



Software Update Manager User Guide

October 2011

© 2011 Avaya Inc.

All Rights Reserved.

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.

For full support, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03–600758.

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 Web sites 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 Web site: <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.

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.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

Trademarks

Avaya is a registered trademark of Avaya Inc.

Adobe® Flash® Player. Copyright © 1996 - 2009. Adobe Systems Incorporated. All Rights Reserved. Patents pending in the United States and other countries. Adobe and Flash are either trademarks or registered trademarks in the United States and/or other countries.

Contents

Chapter 1: About help topics	5
Opening Help to a topic of interest.....	5
Opening Help to the contents page.....	5
Chapter 2: Introduction	7
Overview.....	7
What is new in Release 6.0.....	8
Chapter 3: Getting started	11
The user interface.....	11
Toolbar.....	11
View Tabs.....	12
Dialog Area.....	12
Status Line.....	12
Using Tooltips.....	13
Starting Avaya Software Update Manager.....	13
Configuration and Settings.....	14
Defining Web site download parameters.....	14
Chapter 4: Application workflows	19
Viewing Tabs.....	19
The Targets Table.....	19
Targets Table views.....	19
Managing Targets Tables.....	21
Saving the Targets Table.....	26
Printing the Targets Table.....	27
Detecting targets.....	27
Starting the Detection Process.....	27
Detecting All Targets.....	28
Detecting New Targets.....	28
Updating Information for Selected Targets (Refresh).....	29
Detecting Targets Using Filters.....	30
Using Wildcards and Ranges in an IP Address.....	31
Filtering the Targets table.....	31
Filtering the Targets Table.....	31
Filtering the Targets Table - CM Branch, Gateways, Data Switches, and Circuit Packs view.....	32
Filter Criteria - CM Branch, Gateways, Data Switches, and Circuit Packs view.....	33
Filtering the Targets Table - IP Phones View.....	34
Filter Criteria - IP Phones view.....	36
Filtering the Targets Table - Communication Manager Software Management View.....	36
Filter Criteria - Communication Manager Software Management View.....	38
Filtering by Device Type.....	39
Analyzing and retrieving files from the web.....	39
Performing Web Analysis.....	39
Retrieving New Versions from the Web.....	40
Manually Adding files.....	42
Configuring Product Defaults.....	43

Setting Product Defaults.....	43
Managing Software Libraries.....	44
Configuring Software Libraries.....	44
Defining a Remote Software Library.....	45
Software Libraries Parameters.....	45
Viewing files available to download.....	46
Adding, Editing, or Deleting a file.....	47
Configuring the media server software repository.....	49
Performing Upgrade or Update.....	56
Configuring download parameters.....	56
Performing Downloads.....	58
Scheduling Downloads.....	68
Resetting Modules.....	72
Managing IP phone software.....	73
Managing IP Phone software.....	73
The IP Phones Interface.....	74
Downloading software.....	74
Importing Files to the Local Software Library.....	77
The Log File.....	79
The Log File.....	79
Viewing the Log.....	79
Saving the Log.....	80
Clearing the Log.....	81
Closing the Log.....	81
Chapter 5: ASCA Reporting Tool.....	83
Avaya Software Compatibility Audit Report Overview.....	83
Running the Inventory Script on the Communication Manager.....	83
Downloading the inventory file to your computer.....	84
Generating and Using an ASCA Report.....	84
Using the ASCA Report Filter.....	86
Upgrading the gateway using the LSP/TFTP server.....	86
Index.....	91


Chapter 1: About help topics

Opening Help to a topic of interest

About this task

To open Help directly to a topic of interest:

Procedure

1.
 - Select **Help > > Help ON**.
The cursor changes to the shape of an arrow with a question mark.
 - Click the  icon.
 2. In the Software Update Manager, click a point of interest.
Help opens to the topic explaining the clicked feature.
-

Opening Help to the contents page

Procedure

- Select **Help > Contents**.
The system displays the contents page.
-

Chapter 2: Introduction

Overview

The Software Update Manager is an application that downloads software to managed Avaya devices. Software Update Manager can also check the software versions currently in use against the latest versions available from Avaya and recommend updates when a newer version is available. In this guide, the word target is used to define any device to which a software can be downloaded.

Software Update Manager can download a new release from Avaya's Web site and store it on your hard disk for subsequent downloading to the appropriate devices.

Software Update Manager includes a server hosted on the workstation running Avaya Network Manager in the Standalone mode. The server stores all the software retrieved from the web and downloads the software to appropriate devices. Files containing embedded software are copied to the server.

You can access the server locally or from remote. This allows you to update the software on your devices from any location.

The Software Update Manager is used to retrieve software from the Web and download it to appropriate devices in your network. You can perform the following tasks using Software Update Manager:

- Starting SUM: For instructions on starting SUM, refer to [Starting Software Update Manager](#) on page 13.
- Detecting the download targets associated with devices in the network: For instructions on detecting targets, refer to [Detecting Targets](#) on page 27.
- Analyzing the software on the network devices to determine if there are new versions: For instructions on analyzing device software, refer to [Performing Web Analysis](#) on page 39.
- Retrieving new versions of software from the Web: For instructions on retrieving software from the web, refer to [Retrieving New Versions from the Web](#) on page 40.

- Downloading the new software to the relevant devices in your network: For instructions on downloading software to devices, refer to *Downloading*.
- Resetting devices in the network as necessary: For instructions on resetting devices, refer to [Resetting Modules](#) on page 72.

What is new in Release 6.0

Software Update Manager introduces the following enhancements for Release 6.0 Service Pack 4.

- Software Update Manager does not allow to specify an Secure Copy (SCP) account name longer than ten characters.
- You can change parameters in Software Update Manager in the File/Options menu no matter what the screen resolutions of your computer are.
- Proxy authentication for SAFE login is enabled. This ensures that you can get entitlements.



Note:

You must restart Avaya Services after you change proxy information in SUM. This is to avoid unexpected results due to caching of user credential by Java API.

Software Update Manager introduces the following enhancements for Release 6.0 Service Pack 3.

- Software Update Manager checks if you have the latest version of the End User License Agreement (EULA). If you already have the EULA, the system allows you to proceed to download from SAFE. If you do not have the latest EULA certificate, the system displays the latest version which you must accept before you proceed to download from SAFE.
- There is support for MM721 BRI Media Module BG 6.2 release.

Software Update Manager release 6.0 has the following enhancements:

- Software Update Manager does not support the upgrade to system platform. There is no upgrade from the 5.2 release to the 6.0 release. You will only be able to view content in the 6.0 release.
- Supports the 85XX Avaya Aura[®]Communication Manager platform.
- Supports the 8300D Avaya Aura[®]Communication Manager platform.
- Supports the S8800 Avaya Aura[®] Communication Manager platform.
- Supports IP Office 6.0 and ip500v2 (new IP Office device).

- Supports ASG with DES and AES encryption.
- No option to update the licence file or the authentication file. These features are disabled.

Chapter 3: Getting started

The user interface

The Software Update Manager user interface consists of the following elements:



- **Menu Bar**- Menus for accessing SUM's functions. For a list of menu items, refer to [Appendix B: Menus](#).
- [Toolbar](#) on page 11 - Toolbar buttons for accessing SUM's main functions.
- [View Tabs](#) on page 12 - Tabs for switching between the different Targets Table views.
- [Dialog Area](#) on page 12 - An area where all dialog boxes are displayed. When no dialog box is open, the **Dialog Area** disappears and the Targets Table expands to take its place.
- **Log File Area** - Log file detailing all activities performed in the Software Update Manager. For more information on the Log File area, see [The Log File](#) on page 79.
- [Status Line](#) on page 12 - The status line displays the current user name, time when the Targets Table is filtered, and the progress during discovery.







Related topics:

- [Toolbar](#) on page 11
- [View Tabs](#) on page 12
- [Dialog Area](#) on page 12
- [Status Line](#) on page 12
- [Using Tooltips](#) on page 13

Toolbar

The Toolbar provides shortcuts to the main Software Update Manager functions. The table below describes the buttons on the toolbar and gives the equivalent menu options.

Button	Description	Menu Item
	Downloads Targets Detection	Actions > Downloads Targets Detection
	Targets Detail	Actions > Targets Details

Button	Description	Menu Item
	Schedule downloads	Actions > Schedule Download
	Reset selected modules	Actions > Reset
	Perform Web analyzing	Tools > Image Analyzer
	Retrieve files from the Web	Tools > Retrieve from the Web
	Add Image File	Tools > Add Image File
	Show Software Libraries	Tools > Show Software Libraries

View Tabs

The Targets Table has the following viewing options:

- [CM Branch, Gateways, Data Switches, and Circuit Packs View](#) on page 20
- [IP Phones View](#) on page 20
- [Communication Manager Software Management View](#) on page 20

To display a specific view, click the appropriate view tab. The selected view opens. For information regarding the information provided and actions performed in the different views, refer [The Targets Table](#) on page 19.

Dialog Area

The area to the right of the Targets Table is where all dialog boxes open. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box opens, it replaces the current dialog box in the **Dialog Area**. When no dialog box is open, the **Dialog Area** disappears and the Targets Table expands to take its place.

Status Line

The Status Line displays the name of the currently logged in user. In addition, it displays and discovery progress, and shows when the Targets Table is filtered.

Using Tooltips

About this task

The Software Update Manager has a tooltips feature. Tooltips allows you to display additional information about targets and software versions. Tooltips are available in the Targets Table.

Procedure

1. To display additional information about a target, place the cursor on the target's row.

After about one second, a tooltip appears with information about the target.

S. #	Name	IP Address	Module #/Location	Device
1	PUMG350-01	135.27.162.188	6	Avaya G350
2	PUMG350-01	135.27.162.188	7	Avaya G350
3	PUMG350-01	135.27.162.188	10	Avaya G350
4	PUMG350-01	135.27.162.188	10	Avaya G350
5	PUMG350-01	135.27.162.188	10	Avaya G350
6	PUMDEV-G700-1		1	Avaya G700
7	PUMDEV-G700-1		1	Avaya G700
8	PUM-G700-02	135.27.162.188	1	Avaya G700
9	PUM-G700-02		1	Avaya G700
10	PUM-G700-02-MC		3	Avaya G700
11	PUM-G700-02-MC		4	Avaya G700
12	PUM-G700-02-MC		10	Avaya G700
13	PUM-G700-02-MC		10	Avaya G700
14	puim	Bank A	2	Juniper T230
15	puim	Bank B	3	Juniper T230
16	puim	Active Bank	vice	Juniper T230
17	135.27.162.222	Hardware Version	0	Avaya G350
18	135.27.162.222	Serial Number	2	Avaya G350
19	135.27.162.237	Last Refresh Time	4	Avaya G350
20	135.27.162.237	Download Status	7	Avaya G350
21	135.27.162.237	Update State	0	Avaya G350
22	135.27.162.237	Last Release	0	Avaya G350
23	135.27.162.237	Entitled Release	0	Avaya G350
24	PUM-I2350		1	Avaya I2350
25	PUM-I2350	135.27.165.91	1	Avaya I2350
26	PUM-I2350	135.27.165.91	1	Avaya I2350
27	PUM-I2350	135.27.165.91	2	Avaya I2350
28	PUM-I2350	135.27.165.91	3	Avaya I2350



Note:

- Tooltips are not available in the IP Phones view.
- Tooltips are disabled by default.

2. Select **View > ToolTip** to toggle the tooltips feature.

Starting Avaya Software Update Manager

About this task

To start the Software Update Manager from the Avaya Network management Console select **Tools > Avaya Software Update Manager**.

The system displays the **Software Update Manager Targets Table**.

To begin working in SUM and to be able to download software, you need to do the following from the **File > Options** dialog box:

Define a source Web site - see the [Defining Web site download parameters](#) on page 14

Define the Proxy Settings - see the [Defining server proxy settings](#) on page 15

Define the SFAP Login Parameters - see the [SFAP login parameters](#) on page 16

Define the LSP/TFTP Server - see the [LSP/TFTP server](#) on page 17 details

Configuration and Settings

Defining Web site download parameters

About this task

To enable downloading of files from the Avaya Web site, it is necessary to define the Avaya source Web site and download intervals in the **Options** dialog box. To define the Avaya Support Web site as the source Web site, follow these steps:

Procedure

1. In the Web site area, select **Avaya Support Web Site**.
2. Click **Apply**.

Related topics:

[Defining another Web site as source Web site](#) on page 14

[Defining download intervals](#) on page 15

[Defining server proxy settings](#) on page 15

[Defining SFAP login information in Software Update Manager](#) on page 16

[Gateway Upgrade using the LSP/TFTP Server](#) on page 17

Defining another Web site as source Web site

About this task

The following steps allow you to define another Web site as the source Web site:

Procedure

1. In the Web site area, select **Other**.
 2. Type the web address of the source Web site you want to use in the text box.
 3. Click **Apply**.
-

Defining download intervals

About this task

You can configure Software Update Manager to automatically retry downloading files in the event of a download failure.

Procedure

1. In the **Maximum Download Retries** field enter the maximum number of download retries you want the Software Update Manager to attempt.
(The maximum number of times you can try to download is 10.)
 2. In the **Delay Between Retries (seconds)** field enter the number of seconds delay you require between download attempts.
(The maximum time delay between download attempts is 600 seconds.)
 3. Click **Apply**.
-

Defining server proxy settings

About this task

If you use a proxy server to connect to the internet, you must first define your server proxy settings in the **Options** dialog box before you can begin downloading software from the Avaya Web site.

Procedure

1. Select the **Use Proxy** check box to enable server proxy settings in the Server Proxy Settings area.
2. In the **Host** field enter the proxy host .
3. In the **Port** field enter the proxy port number .

