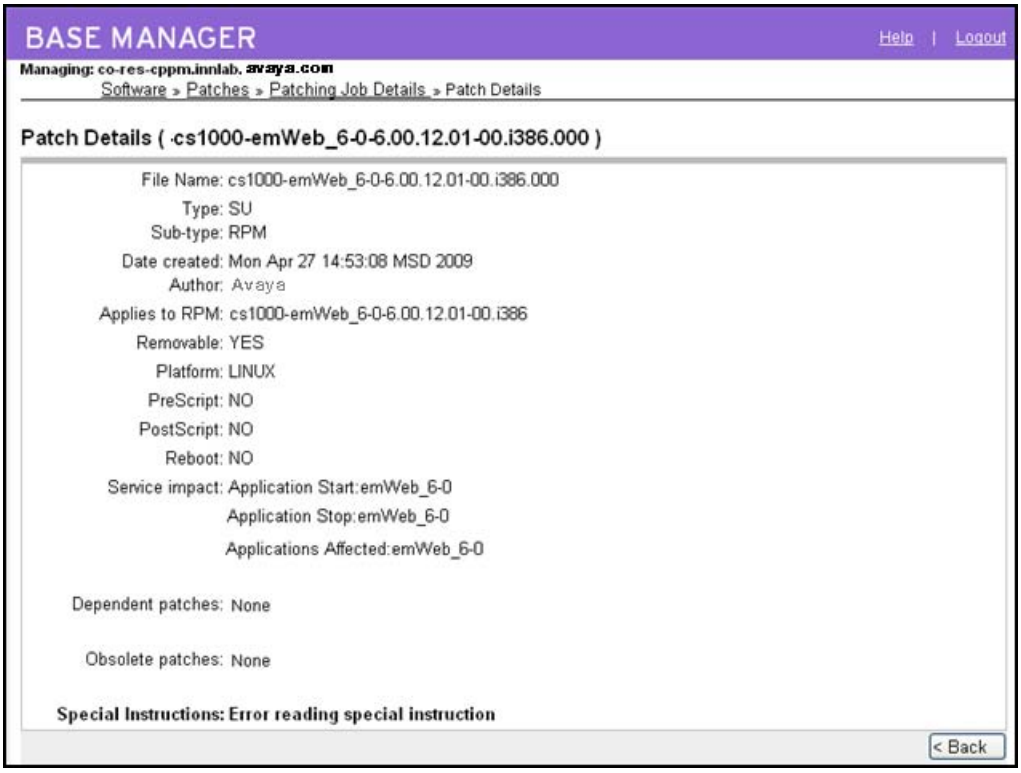

Figure 79: Patch Details (patch_name)

7. Click **Back** to return to the Patching Job Details page.
8. Click Commit.

   The status changes from Queued for Patching to In Progress. For more information, see Table 2: Status information on page 33.

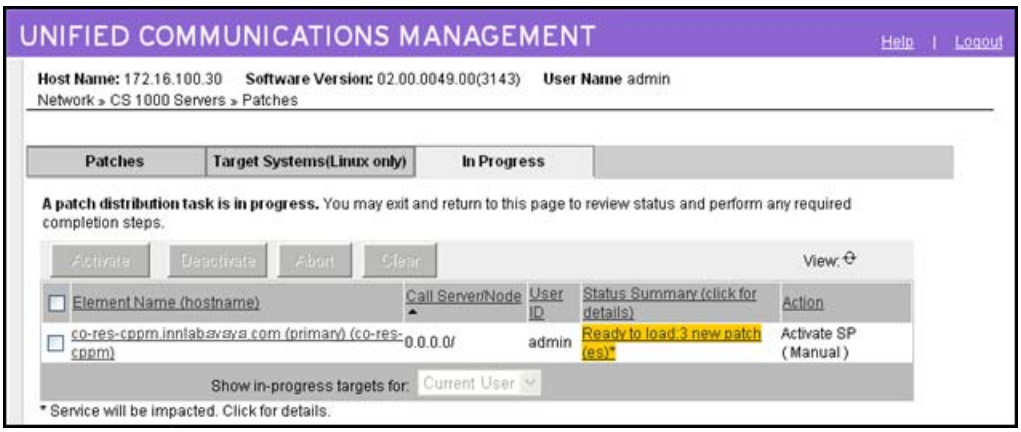

Figure 80: Patching Job Details - In Progress

9. Wait while the service pack is activated.

   The time required to activate a service pack depends on the number patches in the service pack.

   When the service pack is activated, the Status field changes to Completed (at the top of the window). The overall status for the service pack activation is provided as a link at the top of the page.

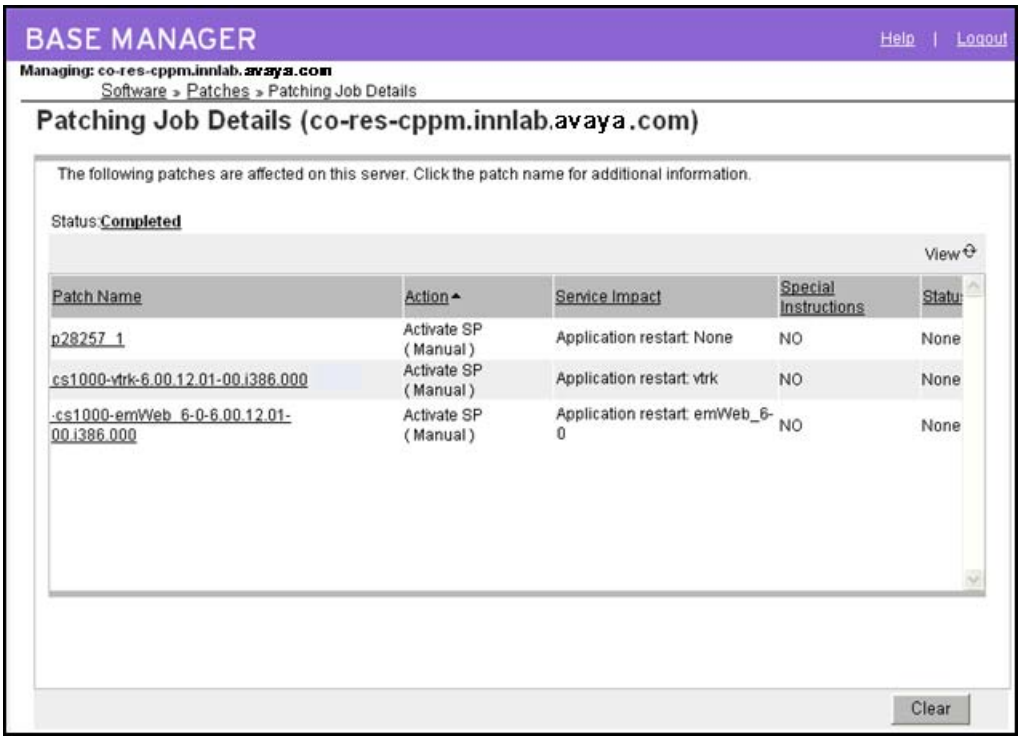

Figure 81: Activation complete

10. Click the **Completed** status link.

The Service Pack Status page appears and the output from the underlying base service pack installation appears.