4. Enter the Username and Password in the respective fields (this is required in case of authenticated proxy).
 5. Do one of the following:
 - Click **Ok**.
The system applies the changes and closes the dialog box.
 - Click **Apply**. .
The system applies the changes and keeps the dialog box open.
-

Defining SFAP login information in Software Update Manager

About this task

The Avaya Web site has all the software, firmware, and security downloads for Avaya supported devices. You must first define the Software and Firmware Access Policy (SFAP) authorization information in the Software Update Manager before you can download files from the Avaya Web site.

To define SFAP login information in Software Update Manager, follow these steps:

Procedure

1. From the **File > Options**, select the **Use SFAP** check box.
2. Enter the following parameters:
 - User Name
 - Password
 - Confirm Password
3. Select the **Use BPLinkID** check box and provide BPLinkID if you are an Avaya Business partner and have this ID.
4. Click **Retrieve Sold To's**.
 - The system displays the list of Sold To's appears in the **Sold To** drop-down list.
 - A Sold To represents the location at which a device is installed. The association between device and location is taken into consideration when checking entitlements to install software onto that device. You will only be able to download software for devices associated with the selected **Sold To**
5. Select the required **Sold To** from the **Sold To's** drop-down list.
6. Click **Ok**.

The system applies the changes and closes the dialog box.

Or

Click **Apply**. The changes are applied and the dialog box remains open.

Gateway Upgrade using the LSP/TFTP Server

Procedure

Select the **Activate** check box to upgrade the Gateway using the LSP/TFTP Server.



Note:

Please refer [Appendix E Upgrade the Gateway using the LSP/TFTP Server](#) on page 86 for more details.

Chapter 4: Application workflows

Viewing Tabs

The Targets Table

This section of the online help explains how to use the Targets Table. The Targets Table lists detected download targets and displays information about them. It includes the following topics:

- [Targets Table Views](#) on page 19
- [The CM Branch, Gateways, Data Switches, and Circuit Packs Targets Table](#) on page 21
- [The IP Phones Targets Table](#) on page 23
- [The Communication Manager Software Management Targets Table](#) on page 23
- [Sorting the Targets Table](#) on page 25
- [Customizing the Targets Table](#) on page 26
- [Filtering the Targets Table](#) on page 31
- [Printing the Targets Table](#) on page 27
- [Saving the Targets Table](#) on page 26

Targets Table views

Targets Table View options

The Targets Table has the following viewing options:

- [CM Branch, Gateways, Data Switches, and Circuit Packs View](#) on page 20
- [IP Phones View](#) on page 20
- [Communication Manager Software Management View](#) on page 20

The CM Branch, Gateways, Data Switches, and Circuit Packs view

From the **CM Branch, Gateways, Data Switches, and Circuit Packs** view you can detect and download software to targets associated with CM Branch, Gateways, Data Switches, and Circuit Packs. You can also manage IP Office devices from the **CM Branch, Gateways, Data Switches, and Circuit Packs** view.

When you open the Software Update Manager for the first time, the **CM Branch, Gateways, Data Switches, and Circuit Packs Targets Table** appears with no entries. Entries appear once you detect targets from the network. The table appears with the data during the detection process. Each row of the table displays information about a target to which software can be downloaded. A separate row in the Targets Table appears for each type of software that can be downloaded to a specific device. For more information on detecting targets, refer to [Detecting Targets](#) on page 27.

You can use this view to check the software versions currently used by the listed targets against the newest releases on the Avaya Web site and on your hard disk. For more information on checking software status and downloading new software from Avaya Web site, refer to [Analyzing and Retrieving from the Web](#) on page 39.

The IP Phones View

You can manage firmware images and configuration scripts to place on the **IP Telephony** gateways for distribution to IP phones from the **IP Phones** view.

When you open the Software Update Manager for the first time, the Targets Table appears with no entries. Entries appear only after you detect targets from the network. The table is populated by the detection process. Each row of the table displays information about a device from which software can be downloaded. For more information on how to detect targets, see [Detecting Targets](#) on page 27.

For more information on managing the IP Phones software, see [Managing IP Phone Software](#) on page 73.

The Communication Manager Software Management View







From the **CM Software Management** view you can detect and download software to targets associated with the Communication Manager (also referred to as the Media Server).

When you open the Software Update Manager for the first time, the **CM Software Management Targets Table** appears with no entries. Entries appear once you detect targets from the network. The table is populated by the detection process. Each row of the table displays information about a target to which software can be downloaded. A separate row in the Targets Table appears for each type of software that can be downloaded to a specific device. For more information on detecting targets, refer to [Detecting targets](#) on page 27.

Use the **CM Software Management** view to check the software versions currently used by listed targets against the newest releases on Avaya's Web site and on your hard disk. For information on checking software status and downloading new software from the Avaya Web site, refer to [Analyzing and Retrieving from the Web](#) on page 39.

Status Icons

The Targets Table displays a status icon for each target to indicate the update status of the software currently running in the target. The table below displays the icons and explains what they indicate.

Icon	Description
	The current software version is the latest available version.
	A more recent software version is available in the software library of your Software Update Manager server.
	The Avaya Web site has a more recent software version, but it is not downloaded on your Software Update Manager server.
	This target cannot be upgraded and you cannot perform any action on this target.
	Upgrade available for target, but you do not have access to it.
	No information is available for this target.

Managing Targets Tables

The CM Branch, Gateways, Data Switches, and Circuit Packs Targets Table

The **CM Branch, Gateways, Data Switches, and Circuit Packs Targets Table** displays the following information about each target:

Field	Description
State	The update status of the software currently running in the target. For more information, refer to Status Icons on page 21.
Name	The host name of the target.
IP Address	The IP Address of the target.

Field	Description
Main IP Address	The Main IP Address of the Main Communication Manager to which the gateway is registered.
Module#/Location	The number and location of the slot that the module occupies in the target. For stackable devices, this is the module's position in the stack.
Device Type	The type of device associated with the target.
Software Type	The software entity to be downloaded to the target. Options are: <ul style="list-style-type: none"> • Image- An executable file for running the device. • Boot Loader- A low-level executable for starting up the device. • Web Management- An executable file providing web management capability to the device.
Status	Displays the date and time of the scheduled download. During a download, this column displays download process messages.
Current Version	The software version currently running on the target.
Available Version	The latest version of the software available from the Avaya Web site. This field is updated each time you run a web analysis. For more information on web analysis, refer to Analyzing and Retrieving from the Web on page 39.
Entitled Version	The latest version of software available on the Avaya Web site that you have the authority to install.
Downloading Progress	During a download, this column displays the percentage of the file which has been downloaded to the target.
File Size	During a download, this column displays the number of bytes that have been downloaded to the target.
Port Network	The port network associated with the TN Board. This applies to TN Boards only.
Serial Number	The serial number of the target.

Field	Description
Hardware Version	The device hardware version or vintage.
Last Refresh Time	The last time the row in the Targets Table was refreshed.

 **Note:**

You can select which columns to display by using the **Column Chooser**. For information on showing and hiding columns in the Targets Table, refer to [Customizing the Targets Table](#) on page 26.

The IP Phones Targets Table

The IP Phones Targets Table displays the following information about each target:

Field	Description
Name	The host name of the target.
Device Type	The type of device associated with the target.
IP Address	The IP Address of the target.
Location	The physical location of the selected gateway.
Status	The communication status between the Software Update Manager and the target during the upgrade process.
Last Refresh Time	The last time the row in the Targets Table was refreshed.
Download Progress	During a download, this column displays the percentage of the file which has been downloaded to the target.

 **Note:**

You can select which columns to display. To do this use the **Column Chooser**. For more information on how to hide and show columns in the Targets Table, see [Customizing the Targets Table](#) on page 26.

The Communication Manager Software Management Targets Table

The **CM Software Management Targets Table** displays the following information about each target:

Field	Description
State	The update status of the software currently running in the target. For more information, refer to Status Icons on page 21.
Name	The host name of the target.
Kernel Version	This is the kernel version installed on Avaya Aura [®] Communication Manager
Available Kernel Update	This is the latest Kernel service pack update currently available on the Avaya Web site.
Entitled Kernel Update	This is the Kernel service pack update that you are authorized to install.
Available SES Service Pack	This is the latest SES service pack update currently available on the Avaya Web site
Entitled SES Service Pack	This is the SES service pack update that you are authorized to install.
Main IP Address	<ul style="list-style-type: none"> • For simplex servers: The IP address of the server. • For duplex servers: The IP address shared by both servers. • For ESS or LSP servers: The primary Communication Manager server IP address for the ESS or LSP listed.
IP Address	The IP address of the target.
Server Status	<p>The status of the server displayed.</p> <ul style="list-style-type: none"> • For simplex servers the status is displayed as either active or dormant. • For duplex servers, the status is displayed as active, standby, busy out, or dormant.
Server Type	The type of server selected. The internal server name is displayed in parentheses.
Server Config	The configuration of the server (Main , ESS , or LSP).
Software Version	The software version, including details of the release and load number.
Available Service Pack	The latest service pack update currently available on the Avaya Web site.
Entitled Service Pack	The service pack update that you have the authorization to install.

Field	Description
Available Platform/Security Update	The latest platform or security update currently available on the Avaya Web site.
Entitled Platform/Security Update	The platform or security update that you have the authorization to install.
R1 on Hard Drive	The first release available to install on the Media Server.
R2 on Hard Drive	The second release available to install on the Media Server.
R3 on Hard Drive	The third release available to install on the Media Server.
CD-ROM	Software releases available to copy to the hard drive from the CD-ROM.
Status	The communication status between the Software Update Manager and the target during the upgrade process.
Last Refresh Time	The last time the row in the Targets Table was refreshed.

 **Note:**

You can select which columns to display by using the **Column Chooser**. For information on showing and hiding columns in the Targets Table, refer to [Customizing the Targets Table](#) on page 26.

Sorting the Targets Table

About this task

According to your requirements you can rearrange the information in a Targets Table. In the Targets Table you can sort by any column.

To sort a Targets Table, follow these steps:

Procedure

1. Click the column's title.
An arrow appears in the column heading.

 **Note:**

- An upward pointing arrow indicates that the Targets Table is sorted in ascending order.

- A downward pointing arrow indicates that the Targets Table is sorted in descending order.
2. To toggle between ascending or descending order, click the column title.
-

Customizing the Targets Table

About this task

The Targets Table can be customized to show and hide columns. This enables you to view only relevant columns. You can customize columns in the Targets Table at any time, without having to re-detect download targets.

To customize columns in the Targets Table:

Procedure

1. Click the view in which you want to customize the columns (either the **CM Branch, Gateways, Data Switches, and Circuit Packs** view or the **CM Software Management** view).
 2. Right-click any column in the Targets Table.
The system displays the **Column Chooser** dialog box for that view.
 3. Select the columns you want to display.
 4. Click **Ok**.
The system closes the dialog box and displays the selected columns.
-

Saving the Targets Table

About this task

To save the information in the Targets Table as a text file, follow these steps:

Procedure

1. Select **File > Save As**.
The system displays a file browser dialog box.
 2. Enter the path and filename.
 3. Click **Save**.
The information in the Targets Table is saved in the specified file.
-

Printing the Targets Table

About this task

To print the Targets Table, follow these steps:

Procedure

1. Select **File > Print**.
The system displays a standard print dialog box.
 2. Select a printer.
 3. To print the Targets Table, click **Ok**.
-

Detecting targets

Related topics:

[Starting the Detection Process](#) on page 27

[Detecting All Targets](#) on page 28

[Detecting New Targets](#) on page 28

[Updating Information for Selected Targets \(Refresh\)](#) on page 29

[Detecting Targets Using Filters](#) on page 30

[Using Wildcards and Ranges in an IP Address](#) on page 31


Starting the Detection Process

About this task

When you first open the Software Update Manager the system displays an empty Targets Tables. To populate the Targets Table, you need to detect new targets.

To start the detection process, follow these steps:

Procedure

1. Select the view in which you want to work.
2.
 - Select **Actions > Download Targets Detection**.
 - Click the  icon.

The system displays the **Download Targets Detection** dialog box.

Detecting All Targets

About this task

The Software Update Manager server regularly detects the targets from the management platform. The targets list is retrieved from the server when you detect targets using the Software Update Manager.

To detect all targets, follow these steps:

Procedure

1. From the **Download Targets Detection** dialog box, select **Detect all the devices in the network map**.

2.
 - Click **OK**.

Targets associated with all managed devices in the selected view are detected and added to the Targets Table, and the **Download Targets Detection** dialog box closes.

- Click **Apply**.

Targets associated with all managed devices in the selected view are detected and added to the Targets Table, and the **Download Targets Detection** dialog box remains open.

Detecting New Targets

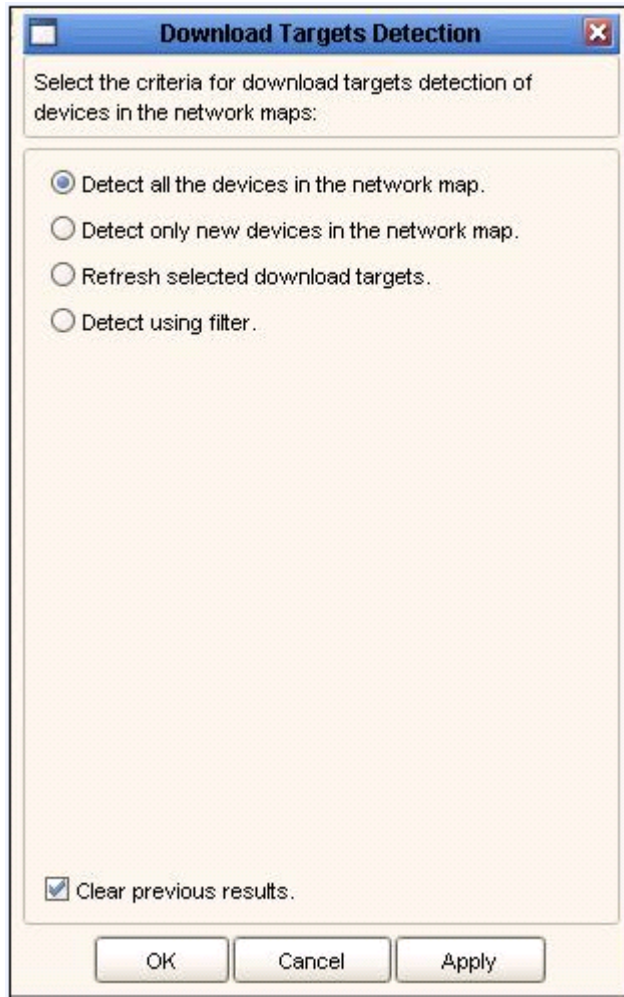
About this task

The Software Update Manager enables you to detect targets associated with new devices. This ensures that if devices were added to the **Network Management Console** either while you were working or since the last detection was performed, the targets associated with the new devices are added to the Targets Table.

To detect targets associated with new devices, follow these steps:

Procedure

1. From the **Download Targets Detection** dialog box, select **Detect only new devices in the network map**.



2. • Click **OK**.

Targets associated with new devices are detected and added to the Targets Table, and the **Download Targets Detection** dialog box closes.

- Click **Apply**.

Targets associated with new devices are detected and added to the Targets Table, and the **Download Targets Detection** dialog box remains open.

Updating Information for Selected Targets (Refresh)

About this task

You can update or refresh information of targets in the Targets Table.

Procedure

1. In the Targets Table, select the targets to update.
2. From the Download Targets Detection dialog box, select **Refresh selected download targets**.
3. In the Download Targets Detection dialog box, do one of the following:
 - Click **OK**.

The selected targets are detected and updated. The Download Targets Detection dialog box closes.
 - Click **Apply**.

The selected targets are detected and updated. The Download Targets Detection dialog box stays open.

Detecting Targets Using Filters

About this task

You can use filters to detect targets. You can filter targets based on:

- Product Type
- IP Address
- Both Product Type and IP Address

To detect targets using filters, follow these steps:

Procedure

1. From the **Download Targets Detection** dialog box, select **Detect using filter**. In the **Download Targets Detection** dialog box, the system displays the **IP Address Filter** section and the **Product Filter** section.
2.
 - To filter by IP address, in the **IP Address Filter** section, enter the IP address of the target you want to detect.



Tip:

You can use the asterisk (*) wildcard or enter a range of values to define a group of targets. For details, refer to [Using Wildcards and Ranges in an IP Address](#) on page 31.

- To filter by product type, in the **Product Filter** section, select the types of products you want to detect.
3.
 - Click **OK**.

The targets that meet the filter criteria are added to the Targets Table, and the **Download Targets Detection** dialog box closes.

- Click **Apply**.

The targets that meet the filter criteria are added to the Targets Table, and the **Download Targets Detection** dialog box remains open.

Using Wildcards and Ranges in an IP Address

You can use an asterisk (*) wildcard in the IP address. The asterisk must replace an entire octet, rather than individual digits. For example, 149.49.50.* and 149.49.*.* are valid entries. However, 149.49.40.1* and 149.49.* are not valid entries.

You can use a range to represent the last octet. For example, 149.49.48.101-110 is a valid range. However, 149.49.48.101-9 and 149.49.35-40.101 are not valid ranges. The IP address must be written without any spaces.

Filtering the Targets table

Filtering the Targets Table

To reduce the number of targets displayed in the selected view, filter the Targets Table. You can run the filter again and to add these targets — without having to detect the targets again.

 **Note:**

The **Filter devices** dialog box is only available for the **CM Branch, Gateways, Data Switches, and Circuit Packs** view and the **CM Software Management** view.

Filtering the Targets Table - CM Branch, Gateways, Data Switches, and Circuit Packs view

About this task

For more information on filter criteria, see [Filter Criteria - CM Branch, Gateways, Data Switches, and Circuit Packs View](#) on page 33.

For more information about filtering by device type, see [Filtering by Device Type](#) on page 39.

To filter the Targets Table from the **CM Branch, Gateways, Data Switches, and Circuit Packs** view, follow these steps:

Procedure

1. Select the **CM Branch, Gateways, Data Switches, and Circuit Packs** tab.
2. Select **View > Filter**.
The system displays the **Filter Devices** dialog box.
3. Select the criteria for the targets you want to display.



Note:

The Targets Table only displays targets that meet all the selected criteria.

For more information on filter criteria, see [Filter Criteria - CM Branch, Gateways, Data Switches, and Circuit Packs View](#) on page 33.

4.
 - Click **OK**.
The filtering criteria is activated and the **Filter Devices** dialog box closes.
 - Click **Apply**.
The filtering criteria is activated and the **Filter Devices** dialog box stays open.

Deactivating filtering

Procedure

1. Click **Clear**.
All filtering criteria are cleared.
2. Click **Ok**.
Filtering is deactivated and the dialog box closes.

**Note:**

When filtering is active, the  icon is displayed in the Status Line.

Filter Criteria - CM Branch, Gateways, Data Switches, and Circuit Packs view

The following table displays the list of fields you can use to filter the information displayed in the Targets Table from the **CM Branch, Gateways, Data Switches, and Circuit Packs** view. You can filter by any combination of these fields.

Field	Description
Device Name	In the Enter matching pattern field, enter the name of the target you want to display. The name can contain only one wildcard (*).
IP Address	In the Enter matching pattern field, enter the IP address of the target you want to display. The IP address can contain a wildcard (*), or a range (0-255), or a number in the range (0-255).
Main IP Address	In the Enter matching pattern field, enter the main IP address of the target you want to display. The IP address can contain a wildcard (*), or a range (0-255), or a number in the range (0-255). (Only available in the CM Software Management view.)
Avaya Aura [®] Communication Manager	In the Select Avaya Aura[®] Communication Manager field, select the communication manager used for the targets you want to display. (Only available in the CM Branch, Gateways, Data Switches, and Circuit Packs view.)
Device Type	In the Device Type section, select the product categories and sub-categories you want to display. For more information on filtering by device type, refer to Filtering by Device Type on page 39.
Software Version	In the Sw version section, select the software version used for the target you want to display.

Field	Description
Hardware Version	In the Hw version section, select the hardware version currently running the target you want to display. (Only available in the CM Branch, Gateways, Data Switches, and Circuit Packs view.)
Port Network	In the Port Network section, select the port network number for the TN boards you want to display. (Only available in the CM Branch, Gateways, Data Switches, and Circuit Packs view.)
Software Type	In the Software Type section, select the software entity (Boot Loader, Image, or Web Management) to display targets using that type of software. (Only available in the CM Branch, Gateways, Data Switches, and Circuit Packs view.)
Server Status	In the Server Status section, select the status of the server that you want to display. (Only available in the CM Software Management view.)
Analyzer State	In the Analyzer State section, select the icon or icons representing the version update status of targets you want to display.

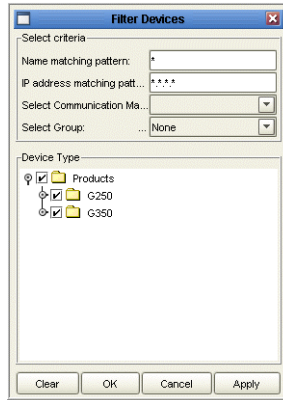
Filtering the Targets Table - IP Phones View

About this task

To filter the Targets Table from the **IP Phones** view, follow these steps:

Procedure

1. Select the **IP Phones** tab.
2. Select **View > Filter**.
The system displays the **Filter Devices** dialog box for the **IP Phones** view



3. Select the criteria for the targets you want to display.



Note:

The Targets Table only displays targets that meet all the selected criteria.

For more information on filter criteria, refer to the [Filter Criteria CM Branch, Gateways, Data Switches, and Circuit Packs view](#) on page 33.

4. Click **OK**.

- Click **OK**.

The filtering criteria is activated and the **Filter Devices** dialog box closes.

- Click **Apply**.

The filtering criteria is activated and the **Filter Devices** dialog box stays open.

Deactivating filtering

Procedure

1. Click **Clear**.
All filtering criteria are cleared.
2. Click **Ok**.
Filtering is deactivated and the dialog box closes.



Note:

When filtering is active, the  icon is displayed in the Status Line.

Filter Criteria - IP Phones view

The following table displays the list of fields you can use to filter the information displayed in the Targets Table. You can filter by any combination of these fields:

Field	Description
Device Name	In the Name matching pattern field, enter the name of the target you want to display. The name can contain only one wildcard (*).
IP Address	In the IP address matching pattern field, enter the IP address of the target you want to display. The IP address can contain a wildcard (*) or a range (0-255) or a number in the range (0-255).
Communication Manager	In the Select Communication Manager field, select the communication manager used for the targets you want to display.
Select Group	In the Select Group field, select the PIM group to filter. This enables filtering devices by device groups defined in the Avaya Provisioning and installation Manager.
Device Type	In the Device Type section, select the product categories and sub-categories you want to display. For more information on filtering by device type, refer Filtering by Device Type on page 39.

Filtering the Targets Table - Communication Manager Software Management View

About this task

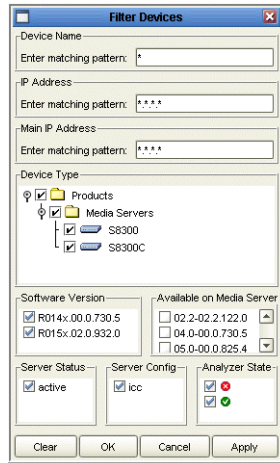
For more information on filter criteria, see [Filter Criteria - CM Branch, Gateways, Data Switches and Circuit Packs View](#) on page 33.

For more information on filtering by device type, see [Filtering by Device Type](#) on page 39.

To filter the Targets Table from the **CM Software Management** view, follow these steps:

Procedure

1. Select the **CM Software Management** tab.
2. Select **View > Filter**.
The system displays the **Filter Devices** dialog box for the **CM Software Management** view.



3. Select the criteria for the targets you want to display.

**Note:**

The Targets Table only displays targets that meet all the selected criteria.

For more information on filter criteria, see [Filter Criteria - CMBE, Gateways, Data Switches, and Circuit Packs](#) on page 33.

4.
 - Click **OK**.
The filtering criteria is activated and the **Filter Devices** dialog box closes.
 - Click **Apply**.
The filtering criteria is activated and the **Filter Devices** dialog box stays open.

Deactivating filtering

Procedure

1. Click **Clear**.
All filtering criteria are cleared.
2. Click **Ok**.
Filtering is deactivated and the dialog box closes.

**Note:**

When filtering is active, the  icon is displayed in the Status Line.

Filter Criteria - Communication Manager Software Management View

The following table displays the list of fields you can use to filter the information displayed in the Targets Table. You can filter by any combination of these fields:

Field	Description
Device Name	In the Enter matching pattern field, enter the name of the target you want to display. The name can contain only one wildcard (*).
IP Address	In the Enter matching pattern field, enter the IP address of the target you want to display. The IP address can contain a wildcard (*), or a range (0-255), or a number in the range (0-255).
Main IP Address	<ul style="list-style-type: none"> • For simplex servers - the Main IP Address represents the address of the server. • For duplex servers - the Main IP Address represents the shared IP address that represents both servers. • For ESSs and LSPs - the Main IP Address represents the IP address of the Communication Manager that the ESS or LSP is backing up. <p>In the Enter matching pattern field, enter the main IP address of the target you want to display. The IP address can contain a wildcard (*), or a range (0-255), or a number in the range (0-255).</p>
Device Type	In the Device Type section, select the product categories and sub-categories you want to display. For more information on filtering by device type, refer to Filtering by Device Type on page 39.
Software Version	In the Sw version section, select the software version used for the target you want to display.
Available on Media Server	In the Available on Media Server section, select the release that you want to display from the list of releases available for installation on the Media Server hard drive or CD-ROM drive.

Field	Description
Server Status	In the Server Status section, select the status of the server that you want to display. Options are active, standby, busy out or dormant.
Server Configuration	In the Server Config section, select the type or types of server that you want to display. Options are main, LSP, ESS or ICC.
Analyzer State	In the Analyzer State section, select the icon or icons representing the version update status of targets you want to display.

Filtering by Device Type

When filtering by device type, you can select families of devices and specific module types. Under each device family name, one or more module types are listed.

To display module types, select the device family or click its name.

When you select a device family, all the module types are automatically selected. You can then clear any module types that you do not want to select.

Analyzing and retrieving files from the web

Related topics:

[Performing Web Analysis](#) on page 39

[Retrieving New Versions from the Web](#) on page 40

[Manually Adding files](#) on page 42

Performing Web Analysis


About this task

Performing web analysis to determine if newer software versions are available.

You can use the Software Update Manager to perform a web analysis of the Avaya Web site to determine if newer software versions are available.

To perform web analysis, follow these steps:

Procedure

1. Click the view you want to work in:
 - the **CM Branch, Gateways, Data Switches, and Circuit Packs** view
 - the **CM Software Management** view
2.
 - Select **Tools > Image Analyzer**.
 - Click the  icon.

The Software Update Manager analyzes the software versions available on Avaya's Web site and updates the **State** column in the Targets Table. For information on the status icons used in the Targets Table, refer to [Status Icons](#) on page 21.