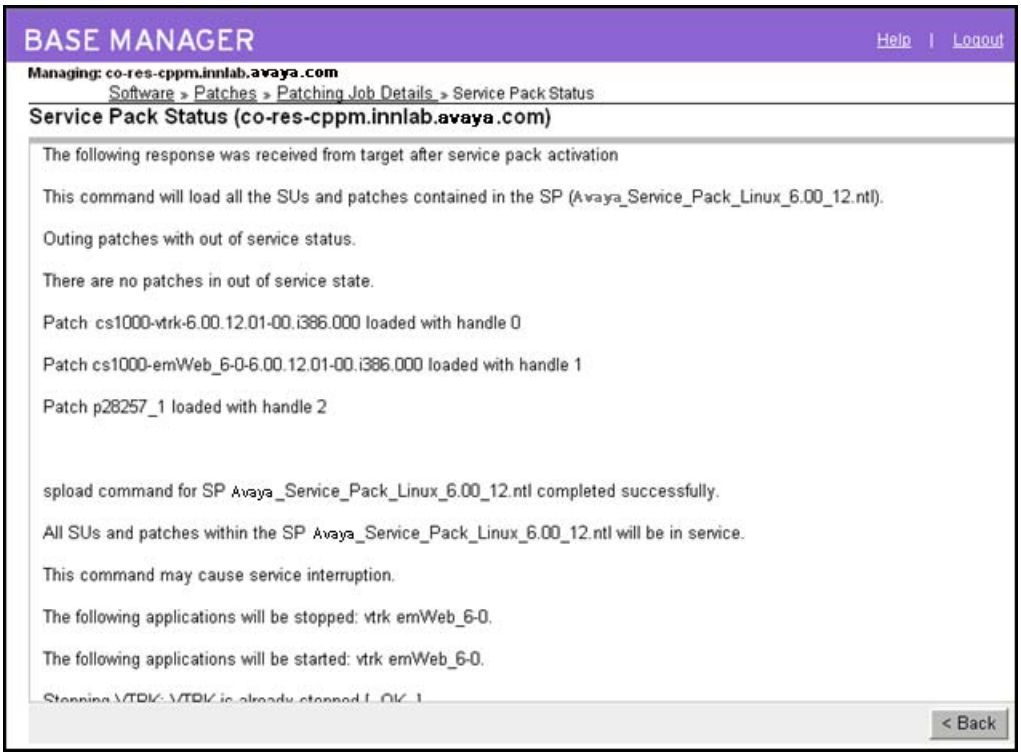

Figure 82: Service Pack Status

11. Click **Back** to return to the Patching Job Details page.
12. On the Patching Job Details page, click **Clear**.

    The Service Pack tab appears.
13. Select the **Patches** tab, in the **Status** column, verify that the patches are **In service**.

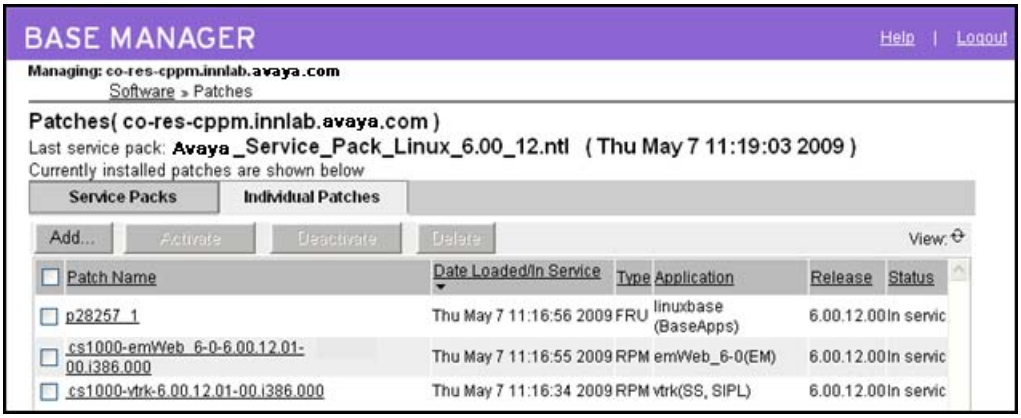

Figure 83: In service patches

Add a patch

Use the following procedure to add a patch to the element.

Adding a patch

1. In the Local Patching Manager, ensure the **Individual Patches** tab is selected.

Figure 84: Patches tab

2. Click **Add**.

   The New Patch File page appears.

Figure 85: New Patch File

3. Click **Browse**.

   The Choose File dialog box appears.

4. In the Choose File dialog box, browse to the find the patch on your client PC.
5. Select the patch file, and click **Open**.

   The file appears in the File field.

6. Click **Upload**.

The Patching Manager validates the file. The patch file appears on the Patches tab. The Patches tab displays the new patch and it details. New patches are in an Unloaded state.

Figure 86: Added patch

For more information, see View patch details on page 110.

View patch details

Use the following procedure to view the details about a specific patch. The Patch Details page displays important details about the patch from the header information.

Viewing patch details

1. In the Local Patching Manager, select the **Individual Patches** tab.
2. To view details for a patch, under the **Patch Name** column, click the name patch.

   The Patch Details (patch_name) page appears; patch_name is the name of the patch.