Retrieving New Versions from the Web

About this task


You can use the Software Update Manager to retrieve software versions from Avaya Web site. The Software Update Manager places the retrieved version in your default directory. You can then download the versions to targets. For information on downloading software to targets, see *Downloading Software to Targets*.

Note:

You must *first* define **SFAP Login Parameters** in Software Update Manager in order to retrieve software from the Web. For more information on how to define **SFAP Login Parameters** in Software Update Manager, see *Getting Started*.

To retrieve new software versions from the web, follow these steps:

Procedure

1. Click the view you want to work in:
 - **CM Branch, Gateways, Data Switches, and Circuit Packs** view
 - **CM Software Management** view
2.
 - Select **Tools > Retrieve Image From the Web**.
 - Click the  icon.

The **Retrieve From the Web** dialog box opens.

 **Note:**

- If you have already performed a web analysis, device types for which newer software is available on the Web site (but not on your hard disk) are automatically selected. If you have not performed a web analysis, or if the Targets Table is empty, you must manually select the device types for which you want to retrieve new software. For more information on selecting device types, see [Filtering by Device Type](#) on page 39.
 - You can display information about the new software version by placing the cursor on a row in the Targets Table. For further information, refer to [Using Tooltips](#) on page 13.
3. From the **Defaults** section in the **Retrieve From the Web** dialog box, select the download default option.

4.
 - From the **Retrieve From the Web** dialog box, click **OK**.

The **Retrieve From the Web** dialog box closes.

- From the **Retrieve From the Web** dialog box, click **Apply**.

The **Retrieve From the Web** dialog box remains open.

The system displays the **Retrieve From the Web** status in the status window. The status window displays the file name and the retrieval progress.

 **Important:**

If the download fails, the Software Update Manager generates an error message.

 **Note:**

Files are downloaded to a local software library directory on the Network Management Station (NMS). The local software library is located at: `x:\Avaya_dir\mode_dir\userver\backup\library\`

- The Avaya Network Manager is installed in: `x:\Avaya_dir`
- If you are running the Avaya Network Configuration Manager in Standalone Mode, then CVS is located at: `mode_dir`

 **Warning:**

Do not modify or delete the local software library directory after downloading files.

5.
 - To abort the current file retrieval process, and to start retrieval of the next file, click **Skip**.
 - To abort the current file retrieval process, and to cancel all the files in the retrieval queue, click **Cancel**.


Manually Adding files

About this task

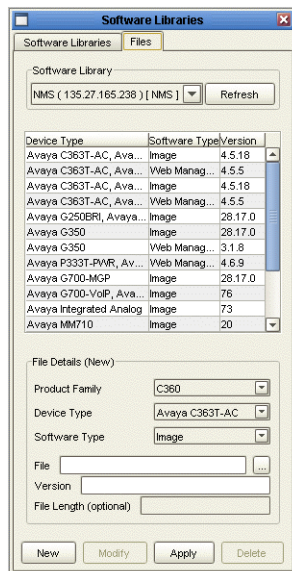
You can manually copy image files to the Software Library.


To copy a download file to the server, follow these steps:

Procedure

- Select **Tools > Add Image File**.
 - Click the  icon.

The system displays the **Software Libraries** dialog box.



2. Select the software library where the new file is located.
3. Select the product family, device type, and software type of the new file in the **Image File Name to upload** section.
4. Click  in the **File** field to browse to the location of the file and click **Open**.
5. Enter the file's version number in the **Version** field (for Remote Mode only).

Note:

If you are not running Software Update Manager in Remote Mode, the Version field is populated automatically when the image from the NMS server is selected.

6. Enter the file's size in the **File Length (optional)** field.
7.
 - Click **OK**.

The file is copied to the server, and the **Software Libraries** dialog box closes.

- Click **Apply**.

The file is copied to the server, and the **Software Libraries** dialog box remains open.



Note:

For a Remote Software Library, the file is registered at the specified location for the device and file type entered.

Configuring Product Defaults

Setting Product Defaults

About this task

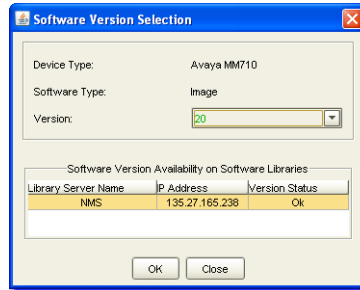
This topic explains how to view and change the default filenames for the software files that are downloaded to targets.

To view and change default filenames:

Procedure

1. Select **Tools > Product Defaults**.
2. Click the name of a product family to display a list of product types belonging to that family.
3. Select a product type.
The default filename for each relevant download file type appears in the appropriate field.
4. Click **Browse...** to look for a different default file.

The system displays the Software Version Selection dialog box, and lists the files



on the server.

5. In the Software Version Selection dialog box, click the file version you want from the **Version** field.
A green version number indicates that the software version is available in all the displayed libraries.
A red version number indicates that the software version is not available in all of the displayed libraries.
6. To close the Software Version Selection dialog box, click **OK**.
7. To save the new filename, perform one of the steps shown below:
 - To save the new filename and keep the Product Defaults dialog box open, click **Apply**.
 - To close the Product Defaults dialog box, click **OK**.

Managing Software Libraries

Configuring Software Libraries

About this task

This section explains how to configure the **Software Libraries** for downloading the files from different locations.

To configure the **Software Libraries**:

Procedure

1. Select the view in which you want to work (the **CM Branch, Gateways, Data Switches, and Circuit Packs** view or the **CM Software Management** view only).
2.
 - Select **Tools > Software Libraries**.

- Click the  icon.

The system displays the **Software Libraries** dialog box. By default, the system displays the Network Management Server (NMS) local software library.



Defining a Remote Software Library

About this task

To define a **Remote Software Library**, follow these steps:

Procedure

1. Select the **Software Libraries** tab.
2. To insert a new line in the **Software Libraries Properties Table**, click **Add**.
The system displays a new line and enables you to edit the software parameters.
3. Edit the software parameters.
For more information on software parameters, refer to [Software Libraries Parameters](#) on page 45.
4. To update the selected software library with the new parameters, click **Apply**.

Software Libraries Parameters

You can define a remote library using software parameters.

For a list of software parameters, see the table below:

Parameter	Description
Name	The name of the software library.
IP	The IP address of the Software Library .
Location	The location of the Software Library .
Description	A description of the software library .
Type	The protocol type supported by the server where the software library resides (FTP, TFTP, SCP, or any combination).
TFTP Server Secure Path	The path of the file to download on the TFTP server. This field is enabled for NMS only.
FTP User Name	The user name for the FTP server. This field is enabled for FTP only.
FTP Password	The password for the FTP server. This field is enabled for FTP only.
Retype FTP Password	Password confirmation for the FTP server. This field is enabled for FTP only.
FTP Server Path	The path of the file to download on the FTP server. This field is enabled for NMS only.
SCP User Name	The user name for the SCP server. This can be a local or domain user name. This field is enabled for SCP only.
SCP Password	The password for the SCP server. This field is enabled for the SCP only.
Retype SCP Password	Password confirmation for the SCP server. This field is enabled for the SCP only.
SCP Server Path	The path of the file to download on the SCP server. This field is enabled for the NMS only.

Viewing files available to download

About this task

You can view files available to download in the Software Libraries dialog box's **Files** tab.

Procedure

1. From the Software Libraries dialog box, select the **Files** tab.
2. Select the software library, whose files you want to view, from the **Software Library** drop-down list.
The system displays the files of the selected **Software Library** in the table.

Adding, Editing, or Deleting a file

Related topics:

[Adding or Editing a file](#) on page 47

[Modifying file details](#) on page 48

[Deleting a file](#) on page 49

Adding or Editing a file

About this task

To add or edit a file in the **Software Library**:

Procedure

1. Click the **Files** tab (from the **Software Libraries** dialog box).
2. Select the required NMS Software Library from the **Software Library** drop-down list.
The system displays the files available in the selected library in a table. It displays the File Details Parameters below the table in the read-only format.
3. Click **New File** to add or edit the File Details Parameters.
The system displays the File Details Parameters in read-write format.
4. Select the relevant Product Family for the file from the **Product Family** drop-down list.
5. Select the relevant Device Type for the file from the **Device Type** drop-down list.
6. Select the relevant Software Type for the file from the **Software Type** drop-down list.
7. Click  to select the file you want to add.
The system displays the **Open** dialog box.
8. Select the file you want to add and click **Open**.
The system displays the file path in the **File** field.

9. Enter the version of the file in the **Version** field.
10. Specify the length of the file in the **File Length** field.
(This parameter is optional.)
11. Add the required notes in the **Notes** field.
12. Click **Add File** to add the selected file to the Software Library.
The system displays the progress of the file download in the Progress Information bar.

Result

You can add file details to a **Remote Software Library**. Software Update Manager cannot add or delete files in remote libraries.

Modifying file details

About this task

To modify file details in the **Software Library**:

Procedure

1. From the **Software Libraries** dialog box, select the **Files** tab.
 2. From the **Software Library** drop-down list, select the software library.
The system displays the files available in a selected library in a table. It displays the **File Details** parameters below the table in the read-only format.
 3. Select the file entry to modify, and click **Modify** to enter file details.
The system displays the **File Details** parameters in the read-write format.
 4. From the **Product Family** drop-down list, select the file's product family.
 5. From the **Device Type** drop-down list, select the file's device type.
 6. From the **Software Type** drop-down list, select the file's software type.
 7. In the **File** field, enter the full path name.
 8. In the **Version** field, enter the file version.
 9. In the **File Length** field, enter the file length.
This parameter is optional.
 10. To update file details in the **Software Library**, click **Apply**.
The **Progress Information** bar displays the file download progress.
-

Deleting a file

About this task

To delete a file from the **Software Library**, follow these steps:

Procedure

1. From the **Files** tab, select the file you want to delete from the Devices Table.
 2. Click **Delete**.
The system deletes the file from the library.
-

Configuring the media server software repository

Configuring the Media Server Software Repository

About this task


This section explains how to manage the software repository on the Media Server. From the **Media Server Details** dialog box, you can manage the updates and install the license or authentication files to the software repository on a single Media Server .

 **Note:**

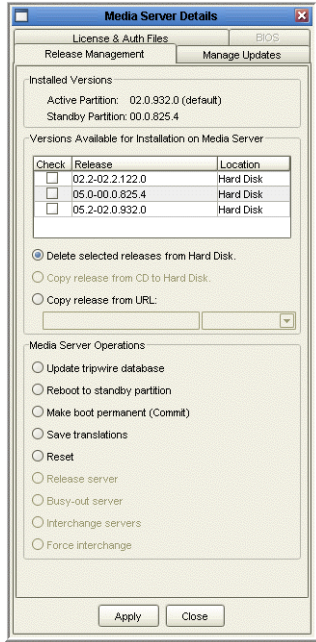
The **Media Server Details** dialog box is accessible from the **CM Software Management** tab only.

To access the **Media Server Details** dialog box, follow these steps:

Procedure

1. Select the **CM Software Management** tab from the Software Update Manager User Interface.
2.
 - Select **Actions > Target Details**.
 - Click the  icon.

The system displays the **Media Server Details** dialog box.



Media Server Release Management

The Release Management tab enables you to copy a release from an HTTP server to the hard drive. It lists the currently installed versions of the Media Server software for both the active and standby partitions. In addition, it lists up to three newer versions available for installation on the Media Server and the functions required to install or delete a release to the hard disk.

The currently installed versions of the Media Server software for both the active and standby partitions appear in the Installed Versions area of the dialog box.

Managing software releases

A table of up to three versions available for installation on the Media Server and their current location (Hard Disk, CDROM or URL) is displayed in the Versions Available for Installation on Media Server area.

To delete a software release from the table:

1. Select the check box of the version you want to delete from the Versions Available for Installation on Media Server Table.
2. Select **Delete selected releases from Hard Disk**.
3. Click **Apply**.

To copy a release from a CD-Rom to the hard disk:

1. From the Versions Available for Installation on Media Server Table, click the check box of the version you want to install.
2. Select **Copy release from CD to Hard Disk**.
3. Click **Apply**.

To copy a release from a URL to the Hard Disk:

1. Select the check box of the version you want to install, from the Versions Available for Installation on Media Server Table.
2. Select **Copy release from URL**.
3. Specify the address of the URL in the **Copy release from URL** field.
4. Specify the software version you want from the drop-down list adjacent to the **Copy release from URL** field.
5. Click **Apply**.

Performing media server operations

The Media Server Operations area of the Release Management Tab enables you to perform a number of functions on the Media Server.

To perform one of the Media Server Operations:

1. Click the operation that you want to perform from those listed in the Media Server Operations area.

The following options are available:

- **Update tripwire database**- Clears all changes following an upgrade.
- **Reboot to standby partition**- Reboots the system to the standby partition.
- **Make boot permanent (Commit)**- Makes the active partition the boot partition.
- **Save Translation**- Saves all translations configured through SAT.
- **Reset**- Resets the Media Server.
- **Release server**- Releases a server currently in busy out service.
- **Busy-out server**- Changes the server from standby to busy out service. (Only duplex servers.)
- **Interchange servers**- Alternates between active and standby servers. (Only duplex servers.)
- **Force interchange**.

2. Click **Apply**.

Media Server Updates

The **Manage Updates** tab on the **Media Server Details** dialog box displays a table with the updates available for installation and their current status (packed, unpacked, or activated). You can install or remove a service update from the Media Server.

The table of installed updates provides the following information - **Update ID** (containing the release version and service update number), **Status**, and **Type**.



Unpacking, activating, or removing a service update Procedure

1. From the installed updates list table, select the service update.
2. From the options below the installed updates list table, click an operation.