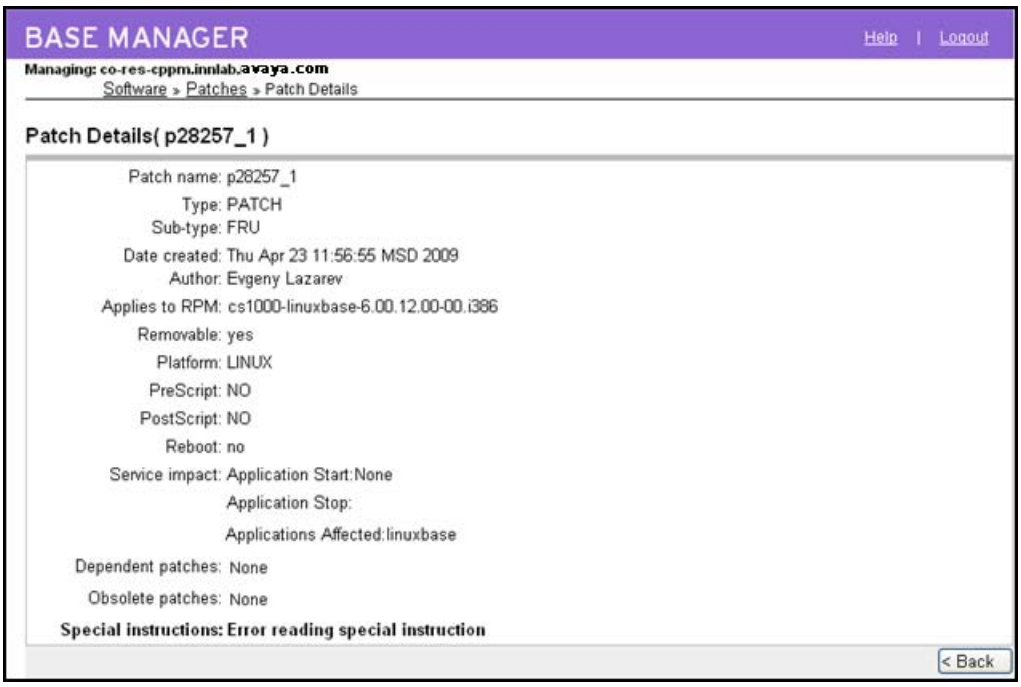

Figure 87: Patch Details

3. On the **Patch Details (patch_name)** page, review the detailed information about the patch.
4. To return to the Patches tab, click **Back** on the Patch Details page.

Activate patches

Use the following procedure to apply a patch or multiple patches to the element. Activating a patch loads the patch and places it in service.

Activating patches

1. In the Local Patching Manager, select the **Individual Patches** tab.
2. From the list of patches, select the check box for the patches to activate on the element.

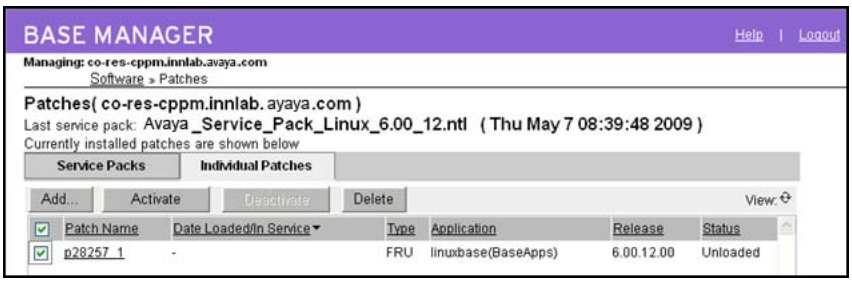

Figure 88: Select patch to activate

3. Click **Activate**.

   The Patching Job Details page appears. The status changes from Preprocessing to Ready to Load. For more information, see Table 2: Status information on page 33.

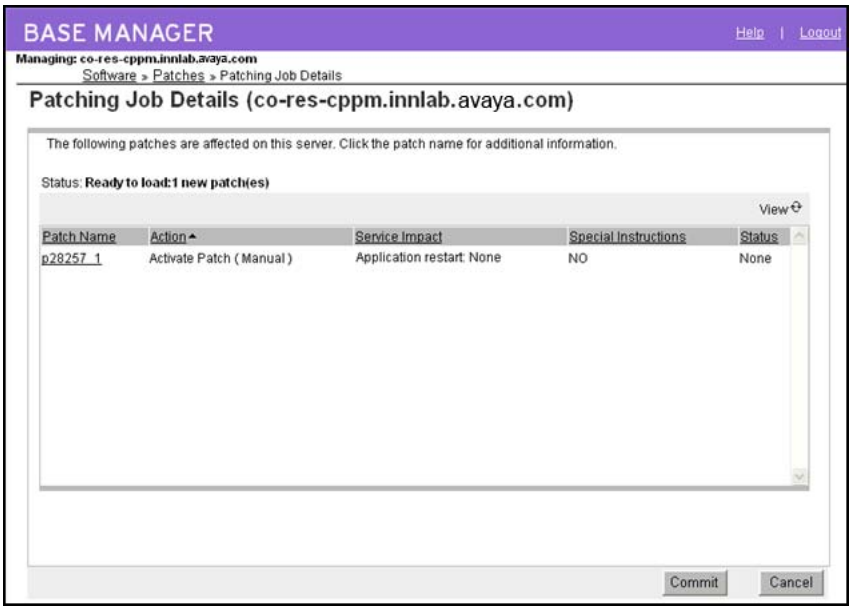

Figure 89: Patching Job Details - Ready to Load

   New patches are in Loaded status. You can select any patches that are loaded (but not in service) and place them in service. Patches may have been placed in the Loaded state by the CLI, by failure of service pack activation, or if an issue arises with installing the patch after it is loaded.

4. Click Commit.

   The status changes from Queued for Patching to In Progress.

5. Wait while the patch is activated.

   When the patch is activated, the status changes to **Completed** (at the top of the window) and the Status column indicates that the patch succeeded.

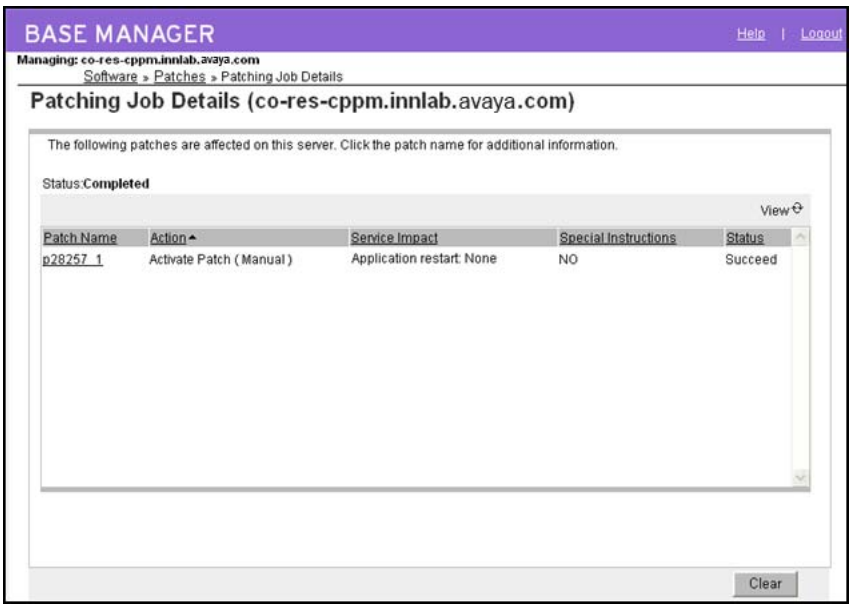

Figure 90: Patching Job Details - Completed

6. Before proceeding with additional patch activation, click **Clear** to end the patching process.

   The Patches tab appears.