The operations that may be performed on a selected service update depend on the status of the update. The following list describes the service update status and the operations that may be performed on a service update with the status described:

- **Packed** - The service update file is located on the media server. You may choose to **unpack** the patch or **remove** it from the `/var/home/ftp/pub` directory.
- **Unpacked** - The service update file is unpacked. You may choose to **activate** the service update or **remove** the extracted files from the `opt/updates` directory.
- **Activated**- The service update is unpacked and activated. You may choose to **deactivate** the service update. When you deactivate the service update, the status reverts to **Unpacked**.

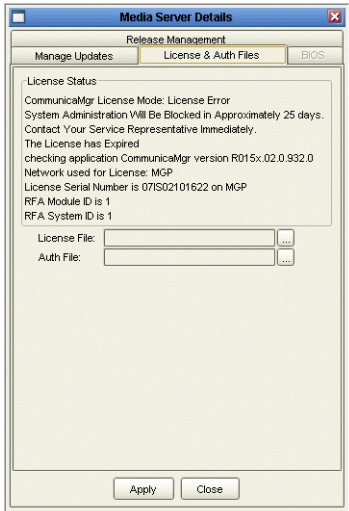
3. Click **Apply**.
4. Click **Close**.
The dialog box closes.

Installing a service update from a library Procedure


1. Select the library from the drop-down list.
The system displays a list of available service updates.
2. From the list of available service updates, select the service update to install, and from the options listed below the List of installed updates table, click **Unpack**.
3. Click **Apply**.
The service update is copied and unpacked. Its status appears as **Unpacked**.
4. To activate the service update, select **Activate**.
5. Click **Apply**.
The status changes to **Activated**.
6. Click **Close**.
The system closes the dialog box.

Media Server License and Authorization Files


The **License & Auth Files** tab on the **Media Server Details** dialog box displays the Media Server's license status information. The **License & Auth Files** tab also lets you install a license file and an authorization file.



Installing a license file Procedure

1. From the **License & Auth Files** tab on the **Media Server Details** dialog box, go to the **License File** field and click the  icon next to it. The system displays the **Open** dialog box.
2. From the **Open** dialog box, select the license file to install and click **Open**. The system displays the path of the selected file in the **License File** field.
3. Click **Apply**.
4. Click **Close** to close the dialog box.

Installing an authorization file Procedure

1. From the **License & Auth Files** tab on the **Media Server Details** dialog box, go to the **Auth File** field and click the  icon next to it. The system displays the **Open** dialog box.
 2. From the **Open** dialog box, select the authorization file to install and click **Open**. The system displays the path of the selected file in the **Auth File** field.
 3. Click **Apply**.
 4. Click **Close** to close the dialog box.
-

Performing Upgrade or Update

Configuring download parameters

Configuring Download Parameters

About this task

This section explains how to view and configure the download parameters from the **CM Branch, Gateways, Data Switches, and Circuit Packs** view or the **CM Software Management** view.


To configure the download parameters, follow these steps:

Procedure

1. Select the view for which you want to configure the download parameters (the **CM Branch, Gateways, Data Switches, and Circuit Packs** view or the **CM Software Management** view).
2. In the Targets Table, select the target or targets you want to configure.

 **Note:**

When you open Software Update Manager for the first time, the system displays the Targets Table with no entries. To populate the Targets Table with data, see [The Targets Table](#) on page 19.

3.
 - Select **Actions > Target Details**.
 - Click the  icon.

The system displays the **Target Details** dialog box. If you selected multiple targets, only the fields which are the same for all the selected targets appear with data. All other fields appear empty.

4. Specify the download parameters.
(For more information on download parameters, refer to [Download Parameters](#) on page 57.)

The screenshot shows a 'Target Details' dialog box with the following fields and values:

- Name: 135.27.162.237
- IP Address: 135.27.162.237
- Module #/Location: 4
- Device Type: Avaya MM712
- Software Type: Image
- Port Network: (empty)
- Hardware Version: 5
- Software Library: NMS (135.27.162.238) [NMS]
- File on USB Flash Drive: (empty)
- Software Version: (empty)
- Download Proxy: (empty)

The 'Selected List' table contains the following data:

Name	IP Address	Module #/L...	Device type	Software t...
135.27.16...	135.27.16...	4	Avaya MM...	Image

Download Parameters

The following table displays a list of download parameters:

Parameter	Description
Name	The logical name of the selected target or targets.
IP Address	The IP address of the selected target or targets.
Module #/Location	The number and location of the slot that the selected target occupies in the device or devices.
Device Type	The type of device associated with the selected target or targets.
Software Type	The type of software downloaded to the selected target or targets.
Port Network	The port network associated with the TN Board. Only applies to TN Boards.
Hardware Version	The device hardware version or vintage.
Software Library	The location from where to download the new file.
File on USB Flash Drive	The name of the USB flash drive file associated with the selected target.
Software Version	The software version of the new file.

Parameter	Description
Download Proxy	The IP address of the Communication Manager to use when downloading files to TN Boards.

**Note:**

If multiple targets are selected, only parameters whose value is the same for all selected targets are displayed.

Performing Downloads

Downloading

This topic describes how to download software to targets, and explains the download status messages that are displayed while the files are downloading. This topic includes:

- [The Download Process - CM Branch, Gateways, Data Switches, and Circuit Packs on page 21](#) [The Download Process - CM Branch, Gateways, Data Switches, and Circuit Packs on page 58](#) - Describes the download process from the CM Branch, Gateways, Data Switches, and Circuit Packs view.
- [The Download Process - Communication Manager Software Management View on page 59](#) - Describes the download process from the Communication Manager Software Management view
- [Download Process Status Messages on page 66](#) - Lists and explains the download status messages.

The Download Process - CM Branch, Gateways, Data Switches, and Circuit Packs

About this task

To start the download process for the Gateways, Data Switches, and TN Boards:


Procedure

1. Select the **CM Branch, Gateways, Data Switches, and Circuit Packs** tab.
2. In the Targets Table, select the target or targets to which you want to download.

 **Note:**

When you first open the Software Update Manager the system displays the Targets Table with no entries. For more information on how to populate the Targets Table with data, see [The Targets Table](#) on page 19.

3. To start the download process

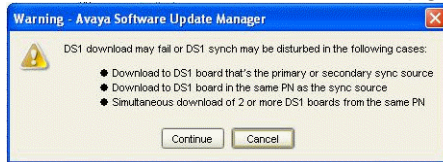
- Select **Actions > Download Now**.
- Click the  icon.

 **Warning:**

You cannot stop the download process after it starts.

Result

If your download includes a DS1 board upgrade, the system may display the following



message.

Click **Continue** to continue with the download

Or

Click **Cancel** to cancel the download.

For details of the download process in the **CM Software Management** view, refer to [The Download Process - Communication Manager Software Management View](#) on page 59.

The Download Process - Communication Manager Software Management View

About this task


The CM Software Management dialog box is used to install and upgrade the Communication Manager Server (Media Server) software, and install license or authentication files to the software repository on the Communication Manager Server. You can perform upgrades on multiple servers at the same time.

 **Note:**

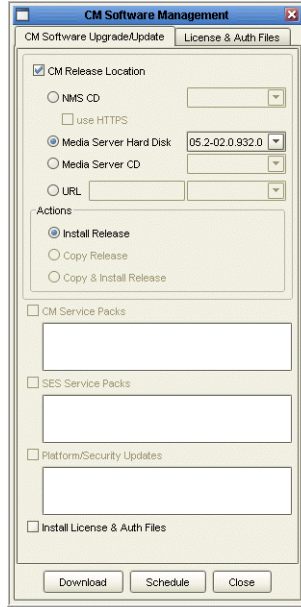
The CM Software dialog box is only accessible from the **CM Software Management** tab.

To access the CM Software Management dialog box, follow these steps:

Procedure

1. Select the CM Software Management tab.
2.
 - Select **Actions > Target Details**.
 - Click the  icon.

The system displays the CM Software Management dialog box.



Note:

In addition to TFTP and HTTP, the Software Update Manager supports HTTPS protocol for secure downloads. The HTTPS protocol is available for **NMS CD** option.

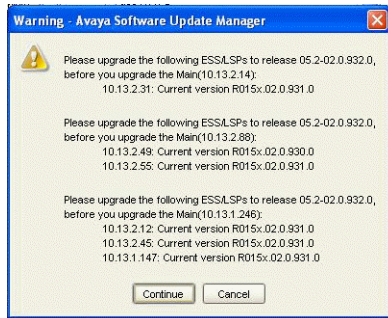
For details of the download process in the **Gateways/Data Switches** view see [The Download Process - CM Branch, Gateways, Data Switches, and Circuit Packs view](#) on page 58.

Upgrades and Updates to the Communication Manager

The **CM Software Upgrade/Update** tab enables you to copy a release from an HTTP server to the hard drive of one or more Communication Manager Servers. You can choose the source location of the release you want to download, copy and/or install a release, and install associated updates, license files, and authentication files.

The Software Update Manager ensures correct upgrade sequence for Main Communication Manager Server by verifying all dependent components of Communication Manager system are upgraded to same release version.

After this check, a warning message appears suggesting upgrades for other components in Communication Manager Server System (For e.g. ESS and LSPs).



Note:

Download the SAMP firmware from the support site prior to the Communication Manager upgrade.

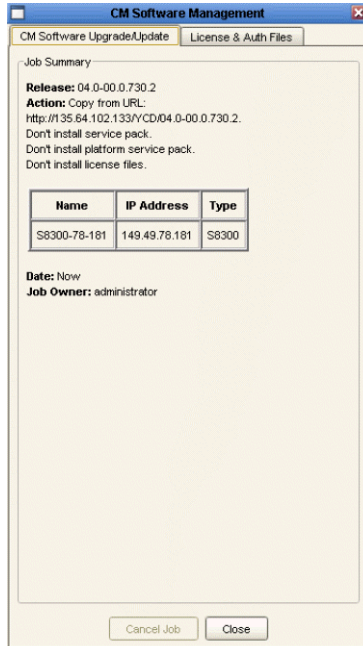
Upgrading or updating media server releases

To install a release on one or more Media Servers:

1. Click the **Communication Manager Software Upgrade/Update** tab.
2. Select one or more of the targets that you want to upgrade in the Targets Table.
3. Select the **Communication Manager Release Location** check box.
4. Click one of the following sources from which you want to download the software release:
 - NMS CD

Select **use HTTPS** check box to use HTTPS protocol to download. The check box is active only if **NMS CD** option is selected.

 - Media Server Hard Disk
 - Media Server CD
 - **URL**- specify the URL from which you want to download the software.
5. Select the software version you require from the drop-down list next to the selected media source.
6. Select one of the following actions to perform:
 - **Install Release**- installs the release to the selected Media Server(s).
 - **Copy Release**- copies the release to the selected Media Server(s).
 - **Copy & Install**- copies the release to the selected Media Server(s) and unpacks and installs it.
7. Click **Download** to begin. The system displays the Job Summary window, with the details of the download currently being performed, in the Communication Manager Software Management dialog box.



Note:

The Cancel Job button is disabled during a download. It is not possible to cancel a job after the download has started.

8. Click **Close** to close the dialog box.

Installing a Communication Manager Service Update

To install a Communication Manager service update:

1. Click the **Communication Manager Software Upgrade/Update** tab.
2. Select one or more of the targets that you want to upgrade in the Targets Table.
3. Select the **Communication Manager Service Packs** check box to display the list of Communication Manager Service Packs appears in the Communication Manager Service Packs table.
4. Select the service update you want to install.
5. Click **Download to open the Job Summary** window in the **CM Software Management** dialog box, displaying a summary of the download currently being performed.
6. Click **Close** to close the dialog box.

Installing a Kernel/Platform/Security Update

To install a platform/security update:

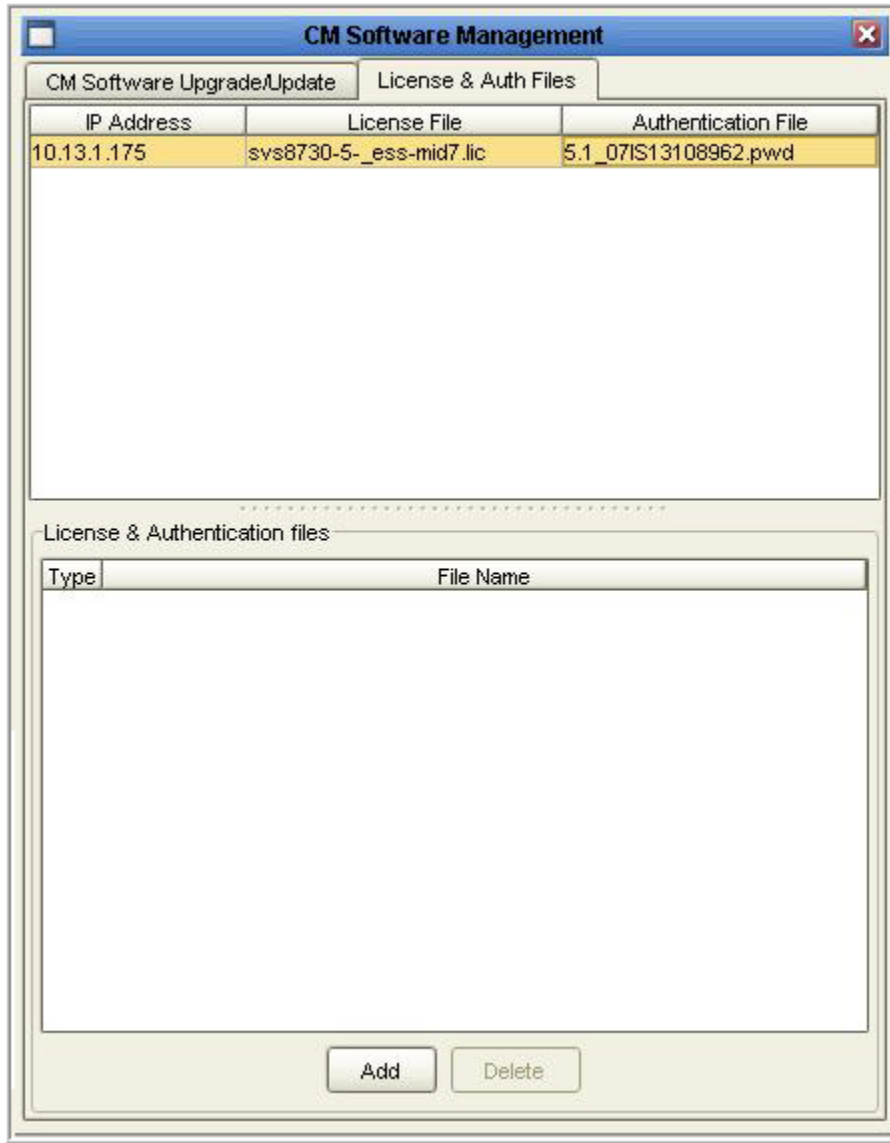
1. Click the **Communication Manager Software Upgrade/Update** tab.
2. Select one or more of the targets in the Targets Table that you want to upgrade.
3. Select the **Kernel/Platform/Security Update** check box.