7. On the Individual Patches tab, under the **Status** column, verify that the patch is **In Service**.

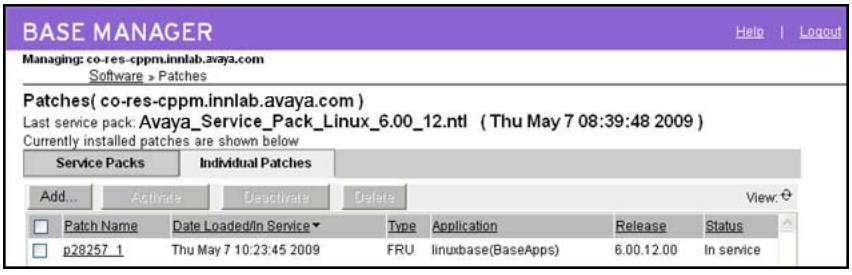

Figure 91: In service patch

Deactivate a patch

Use the following procedure to deactivate a patch or serviceability update. When a patch is deactivated, is it taken out of service and is unloaded.

Note:

You cannot deactivate service packs; however, patches that are part of a service pack can be deactivated.

Deactivating a patch

1. In the Local Patching Manager, select the **Individual Patches** tab.
2. From the list of patches, select the check box for patch to deactivate. (The status of the patch must be In Service.)

   The Deactivate button is enabled.

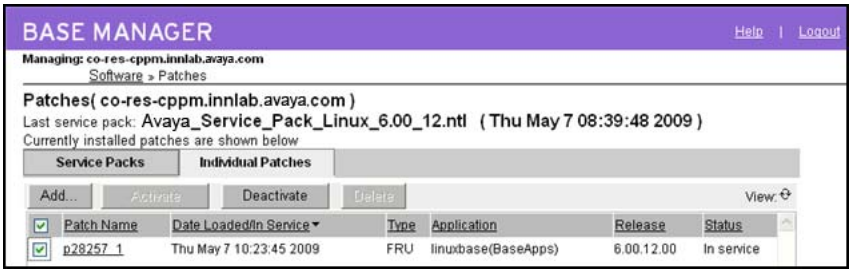

Figure 92: Select patch to deactivate

3. Click **Deactivate**.

   A dialog box appears prompting you to confirm the deactivation of the patch.

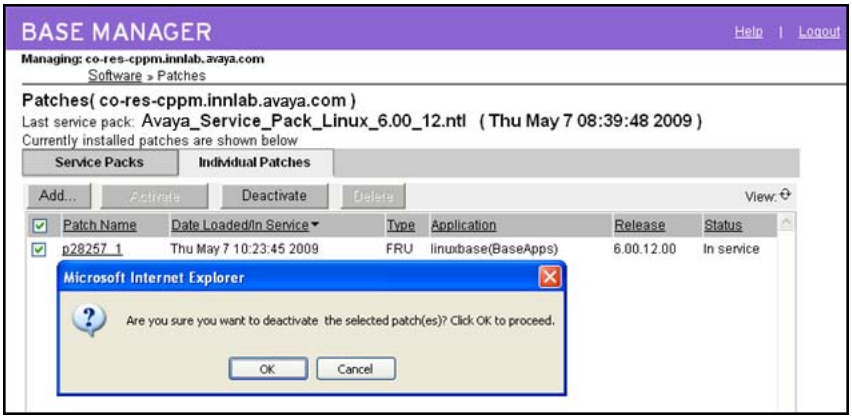

Figure 93: Confirm deactivation

4. Click **OK** to confirm the patch deactivation.
5. Wait for the deactivation process to complete.

   The Patching Job Details appears.
6. On the Patching Job Details page, verify that the **Status** is **Completed** and that the **Status** column displays **Succeed**.

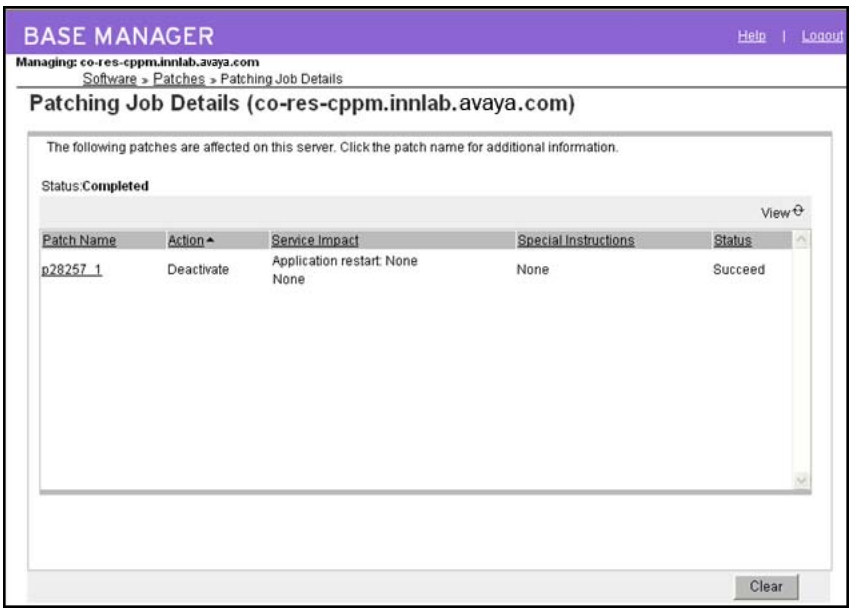

Figure 94: Deactivation Complete

7. On the Patching Job Details page, click **Clear**.

   The Individual Patches tab appears.

8. Verify that the **Status** column says **Unloaded** for the patch you deactivated.

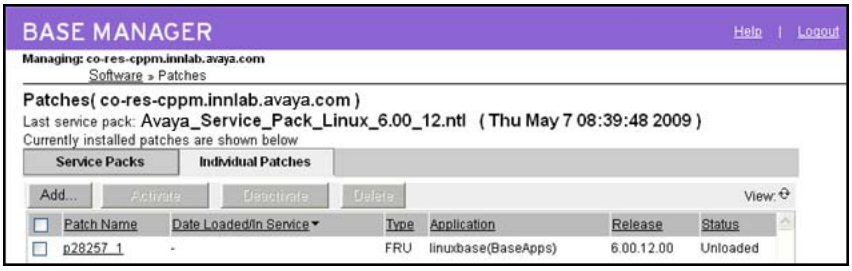

Figure 95: Unloaded patch

Delete a patch

Use this procedure to delete a patch from the element. A patch must have an Unloaded status to be deleted.