4. Select the service update you want to install.
5. Click **Download**. The Job Summary window opens in the Communication Manager Software Management dialog box, displaying a summary of the download currently being performed.
6. Click **Close** to close the dialog box.

Assigning License and Authentication files

Assigning License and Authentication Files

The **License and Authentication** tab of the Communication Manager **Software Management** dialog box enables you to view, add, assign or delete license and authentication files for devices selected. The Assignment Table lists the licenses and authentication files assigned to the devices selected in the Targets Table. The License & Authentication files Table displays files available to assign.



Viewing assigned license and authentication files

About this task

To view the license and authentication files assigned to devices in the Targets Table:

Procedure

1. In the Targets Table, select the devices whose license and authentication files you want to see.
2. Click the License & Auth Files tab.
The system displays the licensing and authentication file information for the selected devices in the Devices Table (upper table).

Assigning license and authentication files to a device

About this task

The License & Authentications Files Table (lower table) lists the license and authentication files available for installation.

To assign a file from the License & Authentications Files Table to a device:

Procedure

1. Click the License & Auth Files tab.
2. Select the file that you want to assign from the License & Authentications Files Table.
3. In the Devices Table, click the row of the device to which you want to assign the file.

The system displays a drop-down list with available files.

Note:

If you click the Authentication file row when trying to assign a License file, or click the License file row when trying to assign an Authentication file, the option to assign the file is not available and the Assign tab is disabled.

4. To assign the file to the selected device, select the appropriate file from the drop-down list.
5. Click the **Install License & Auth Files** check box in the **CM Software Upgrade/Update** tab.

This ensures that the file is assigned when the software upgrade is performed.

Note:

A License or Authentication file can only be assigned once.

Adding a file to the license and authentication files table

About this task

To add a file to the **License & Authentication Files Table**:

Procedure

1. Click the License & Authentication Files tab.
2. Click **Add** to open the **Open** dialog box.
3. Select the file you want to add.
4. Click **Open**.
The system displays the selected file in the **License & Authentication Files Table**.

Deleting files from the license and authentication files table

About this task

To delete files from the **License & Authentication Files Table**, follow these steps:

Procedure

1. Click the **License & Auth Files** tab.
2. From the **License & Authentication Files Table** select the file you want to delete
3. Click **Delete**.
The system removes the selected file from the **License & Authentication Files Table**. The system also removes any assignments to devices in the Targets Table associated with the deleted file.

Download Process Status Messages

During the download process, the Software Update Manager displays the download progress for each target in the **Download Progress** and **File Size** columns of the Targets Table.

The Software Update Manager also displays the download status in the **Status** column of the Targets Table. The statuses that are displayed vary from device to device. The table below lists the different statuses, with a description of each status and the device types to which the status is applicable. For more information about the Targets Table, refer to [The Targets Table](#) on page 19. For a list of errors that can occur during download, refer to [Troubleshooting](#).

Status	Description	Devices
Ready	The target is idle and downloading can begin. Only displayed before the first download for the target after the target was added to the Targets Table, or after a delayed download was cancelled.	All
Waiting / Pending	Download process is waiting while the software is being downloaded to other targets.	All
Waiting for download on <i>(time and date)</i>	User requested download to begin later.	All
Setting Parameters	Configuration details are being sent to the agent.	All gateways and service packs
Testing	The agent is testing whether download is possible.	Only for Avaya P330 Devices

Status	Description	Devices
Erasing Flash	The agent is erasing flash memory.	Only for Avaya P330 Devices
Downloading	The software is being downloaded.	All Devices
Rebooting After Download	The device associated with the target is rebooting.	All except for Avaya P330 Devices
Data Connection Established	The software is being downloaded.	All
Download Successful	The download was completed successfully.	All
Download Failed	The download failed.	All
Download Failed with error: <i>Error description</i>	The download failed due to the listed error. For more information about error messages, refer to Troubleshooting .	All
Setting Default Flash	The version that was downloaded was made into the default version.	All
Downloading Boot Image	A Boot Image is being downloaded.	All
Downloading Image to APP1	The Image is being downloaded to Bank A of the device.	All
Downloading Image to APP2	The Image is being downloaded to Bank B of the device.	All
Synchronizing Standby Supervisor	After a successful download, the files are being copied to the backup agent, if it exists.	All

 **Note:**

You might see some different status messages depending on the selected targets.

Scheduling Downloads

Scheduling Downloads

This topic explains how to schedule a download for a later time or date.

Opening the Schedule Download dialog box

About this task

There is more than one way to open the **Schedule Download** dialog box. You can open the **Schedule Download** dialog box from the **CM Branch, Gateways, Data Switches, and Circuit Packs** view or from the Communication Manager Software Management view.

 **Note:**

The `ftp` root directory in the S8300 Communication Manager contains the latest compatible firmware for Gateways. The Software Update Manager allows the use of this local file instead of one in NMS Library. Doing so results in a faster download time and lower bandwidth. You have to configure the Target Details by using the Software Update Manager.

Opening the Schedule Download dialog box from the CM Branch, Gateways, Data Switches and Circuit Packs view

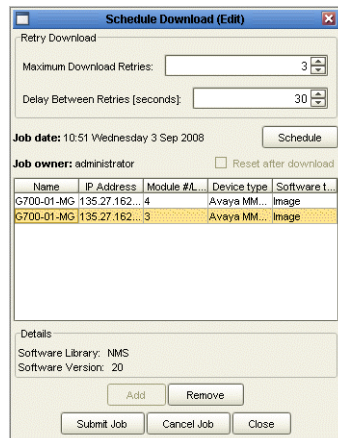
About this task

To open the **Schedule Download** dialog box from the **CM Branch, Gateways, Data Switches, and Circuit Packs** view, follow these steps:

Procedure

1. Select the **CM Branch, Gateways, Data Switches, and Circuit Packs** tab.
2. Select the target or targets to download from the Targets Table.
3. Select **Actions > Schedule Download**.

The system displays the **Schedule Download** dialog box.




Opening the Schedule Download dialog box from the Communication Manager Software Management view

About this task

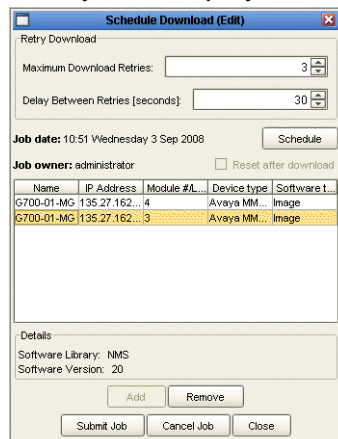
To open the **Schedule Download** dialog box from the Communication Manager Software Management view, follow these steps:

Procedure

1. Select the **CM Software Management** tab.
2.
 - Select **Actions > Schedule Download**.
 - Click the  icon.

The system displays the **CM Software Management** dialog box.

3. From the Communication Manager **Software Upgrade/Update** tab in the **CM Software Management** dialog box, click **Schedule**.
The system displays the **Schedule Download** dialog box.



Viewing Schedule Download Information

The Schedule Download dialog box enables you to view schedule information and target details for the targets you have selected. Select the target you want to view from the Schedule Download Table.

The Schedule Download dialog box displays the following information about the selected target:

Parameter	Description
Maximum Download Retries	The maximum number of times for Software Update Manager to retry downloading in the event of a download failure.
Delay Between Retries (Seconds)	The number of seconds delay between download retries, in the event of a download failure.
Job Date	The date the download is to be executed for the selected target.
Job Owner	The owner of the scheduled job.
Reset After Download	Resets the device following a successful download if this check box is selected.
Software Library	The Software Library from which the software is downloaded.
Software Version	The Software Version of the selected target.

Scheduling Software Downloads

About this task

This topic explains how to schedule a download for a later time or date.

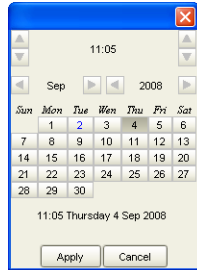
To schedule downloads, follow these steps:

Procedure

1. In the **Retry Download** area, specify the **Maximum Download Retries** and the **Delay Between Retries** in the event of a download failure.
 - a. Enter the number of times you want the system to attempt downloads in the **Maximum Download Retries** field.

- b. Enter the amount of time you want the system to wait between downloads in the **Delay Between Retries** field.
2. To automatically reset the device after a successful download, click the **Reset after download** check box.
3.
 - For immediate download, click **Download**.
 - To schedule the download for a later date and time, click **Schedule**.

The system displays the Schedule Calendar.



4. Set the time, date, and month at which you want the download to begin, as follows:
 - Use the change hour buttons to set the hour.
 - Use the change minute buttons to set the minute.
 - Use the change year buttons to set the year.
 - Use the change month buttons to set the month.
 - In the calendar section, click the day of the month to set the day.
5. Click **Apply**.

In the Targets Table, the Status column for the device set for scheduled download displays *Waiting for download on [time and date of download]* until the download begins.

Canceling a Scheduled Download

About this task

To cancel a scheduled download, from the relevant view:

Procedure

1. Select the device or devices whose scheduled download you want to cancel.
2. Select **Actions >Schedule Download**.
3. Select the targets whose scheduled download you want to cancel.
4. Click **Remove** to cancel the scheduled downloads.



Note:

This option is only available if all the devices you selected are configured for a scheduled download.

Resetting Modules

About this task

Some device modules need to be reset before the change to their software can take effect. The Software Update Manager provides the ability to reset selected modules on your network.



Warning:

Resetting an individual module in a device may cause the entire device to reset.

For example, if you reset the module that is the device's current master agent, the entire device will get reset. This may disrupt traffic on your network.

To reset modules on your network, follow these steps:

Procedure

1. Click the view you want to work in:
 - the **CM Branch, Gateways, Data Switches, and Circuit Packs** view
 - the **CM Software Management** view
2. In the Targets Table, select the targets for the modules to reset.



Note:

Each type of software for a module is represented by a row in the Targets Table. Some modules may have more than one entry in the table.

3.
 - Select **Actions > Reset**.
 - Click the  icon.

The system resets the selected modules.

Managing IP phone software

Managing IP Phone software

This section of the online help explains how to manage IP phone software distribution and IP phone configuration updates to gateway devices. IP phones receive their firmware updates and configuration scripts from the gateways through a TFTP or HTTP server selected by the DHCP server function.

Each gateway device contains a TFTP or HTTP server which stores firmware files and script files. Firmware files are stored in device RAM and phone scripts (composed of a settings script with phone configuration and an upgrade script with instructions for software upgrade) are stored in device NVRAM.

Software Update Manager enables you to download the firmware and configuration scripts for IP phones to any Avaya gateway device that the system supports. Software Update Manager does not directly update the phone firmware or phone configuration.

Avaya Software Update Manager can manage IP Phone scripts only on the following devices:

- G250 devices

 **Note:**

G250 device can store up to six firmware files and four setting script files per device.

- G350 devices

 **Note:**

G350 device can store up to six firmware files and four setting script files per device.

- G430 devices
- G450 devices
- IP Office devices

The IP Phones view includes facilities for detecting gateways, managing software images and settings scripts, and transferring configuration files to IP phones.

 **Note:**

Some H.248 Gateways do not support `96xxsettings.txt`.

This section includes the following topics:

- [The IP Phones Interface](#) on page 74
- [Downloading software](#) on page 74
- [Importing Files to the Local Software Library](#) on page 77

The IP Phones Interface

Click the **IP Phones** tab in the View Tabs section of Software Update Manager User Interface to view the IP Phones Interface.

The **IP Phones Software Libraries** interface includes the following areas:

- **Toolbar** - Toolbar buttons for accessing Avaya Software Update Manager's main functions.
- **View Tabs** - Enables you to alternate between the IP Phones view and views for managing software distribution on other devices.
- **Targets Table** - Displays information on available gateways, software images, scripts, and software libraries. For information about the Targets Table and the IP Phones view in particular, refer to [The Targets Table](#) on page 19.
- **Log File Area** - Displays error and status messages from the system. For information about the log file area, refer to [The Log File](#) on page 79.
- **Dialog Area** - An area where all dialog boxes are displayed. When no dialog box is open, the Dialog Area disappears and the Devices Table expands to take its place.
- **Status Line** - Displays the currently logged in user, filter indication and discovery progress.



Note:

Only the **Help On** option is available in the Toolbar for the IP Phones tab.