Deleting a patch

1. In the Local Patching Manager, ensure the **Individual Patches** tab is selected.
2. Select the check box for the patch to delete and verify that the patch has an **Unloaded** status.

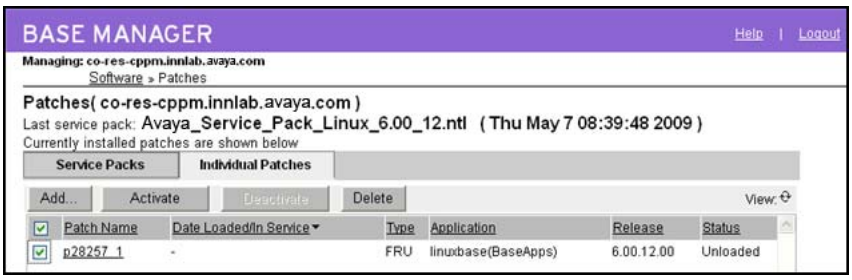

Figure 96: Select patch

3. Click **Delete**.

   A dialog box appears prompting you to confirm the deletion of the patch.

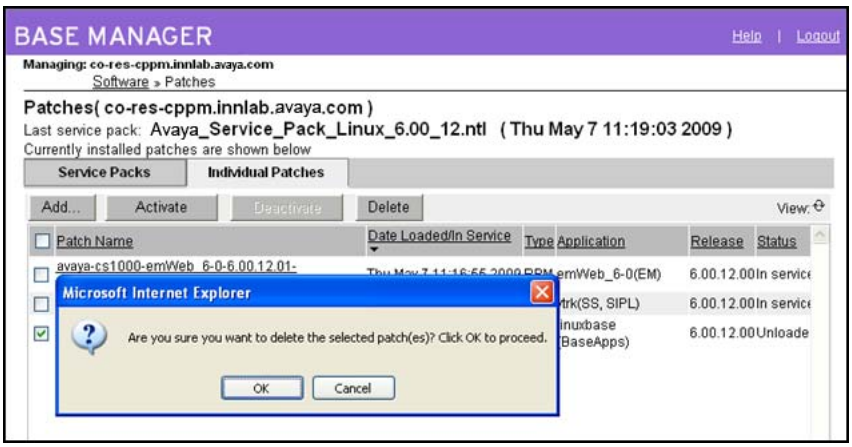

Figure 97: Confirm deletion

4. Click **OK** to confirm the patch deletion.

   The patch is removed from the list.

Chapter 8: CLI commands

This chapter describes the Command Line Interface (CLI) commands for Linux and VxWorks patching.

You must have an account with the patching permissions to run these CLI commands.

The CLI commands are available for patches, serviceability updates, loadware, deplists, and service packs. For more information, see the following:

- Target patch and serviceability update commands on page 119
- Loadware commands on page 123
- Target service pack commands on page 125
- Call Server target commands on page 129

Use the following procedure to issue patching CLI commands.

Patching using the CLI

1. Log on using the admin2 account.
2. After you log on, enter the CLI command **`swVersionShow`** and press Enter.

   The installed applications and the application version numbers are displayed, as shown in Figure 98: Installed applications and version numbers on page 118.

   Figure 98: Installed applications and version numbers on page 118 contains the base or application name in the left column and the corresponding version number in the right column. Note the Product Release that you are patching. You must use the correct version number to retrieve the correct patch or serviceability update from the ESPL.

   Important:

   The application version returned by the **`swVersionShow`** command may not match the versions of RPMs constituting the application. Always refer to the RPM versions returned by the **`issp`** command when determining patch applicability.

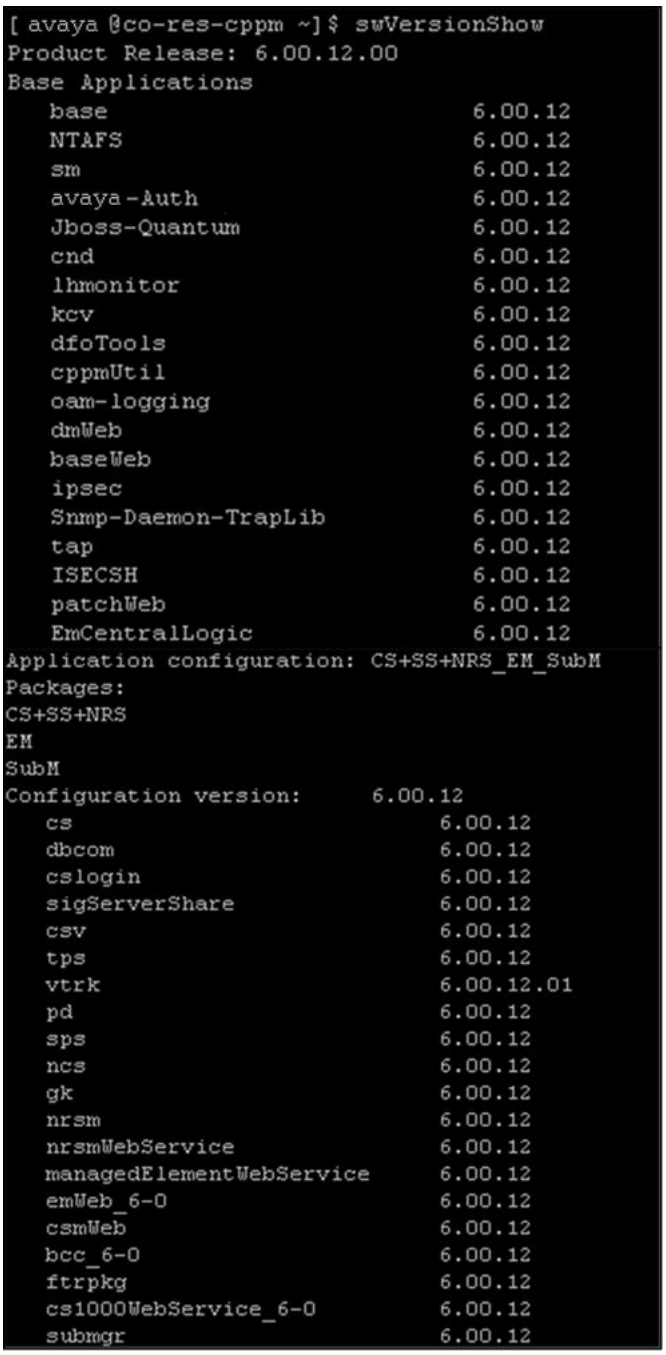

Figure 98: Installed applications and version numbers

3. Retrieve a patch, serviceability update, or service pack file from the ESPL. For more information, see Download and save patches, serviceability updates, and service packs on page 40.
4. Upload the serviceability updates and patch files to the Linux server and save it in the /var/opt/avaya/patch folder. Service packs are uploaded to the Linux server and are saved in the /var/opt/avaya/sp folder.

Secure File Transfer Protocol (SFTP) and Secure Copy (SCP) are the supported methods of patch file transfer.

The patch file transfer is initiated from the Linux server or from an external computer.

- To initiate the patch file transfer from within the Linux server:
  - Log on to the Linux server as admin2.
  - Enter the **sftp** or **scp** CLI command.
  - Enter the **get** command (for **sftp**) or the **scopy** command (for **scp**) to transfer the patch to the Linux server.
- To initiate the patch file transfer from an external machine:
  - Initiate an SFTP or Secure Shell (SSH) program.
  - Provide the IP address (or host name) of the Linux server, the Avaya user ID, and password as parameters.
  - Enter the **put** command (for **sftp**) or the **scopy** command (for **scp**) to transfer the patch to the Linux server.

5. Perform the required on-target patch management CLI commands. The on-target patch management CLI provides an interface command set similar to the CS 1000 patcher. For more information, see the following:
   - Target patch and serviceability update commands on page 119
   - Target service pack commands on page 125

Target patch and serviceability update commands

The following CLI commands are available for patches and serviceability updates:

pstat

Syntax: **pstat** <*handle*>|-l, --list|-a, --all|-h, --help

Parameter	Description
<*handle*>	Prints status information about the patches and serviceability updates with <*handle*>.
--list or -l	Lists all installed in-service patches and serviceability updates.
--all or -a	Lists all in-service and out-of-service patches and serviceability updates in detail.
--help or -h	Prints information about the **pstat** command.

Description: Prints a status summary of all installed patches and serviceability updates (loaded, in-service, and out-of-service patches and serviceability updates).

Example 1: Print the information for all installed in-service patches and serviceability updates.

```
$ pstat -l

Product Release: 6.00.00.00
In service patches: 1
```

PATCH#	NAME	IN_SERVICE	DATE	SPECINS	TYPE	RPM
1	p20002_1	yes	10/03/07	no	FRU	mlocate-0.15-1.el5

```
Applied service updates: 1
```

SU#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
4	yes	10/03/07	no	yes	acl-2.2.39-2.1.el5.001

plis

Syntax: **plis** <*patch_handle*>|--help

Parameter	Description
<*patch_handle*>	Prints status information about the patch with <*patch_handle*>.
--help	Prints information about the **plis** command.

Description: Print detailed information about a specific patch.

Example 1: Print information for the patch with 1 handle.

```
$ plis 1
```

```
Handle: 1
Type: PATCH
Filename: p19000_1.ntl
Dependency: None
CR number: Q000000000
Engineer: John Doe
Created: Tue Sep 16 15:49:33 2008
Loaded: Tue Sep 23 12:21:59 2008
Patch is in-service In-service date: 10/03/07 01:24:08
Special Instructions: no
Applications stopped: None
Applications started: None
Requires reboot: No
PrePatch script: No
PostPatch script: No
Patch member type: JAR RPM: avaya-cs1000-vtrk-6.00.00-
00.i386.rpm
```

pload

Syntax: **pload** [--all]|<*patch_name*>.ntl|--help

Parameter	Description
--all	Loads all patches from the patch directory.
<*patch_name*>.ntl	Loads the patch called <*patch_name*> from the patch directory.
--help	Prints information about the **pload** command.

Description: The **pload** command loads a patch from a disk file and updates the on-switch database with the specific patch information.

The /var/opt/avaya/patch directory must contain the patch file to load.

The patch type includes the following:

- Patch—WAR or FRU. The format of patch name is pxxxxx_x.ntl.
- Serviceability Update (SU)—The format of SU name is <any_SU_name>.ntl.

Example 1: Use the following command to load the p20002_1.ntl patch.

```
$ pload p20002_1.ntl

Loading patch /var/opt/avaya/patch/p20002_1.ntl
Patch handle is: 1
```

Example 2: Use the following command to load all patches.

```
$ pload --all

Loading patch /var/opt/avaya/patch/p19000_1.ntl
Patch handle is: 0


Loading patch /var/opt/avaya/patch/p20002_1.ntl
Patch handle is: 1
```

pins

Syntax: **pins** <*patch_id*>|--all|--help

Parameter	Description
<*patch_id*>	Activates the patch with <*patch_id*> handle (as identified by **pload** or **pstat** commands).
--all	Activates all loaded patches.
--help	Prints information about the **pins** command.

Description: The **pins** command places a patch in service. The patch is placed into service for all processes to which it applies.

The patch must load (using the **pload** command) before the patch can be placed in service. The patch cannot be placed in service if it conflicts with another patch. The patch conflict checking includes application checking and patch element checking.

Example 1: Activate a patch with 4 handle (patch_id = 4).

```
$ pins 4

Patch handle: 4
All Avaya applications will be stopped.
Do you want to continue (Y/N) [N]? y
...
```

poos

Syntax: **poos** <*patch_id*>|--all >>|--help,-h

Parameter	Description
<*patch_id*>	Deactivates the patch with <*patch_id*> handle.
--all	Deactivates all patches.
--help or -h	Prints information about the **poos** command.

Description: Removes a patch from service. The patch is removed from service for all processes in which it was in service. A patch is always retained until the **poos** CLI command explicitly puts the patch out of service.

Note:

In some cases, you cannot remove a patch (that is, the **poos** CLI command fails).

Example 1: Deactivate all patches.

```
$ poos --all

Patch handle: 0
Performing the uninstallation:
The patch 0 has been deactivated successfully
Patch handle: 1
Performing the uninstallation:
The patch 1 has been deactivated successfully
Patch handle: 2
Performing the uninstallation:
The patch 2 has been deactivated successfully
```

pout

Syntax: **pout** <*patch_id*>|--all|--help

Parameter	Description
<*patch_id*>	Unloads the patch with <*patch_id*> handle.
--all	Unloads all out of service patches.
--help	Prints information about the **pout** command.

Description: Unloads a patch that was loaded using the **pload** command and cleans up the on-switch database of the specific patch information.