Downloading software

Downloading software

About this task

The IP Phones view enables you to download the firmware and configuration scripts for IP phones to any supported Avaya gateway device from the Software Update Manager server. The Targets Table displays a list of available gateway devices. The Files inventory for selected device dialog box provides information about the software and script files residing on each device, when accessed from the **IP Phones** view.


To view the software and script files residing on a device, follow these steps:

Procedure

1. Select the **IP Phones** tab.
2. Select the device you want to view in the Targets Table.

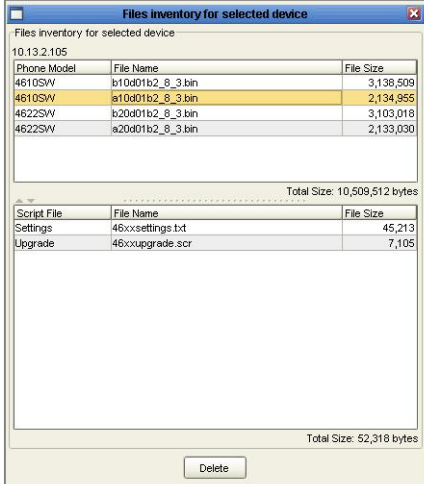
Note:

When you open the Software Update Manager for the first time, the Targets Table appears with no entries. To populate the Targets Table with data, see [The Targets Table](#) on page 19.

3.
 - Select **Actions > Target Details**.
 - Click the  icon.

The system displays the Manage IP Phones Software on the gateway dialog box.

The Phones Software Table displays an entry for each type of software residing on the selected device. The Script File Table displays a entry for each available upgrade script and configuration settings script for the selected device.



Phone Model	File Name	File Size
4610SW	b10d01b2_8_3.bin	3,138,509
4610SW	a10d01b2_8_3.bin	2,134,856
4622SW	b20d01b2_8_3.bin	3,103,018
4622SW	a20d01b2_8_3.bin	2,133,030

Total Size: 10,509,512 bytes

Script File	File Name	File Size
Settings	46cxcsettings.txt	45,213
Upgrade	46cxcupgrade.scr	7,105

Total Size: 52,318 bytes

Delete

Perform the following steps to download software to a device:


- [Downloading Software to Selected Devices](#) on page 75- Select the software from an NMS library or directory and download it to the device or devices you wish to upgrade.
- [Viewing Log Files](#) on page 77- View the file transfer logs for upload success status.

Downloading software to selected devices

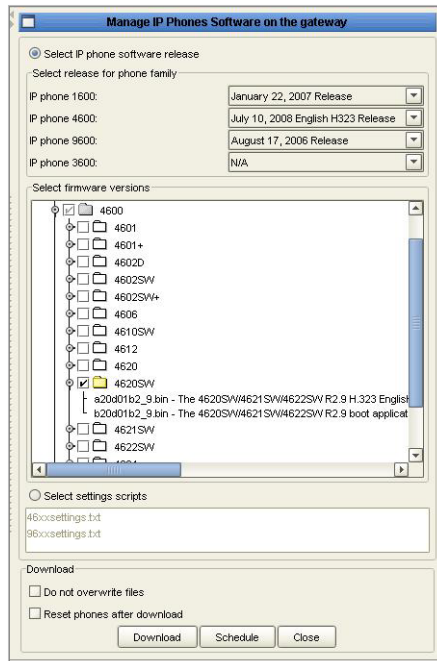
The IP phone firmware images and configuration settings scripts to be uploaded to devices can be located either in a file on the client workstation or on the Network Management Server.

Software for upload is selected from the Manage IP Phones Software on the gateway dialog box.

Accessing the Manage IP Phones Software Procedure

- Select **Actions > Download Now**.
- Click the  icon.

The **Manage IP Phones Software on the gateway** dialog box opens.



Selecting files for upload Procedure

1. From the Targets Table, select one or more devices to which you want to upload the files.
2. Click **Select IP phone software release**.
3. From the drop-down lists in the **Select release for phone family** area, select the releases for the phone families applicable to the IP Phones connected to the selected device(s).
4. Select the phone models that you wish to update.
For firmware files, select the firmware files you wish to update from the list of check boxes appearing in the **select firmware versions** area. The list only displays the

firmware versions applicable to the phone releases for the phone families selected in the **Select IP phone software release** area.

Uploading the setting scripts

Procedure

1. Select **select settings scripts**.
The system displays the list of scripts.
2. Select the required scripts from the displayed list.

Downloading selected files

Procedure

1. To keep the files that currently exist on the gateway, select **Do not overwrite files** from the **Download** area.
2. Do one of the following:
 - For immediate software download to the target gateways, click **Download**.
 - To schedule the software download to the target gateways for a later time or date, click **Schedule**. For more information on how to schedule downloads, see [Scheduling Downloads](#) on page 68.
3. To close the dialog box, click **Close**.

Viewing Log Files

You can review the results of your uploads in the Log File area. For more information on the Log Files in Software Update Manager, refer to [The Log File](#) on page 79.

 **Note:**

There is no unique log file for IP Phone software distribution functions. Upload activity appears as a normal log entry and is included in all log events. New entries appear at the top of the log file.

Importing Files to the Local Software Library

About this task

You can use the Network Management Server software library to store IP phone software and configuration files, enabling you to view files distributed to gateways and to initiate file distribution to gateways from the Software Update Manager client without storing the files on


the client workstation. Software images can be obtained directly from Avaya. For more information on how to get software images from Avaya, see [Retrieving New Versions from the Web](#) on page 40.

The **IP Phones Software Libraries** dialog box provides a tree view of available software releases and settings scripts contained in the Network Management Server software library and enables you to import them.



To Import new files into the IP Phones software library:

Procedure

1. To open the **IP Phones Software Libraries** dialog box:
 - Select **Tools > Software Libraries**.
 - Click the  icon.

The system displays the **IP Phones Software Libraries** dialog box.

2. From the **IP Phones Software Libraries** dialog box, click **Import**.
The system displays the Import window.
3. Select the file you want to import from the client workstation and click **Import**.
The selected file is imported into the IP Phones Software Library.
4. View log files to confirm the import, if desired.
For more information on how to view log files, see [Viewing Log Files](#) on page 77.

Deleting files from the IP Phones Software Library

Procedure

1. Select the file or files that you want to delete in the Server Library tree.
2. Click **Delete**.
The files are deleted from the tree.

The Log File

The Software Update Manager keeps a log of all activity. New log information is appended to the end of the existing log.

This section of the on-line help includes the following topics:

- [Viewing the Log](#) on page 79 - Describes the information contained in the log.
- [Saving the Log](#) on page 80 - Explains how to save the log.
- [Clearing the Log](#) on page 81 - Explains how to clear the log.
- [Closing the Log](#) on page 81 - Explains how to close the log.

The Log File

The Software Update Manager keeps a log of all activity. New log information is appended to the end of the existing log.

This section of the on-line help includes the following topics:

- [Viewing the Log](#) on page 79 - Describes the information contained in the log.
- [Saving the Log](#) on page 80 - Explains how to save the log.
- [Clearing the Log](#) on page 81 - Explains how to clear the log.
- [Closing the Log](#) on page 81 - Explains how to close the log.

Viewing the Log

About this task

To open the log:

Procedure

1. Select the view in which you want to work.
2. Select **View > Log Report**.
The system displays the log below the Targets Table.

You can resize the log by dragging the horizontal splitter bar. When a dialog box is open, you can also resize the log by dragging the vertical splitter bar.

Severity	Date/Time	User	Source	Message
Warning	20:56 Monday 1 Sep...	Server	135.27.162.19	Couldn't find connection parameters for SBxx server.
Warning	20:56 Monday 1 Sep...	Server	135.27.162.100	Couldn't find connection parameters for SBxx server.
Warning	20:56 Monday 1 Sep...	Server	135.27.162.185	Couldn't find connection parameters for SBxx server.
Warning	20:56 Monday 1 Sep...	Server	135.27.164.48	Couldn't find connection parameters for SBxx server.
Warning	20:56 Monday 1 Sep...	Server	135.27.164.47	Couldn't find connection parameters for SBxx server.
Warning	20:56 Monday 1 Sep...	Server	135.27.164.26	Couldn't find connection parameters for SBxx server.
Warning	20:38 Monday 1 Sep...	Server	135.27.162.19	Couldn't find connection parameters for SBxx server.
Warning	20:38 Monday 1 Sep...	Server	135.27.162.100	Couldn't find connection parameters for SBxx server.
Warning	20:38 Monday 1 Sep...	Server	135.27.162.185	Couldn't find connection parameters for SBxx server.

The log contains the following information about significant system events:

Item	Description
Severity	<p>The severity of the event, as follows:</p> <ul style="list-style-type: none"> Normal: A successful action, such as a completed download. Warning: An unsuccessful action, such as failure to detect a target. Major: An event relating to a failure to download to a target.
Date/Time	The date and time the event occurred.
Source	The IP address or the full identification of the target to which the event occurred.
Message	The nature of the event, such as a successful download to a target or retrieval from the web or an aborted or failed download or retrieval from the web.

Saving the Log

About this task

To save the log as a text file:

Procedure

1.
 - Select **File > Save Log File.**
 - Click the icon.

The system displays the **Save** dialog box.


2. In the **Save** dialog box, enter the path and filename.
3. In the **Save** dialog box, click **Save.**
The system saves the log file as a text file.

Clearing the Log

About this task

To clear the contents of the log, follow this step:

Procedure

To the left of the log area, click the  icon.

Closing the Log

About this task

You can toggle the log window to open or close.

To open or close the log window, follow this step:

Procedure

Select **View > Log**.

Chapter 5: ASCA Reporting Tool

Avaya Software Compatibility Audit Report Overview

The Avaya Software Compatibility Audit (ASCA) Report enables users without access to Software Update Manager to generate inventory reports. A script is run on the Communication Manager to generate an inventory file. Then the Avaya Software Compatibility Audit Report outputs the inventory file to an inventory report in HTML format. The information in the HTML report can be filtered, to display only the information you require.

This section describes the following:

- [Running the Inventory Script on the Communication Manager](#) on page 83
- [Downloading the Inventory File to your Computer](#) on page 84
- [Generating and Using an ASCA Report](#) on page 84
- [Using an ASCA Report Filter](#) on page 84

Running the Inventory Script on the Communication Manager

About this task

The inventory script generates the inventory file that the ASCA reporting tool uses to generate an HTML ASCA report.

To generate the inventory file on the Communication Manager, follow these steps:

Procedure

1. Using an account with root privileges from a telnet or a SSH session, log into an active Communication Manager server.
2. From CLI, change the directory to `/opt/ecs/sbin`.
3. To run the script, type `asca_poll_script`.
The system generates the inventory file and saves it to the `/var/opt/platform/ASCA` folder. The script automatically logs into each gateway using `root/root`.

 **Caution:**

You need to manually log into the gateways

If you have changed passwords on any gateway, you will need to manually log into those gateways. To do this, you must execute the script with the -u option, i.e. **asca_poll_script -u**.

 **Note:**

It is possible to run a more specific inventory when you run the script on the Communication Manager. Type `man asca_poll_script` for a complete guide to running the script.

Downloading the inventory file to your computer

About this task

In order to generate an ASCA report you must have a copy of the inventory file on your computer.

You can download the inventory file onto your computer *after* the inventory file is generated on the Communication Manager.

To download the inventory file to your computer, follow these steps:

Procedure

1. From your computer, use FTP or SSH to navigate to the file.
 2. From the Communication Manager go to the `/var/opt/platform/ASCAfolder`.
 3. Copy the file `ASCA_Inventory.txt` to your computer..
You can now generate an ASCA report. For more information on how to generate an ASCA report, see [Generating and Using an ASCA Report](#) on page 84.
-

Generating and Using an ASCA Report

About this task

The ASCA report displays information for all the elements of the Communication Manager, including the following groups:

- Main servers
- ESS's
- LSPs
- H.248 Gateways
- TN Circuit Packs
- DCP Endpoints
- IP Endpoints

For elements that have a version, you can display the currently installed version and the latest version available.

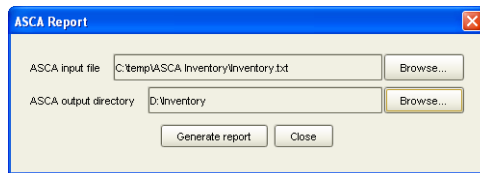
+ Tip:

If the currently installed version is highlighted in red, then you have not installed the latest version available.

To generate an ASCA Report, follow these steps:

Procedure

1. From the Software Update Manager, select **Tools > Generate ASCA Report**. The system displays the **ASCA** dialog box.



2. In the **ASCA** dialog box, click **Browse...** next to the **ASCA input file** field. The system displays the **Open** dialog box.
3. In the **Open** dialog box, select the input inventory file.
4. In the **ASCA** dialog box, click **Browse...** next to the **ASCA output directory** field. The system displays the **Open** dialog box.
5. In the **Open** dialog box, select the directory to save the ASCA HTML report file.
6. To generate the ASCA report, click **Generate report**. The system displays the **Confirmation** dialog box.
7. In the **Confirmation** dialog box, click **OK**. The system provides the generated ASCA HTML report.
8. To close the **ASCA Report** dialog box, click **Close**.

Using the ASCA Report Filter

About this task

You can filter ASCA Report information by hardware type (using the Group filter), or by software version (using the Version filter).

To filter the ASCA Report, follow these steps:

Procedure

1. To filter the report by group, select the check box of the group (or groups) you want displayed (or hidden).
 2. To filter the report by version, select the check box of the version type.
-

Upgrading the gateway using the LSP/TFTP server

This section of online helps upgrade the gateway and media modules to the latest version using the TFTP server on a Local Survivable Processor (LSP).