Example 1: Unload the patch with 0 handle.

```
$ pout 0

Patch 0 has been removed successfully
```

Loadware commands

The following CLI commands are available for loadware:

- lwstat on page 123
- lwload on page 124
- lwinst on page 124
- lwout on page 125

lwstat

Syntax: **lwstat**

Description: Print a list of installed loadware.

lwload

Syntax: **lwload** <*loadware file name 1*>.lw <*loadware file name 2*>.lw [all]

Parameter	Description
<*loadware file name*>.lw	Load the specified loadware file into the system database.
[all]	Load all available loadware files.

Description: Loads a loadware into the system database.

Example 1: Load a MGC loadware file into the system database.

```
> lwload MGCCAM01.lw

Loading loadware patch from "/u/loadware/MGCCAM01.LW"
Loadware patch number is 0.
```

lwinst

Syntax: **lwinst** <*loadware patch no.*> <*loadware patch no.*> [all]

Parameter	Description
<*loadware patch no.*>	Install the specified loadware patch number. Each loadware file is assigned a number when loaded into the system.
[all]	Install all available loadware files.

Description: Places a loadware in service.

Example 1: Install a MGC loadware file into service and upgrade all MGCs immediately.

```
> lwinst 0

Loadware "MGCCAH19" will be replaced by "MGCCAM01+"
Do you wish to continue (y/n)? [y] y
MGC Loadware patches have been put into service.
Do you want to upgrade all MGCs now (y/n)? [y] y
Please enter the type of upgrade (SEQ/SIM).(Q to quit) SEQ
Sequential Upgrade of all MGCs has been invoked.
```

Example 2: Install a MGC loadware file into service without upgrading all MGCs immediately.

```
> lwinst 0

Loadware "MGCCAH19" will be replaced by "MGCCAM01+"
Do you wish to continue (y/n)? [y] y
MGC Loadware patches have been put into service.
```

```
Do you want to upgrade all MGCs now (y/n)? [y] n
Please use UPGMG commands in Ovl143 to upgrade.
```

lwout

Syntax: **lwout** <*loadware patch no.*> <*loadware patch no.*> [all]

Parameter	Description
<*loadware patch no.*>	Unload the specified loadware patch number. Each loadware file is assigned a number when loaded into the system.
[all]	Unload all available loadware files.

Description: Unloads a loadware from the system database.

Target service pack commands

The following CLI commands are available for service packs:

- issp on page 125
- spstat on page 126
- spload on page 127
- spins on page 127
- spout on page 128

Note:

There is no **spoos** command because service packs cannot be deactivated. For more information about service packs, see Linux service packs on page 21.

issp

Syntax: **issp** [-h, --help]

Parameter	Description
--help or -h	Prints the information for the **issp** command.

Description: Print a list of installed RPMs, serviceability updates, and patches.

Example 1: Print a list RPMs, SUs, and patches in a service pack.

```
$ issp
```

```
START:
##################
Release: 6.00.00.00
Machine: i686
HostName: abc.domain.name.com
##################
RPMs:
pcre-devel-4.5-3.2.RHEL4
PyQt-3.13-1
qt-designer-3.3.3-9.3
kdebase-devel-3.3.1-5.8
kdesdk-3.3.1-2
tetex-afm-2.0.2-22.EL4.7
linuxdoc-tools-0.9.20-14
docbook-utils-pdf-0.6.14-4
compat-libstdc++-296-2.96-132.7.2
libdbi-0.6.5-10.RHEL4.1
gsl-1.5-2.rhel4
unixODBC-kde-2.2.11-1.RHEL4.1
cyrus-sasl-ntlm-2.1.19-5.EL4
rusers-0.17-41.40.1
compat-gcc-32-c++-3.2.3-47.3
zsh-4.2.0-3.EL.3
am-utils-6.0.9-15.RHEL4
elfutils-libelf-devel-0.97-5
tftp-0.39-1
##################
SUs:
basesystem-8.0-5.1.1.001 Start:nrsm Stop:nrsm Reboot:no
Spec:no
kernel-headers-2.6.18-53.el5.002 Start: Stop: Reboot:no
Spec:Yes
zlib-1.2.3.3.003.001 Start:dbcom,sps,ncs Stop:ncs,dbcom
,sps Reboot:yes Spec:no
mktemp-2.0-0.0.0.005.001 Start: Stop: Reboot:yes Spec y
es
##################
Patches:
p12345_1 Start:dbcom Stop:dbcom Spec:no
p22345_1 Start: Stop: Spec:no
p53233_1 Start:dbcom,sps Stop:dbcom,sps Spec:yes
##################
EOF:
```

spstat

Syntax: **`spstat`** `[-l, --list]|[-h, --help]`

Parameter	Description
--list or -l	Lists patch activity done for the currently loaded or in-service service pack.
--help or -h	Prints the information for the **`spstat`** command.

Description: Prints a status summary of all loaded and in-service service packs.

Example 1: Print a summary of installed and in-service service packs.

```
$ spstat 0

The following SP is in loaded status: cs1000e_1.ntl Loaded
by user avaya on Sat Mar 22 00:49:24 2008.
```

```
The following SP is in-service cs1000e_1.ntl Loaded by user
avaya on Sat Mar 20 01:11:33 2008.
```

spload

Syntax: **spload** <*service_pack_file_name*>.ntl|--help

Parameter	Description
<*service_pack_file_name*>.ntl	Loads a service pack called <*service_pack_file_name*> into the system. The format of service pack file name is pxxxxx_x.ntl.
--help	Prints information about the **spload** command.

Description: Loads a service pack (a set of patches and serviceability updates) into the system database. The service pack content types includes the following:

- Patches—WAR or FRU
- Serviceability Updates

If not path is specified for the <*service_pack_file_name*>, the /var/opt/avaya/patch folder must contain the service pack file. If a path is given when specifying <*service_pack_file_name*>, then the service pack file must be in the path.

Example 1: Load the service pack called p20002_1.ntl.

```
$ spload p20002_1.ntl

Loading patch /var/opt/avaya/patch/p19000_1.ntl
Patch handle is: 0
Loading patch /var/opt/avaya/patch/p20002_1.ntl
Patch handle is: 1
...
```

spins

Syntax: **spins** [--help]

Parameter	Description
--help	Prints information about the **spins** command.

Description: Places a service pack in service. Only one service pack can be placed in service at one time. The **spload** command must have ran successfully for this command to work.

Example 1: Place a service pack in service.

```
$ spins

Performing the installation:
Name : avaya-cs1000-solid
```

```
Relocations: (not relocatable)
Version : 5.25.06
Vendor: (none)
Release : 00.4.50.0090
Build Date: Fri 12 Oct 2007 05:43:58 PM MSD
Install Date: (not installed)
Build Host: zbvwh0ja.ca.avaya.com
Group : Application Software
Source RPM: avaya-cs1000-solid-5.25.06-00.4.50.0090.src
.rpm
Size : 17825125
License: Commercial
Signature : (none)
URL : www.avaya.com
Summary : change summary
Description : Solid database server boost engine
distributed with avaya CS1000 product.
Do you want to continue? (Y/N) [Y]?
Performing new RPM patch installation...
Preparing... ########################################
# [100%]
1:avaya-cs1000-solid ################################
######### [100%]
executing Solid DB post install...
Installation avaya Solid database server completed.
Installing the Solid database server package done Done.
The RPM patch installation is completed.
The patch 2 has been activated successfully.
Patch handle: 1
Performing the installation:
The patch 1 has been activated successfully.
Patch handle: 0
Performing the installation:
Warning: installing a new file. Please pay attention to
the /etc/test1 file attributes
The patch 0 has been activated successfully.
Patch handle: 3
...
```

spout

Syntax: **spout** [--help]

Parameter	Description
--help	Prints information about the **spout** command.

Description: Unloads a service pack (the set of patches and serviceability updates) from the system database. The **spload** command must have ran successfully for this command to work. The **spins** command cannot have been run on this service pack.

Example 1: Unload the service pack.

```
$ spout

Patch 0 has been removed successfully
Patch 1 has been removed successfully
Patch 2 has been removed successfully
Patch 3 has been removed successfully
...
```

Call Server target commands

The following CLI commands are available for Call Server targets:

- mdp issp on page 129
- mdp install on page 129
- mdp refresh on page 129
- mdp uninstall on page 130

For media cards, issue these commands from PDT.

For a complete list of MDP commands and descriptions, see LD 143 in *Software Input Output Reference — Maintenance, NN43001-711*.

mdp issp

Syntax: **`mdp issp`**

Description: Prints all inservice MDP patches and patch handle numbers (includes all Deplist patches).

mdp install

Syntax: **`mdp install`** *`<path>/<file>`*

Parameter	Description
<path>	The location of the patch file.
<file>	The name of the patch file to install.

Description: Install the contents of a MDP patch file on a target system.

mdp refresh

Syntax: **`mdp refresh`** *`<path>/<file>`*

Parameter	Description
<path>	The location of the patch file.
<file>	The name of the patch file to refresh.

Description: Refreshes the MDP patches on a target system.

mdp uninstall

Syntax: **`mdp uninstall`**

Description: Removes contents of a previously installed MDP patch distribution from the system. First it deactivates, then removes, all patches from the system.

Chapter 9: Patch maintenance

You must perform regular maintenance to remove patches, serviceability updates, loadware, deplists, and service packs to avoid excessive storage consumption. Another reason to clean up unused patches, serviceability updates, loadware, deplists, and service packs is that they are included when the element is backed up and this can result increased backup times and storage consumption.

When service packs are applied using Patching Manager or CLI, they are not automatically deleted. If application of a service pack results in automatic removal of patches or serviceability updates, these are also not deleted. Deactivation of patches or serviceability updates using Patching Manager results in complete removal of these items.

Use the Local Patching Manager on an element to identify and remove any patches or serviceability updates that are not in service. The Local Patching Manager can also be used to remove service packs.

Note:

After a service pack is applied, you can remove the service pack without affecting the patches and serviceability updates that were installed as part of the service pack.

Clean up must be done on the UCM and all target elements being patched. The **sysBackup** command backs up all patches, serviceability updates, loadware, deplists, and service packs that accumulate on the target elements making the backup files very large and slow to backup.

For more information about deleting service packs, patches, loadware, deplists and serviceability updates, see the following:

- Central Patching Manager
  - Delete a service pack or deplist from the central patch library on page 48
  - Delete a patch from the central patch library on page 51
  - Delete loadware from the central patch library on page 54
- Local Patching Manager
  - Delete a service pack on page 103
  - Delete a patch on page 115

Chapter 10: MAS QFE patches

The following sections contain information about installing and removing MAS Quick Fix Engineering (QFE) patches:

Install a new MAS QFE patch

Install a new QFE patch to apply a change to the system.

Note:

Applying a QFE patch can affect the service of your system.

Important:

You must apply QFE patches in sequential numerical order because new patches are dependent on previously installed QFE patches.

Prerequisites:

- You must lock the system with a pending lock and wait for all active sessions to terminate before you install a QFE patch.

Installing a new QFE patch:

1. Navigate to **System Status** > **Monitoring** > **Active Sessions**. When all sessions terminate or an acceptable amount of time has passed, lock the MAS.
2. Navigate to **System Status** > **Element Status** > **More Actions** > **Lock**. Click **Confirm**.
3. Use the admin2 account to log on to a command prompt window.
4. Upload the QFE patch file to the Linux server and save it in any folder (for example, in /tmp).

   Note:

   Secure File Transfer Protocol (SFTP) and Secure Copy (SCP) are the supported methods of patch file transfer.
5. Enter the command **`maspatch apply <path_to_qfe>`**.
6. In the navigation pane, select **Tools** > **Software Inventory**.
7. Verify the patch version shown in the **Patch Level** column is correct.

8. In the navigation pane, select **System Status** > **Element Status**.
9. In the **More Actions** list, select **Unlock** to unlock the MAS. If someone has already unlocked the MAS, the **Unlock** option appears dimmed.
10. Verify the patch installation; navigate to **System Status** > **Element Status** and verify that the node is started. Place calls to your applications to validate that they work.

Remove a MAS QFE patch

Remove a Quick Fix Engineering (QFE) patch to uninstall it from the system.

Note:

If you remove a QFE patch it can affect the service of the system.

Important:

Remove QFE patches in reverse sequential numerical order.

Prerequisites:

- You must lock the system with a pending lock and wait for all active sessions to terminate before you remove a QFE patch.

Procedure:

1. Navigate to **System Status** > **Monitoring** > **Active Sessions**. When all sessions terminate or an acceptable amount of time has passed, lock the MAS.
2. Navigate to **System Status** > **Element Status** > **More Actions** > **Lock**. Click **Confirm**.
3. Use the admin2 account to log on to a command prompt window.
4. Enter the command **`maspatch list all`**; a list of of applied patches appears.

   Note:

   The name of the file is not necessarily the same as the name of the patch name.
5. Find the name of the patch in the **QFE Name** column.
6. Enter the command **`maspatch remove <patchname>`** to remove the patch.
7. In the navigation pane, select **Tools** > **Software Inventory**.
8. Verify the patch version shown in the **Patch Level** column is correct.
9. In the navigation pane, select **System Status** > **Element Status**.
10. In the **More Actions** list, select **Unlock** to unlock the MAS. If someone has already unlocked the MAS, the **Unlock** option appears dimmed.