In some enterprises if the Software Update Manager server is located at the headquarters and the gateways service at the branch, the TFTP port requires to be open between the branch and the headquarters.

Generally for security reasons, if the TFTP has been disabled, this feature helps download faster because LSP is also located in the branch as the gateway.

Supported Device Types

This feature is supported only on the following **Device Types** and their media modules:

G250
G350
G450
G430
G700
P330

Configuration steps

Follow this three-step procedure to use this feature.

Step 1: Preparation

You can use this feature with any third-party TFTP Server or Communication Manager LSP server registered with the gateway to be upgraded. Avaya recommends that you use the LSP server.

While using the LSP Server, ensure that the gateway is configured correctly and discovered in SUM, and the LSP server has the firmware files on the TFTP root directory.

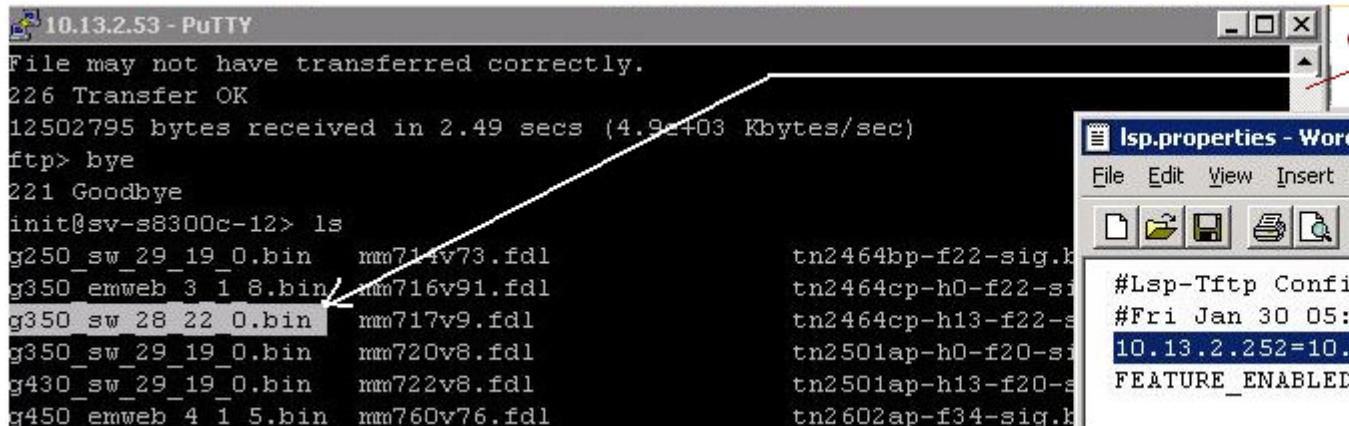
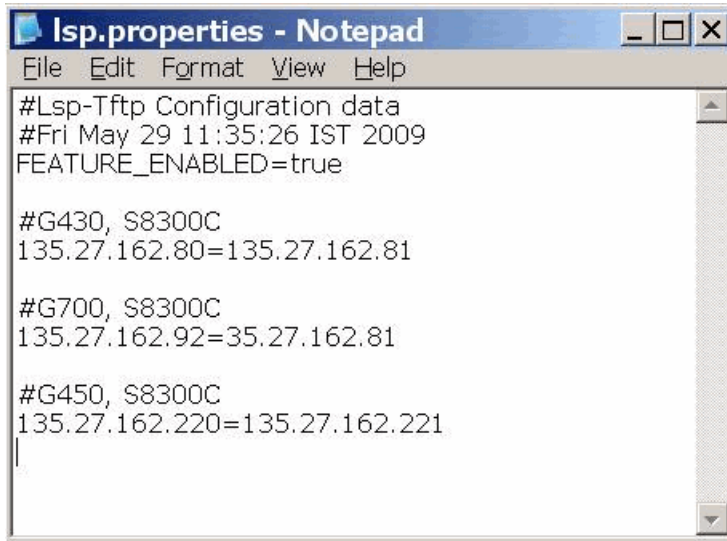


Figure 1: Firmware files present on the LSP server

Step 2: Configuration

Once you launch the SUM Client :

1. Navigate to the **File** menu.
2. Select **Options**. The system displays the dialog box, as shown below (Figure 3: Options dialog box).
3. Select the **Activate** check box and press **OK**. This creates a configuration file at the C:\Program Files\Avaya\Network Management\....\UServer\resource\UpdateMaster\Isp.properties directory.
4. Define <Gateway-IP Address = LSP/TFTP Server IP Address> mapping in this files. See the example in **Figure 1**. You need not restart Avaya Services.
5. Save the file, and close it.



```
lsp.properties - Notepad
File Edit Format View Help
#Lsp-Tftp Configuration data
#Fri May 29 11:35:26 IST 2009
FEATURE_ENABLED=true

#G430, S8300C
135.27.162.80=135.27.162.81

#G700, S8300C
135.27.162.92=35.27.162.81

#G450, S8300C
135.27.162.220=135.27.162.221
```

Figure 2: Configuration Property file

 **Note:**

If the mapping is not present in this file and the mode is activated, SUM will try to find the LSP Server IP address from the gateway using SNMP (CMG MIB cmgStaticControllerHosts.0). So make sure that the LSP-Gateway registration is complete, and the firmware files are present on the LSP server.

Ensure that you go to **Options** and clear the **Activate** check box to disable this mode, so that SUM continues with upgrades from the SUM Server.

Options
✕

Web Site

Avaya Support Web Site

Other:

Retry Download

Maximum Download Retries:

Delay Between Retries [seconds]:

Server Proxy Settings

Use Proxy

Host

Port

User Name

Password

Confirm Password

SFAP Login Parameters

Use SFAP

User Name

Password

Confirm Password

Sold To ▼

Gateway Upgrade via LSP/TFTP Server

Activate

Warning: Use of this feature requires initial setup, Please follow instruction given in SUM User guide.

Server: localhost User: administrator

Figure 3: Options dialog box

Step 3: Upgrade initiation

The upgrade process is similar to the gateway upgrade process (refer to [The Download Process - CMBE, Gateways, Data Switches, and Circuit Packs](#) on page 58 section for more details). The upgrade happens from the TFTP server rather than the SUM server.

Once you are done with the upgrades, ensure that you turn off this mode from the **Options** dialog box.

Index

Numerics

85xx [8](#)
87xx [8](#)

A

Accessing the Manage IP Phones Software [76](#)
Activate [52](#)
 changes [52](#)
Add [28, 30, 45, 65, 66](#)
 Network Management Console [28](#)
 Targets Table [28, 30, 66](#)
Adding or Editing a file [47](#)
After Download [66](#)
 Rebooting [66](#)
All Devices [66](#)
All Targets [28](#)
 Detecting [28](#)
AM110 [73, 75](#)
APP1 [66](#)
APP2 [66](#)
Apply [14–16, 28–30, 32, 34, 36, 40, 43, 45, 50, 52, 54, 57, 70](#)
 TN Boards [57](#)
Area [12](#)
ASCA [8, 83, 84, 86](#)
 filter [86](#)
 generate [84](#)
ASCA dialog [84](#)
ASCA HTML [83, 84](#)
 filter [83](#)
 want [84](#)
ASCA Report [84, 86](#)
 Filtering [84, 86](#)
 generate [84](#)
ASCA Report dialog [84](#)
ASCA_Inventory [84](#)
Asca_poll_script [83](#)
Assigned license [64](#)
 Viewing [64](#)
Assigning [63, 65](#)
 License [63, 65](#)
Assignment Table [63](#)
Auth Files [54, 64–66](#)
Auth Files checkbox [65](#)
Auth Files Table [65](#)
Authentication [63](#)

Authentication Files [63–65](#)
 device [65](#)
Authentication files table [65, 66](#)
Authorization Files [54](#)
Avaya [7, 14, 16, 45, 73, 74, 77](#)
 refer [45](#)
Avaya Network [13](#)
Avaya Network Configuration Manager [40](#)
 running [40](#)
Avaya Network Manager [7, 40](#)
 running [7](#)
Avaya P330 [66](#)
Avaya P330 Devices [66](#)
Avaya P330 M400 [66](#)
Avaya Software Compatibility Audit [83](#)
Avaya Software Compatibility Audit Report Overview [83](#)
Avaya Software Update Manager [5, 7, 13, 15, 16, 20,](#)
 [27, 28, 39, 40, 56, 58, 66, 70, 72–74, 79, 83, 84](#)
 describes [79](#)
 Starting [13](#)
Avaya Software Update Manager Overview [7](#)
Avaya Software Update Manager Targets Table [13](#)
Avaya Software Update Manager User Interface [49](#)
Avaya Support website [14](#)
 define [14](#)
Avaya_dir [40](#)
Avaya's website [7, 14–16, 20, 39, 40](#)

B

Backup/library [40](#)
Bank [66](#)
 downloaded [66](#)
BIOS [8](#)
Boot Image [66](#)
 Downloading [66](#)
Both Product Type [30](#)
Browse [43, 84](#)
Busy out [50](#)
 from standby [50](#)

C

Cancel [40, 58, 71](#)
 Scheduled Download [71](#)
Cancel Job button [60](#)
CD [50](#)

Hard Disk	50	Copy Release	60
CDROM	50	Customizing	26
Changes	52	Targets Table	26
Activated	52	CVS	40
Checkbox	50, 70, 86		
clear	86		
select	86	D	
Checkboxes	75	Data Connection Established	66
Circuit Packs 19, 20, 26, 31, 32, 39, 40, 44, 56, 58, 68, 69, 72		Data Switches 19, 20, 26, 31, 32, 39, 40, 44, 56, 58, 59,	
Circuit Packs Targets Table	19, 20	68,	72
Circuit Packs view	20, 32	69,	
Clear	32, 34, 36, 50, 81, 86	Date/Time	79
checkbox	86	DCP Endpoints	84
Log	81	Default Flash	66
CLI	83	Setting	66
Closing	43, 52, 54, 60, 75, 81, 84	Defaults	40
Log	81	Define Proxy Settings	13
Product Defaults dialog	43	Define SFAP Login Parameters	13
CM	8, 57, 60, 84	Defining	14, 15, 45
install	60	Avaya	14
CM Release Location checkbox	60	download intervals	15
CM Server	59, 60	Remote Software Library	45
CM Server System	60	server proxy settings	15
CM Service Packs	60	Delay Between Retries	15, 70
CM Service Packs checkbox	60	Delete	66, 77
CM Software dialog	59	File	66
CM Software Management ... 20, 26, 31, 36, 39, 40, 44,		Describes	79
49, 56, 58, 59, 68, 69, 72		Avaya Software Update Manager	79
Select	36, 59, 68, 69	Detecting	28–30
Use	20	All Targets	28
CM Software Management dialog	59, 60, 63, 68, 69	New Targets	28
CM Software Management Targets Table	19, 20	Targets Using Filters	30
CM Software Management View	20, 36, 59	Detection Process	27
CM Software Upgrade	60, 65, 68, 69	Starting	27
Column Chooser dialog	26	Device Type	39, 57
Communication Manager	8, 19, 20, 60, 83, 84	Devices	65, 66
Release	83	authentication files	65
Updates	60	Devices Table	64, 65
Computer	84	DHCP	73
Configuring	44, 49, 56	Dialog Area	12
Download Parameters	56	Displays BIOS	8
Software Libraries	44	Distributed Office ... 19, 20, 26, 31, 32, 39, 40, 44, 56, 58,	
Confirm Password	16	68,	72
Console	13	Select	32, 58, 68, 69
Contains	73	Use	20
TFTP	73	Download Failed	66
Contents	5	Download intervals	15
Contents Page	5	Defining	15
Continue	58	Download Now	58, 75
Copied	50	Download Parameters	56, 57
Copy & Install	60	Configuring	56
		Download Process	58, 59
		Download Process Status Messages	66

Download Progress	66
Download Proxy	57
Download Successful	66
Download Targets Detection	27
Download Targets Detection dialog	27–30
Downloads	46, 60, 66, 68, 70, 73–75, 84
Bank	66
Boot Image	66
Image	66
inventory file	84
IP	73
Scheduling	68
Software	74, 75
DS1	8, 58
includes	58

E

Ecs	83
Enables	45
FTP	45
NMS	45
SCP	45
Enter	30
IP	30
Erasing	66
Flash	66
ESS	8, 60, 84

F

File Size	66
Files	13, 46, 66, 74, 77
Deleting	66
Importing	77
Files available	46
Viewing	46
Filter Devices dialog	32, 34, 36
Filtering	31, 32, 34, 36, 83, 84, 86
ASCA	86
ASCA HTML	83
ASCA Report	84, 86
Targets Table	31, 32, 34, 36
Filtering,	39
Device Type	39
Flash	66
Erasing	66
From standby	50
busy out	50
Ftp	45, 52, 84
enabled	45

name	45
FTP Password	45
FTP Server Path	45
FTP User Name	45

G

G250	73
G350	73
G450	73
G450 Telephony	8
Gateway devices	73
IP phone configuration updates	73
Gateways	19, 20, 26, 31, 32, 39, 40, 44, 56, 58, 59, 68, 69, 72, 84
Generate	84
ASCA	84
ASCA Report	84
Generate ASCA Report	84
Group	86
using	86

H

Hard Disk	50
CD	50
URL	50
Hardware Version	57
Help	5
Opening	5
Help ON	5
Host	15
HTML	83
HTML ASCA	83
HTTP	50, 59, 60, 73
HTTP file	8
HTTPS	8, 59, 60
HTTPS protocol	59

I

Image	66
Downloading	66
Image Analyzer	39
Import window	77
Importing	77
Files	77
Including	58
DS1	58
Information	29

Updating	29
Install License	65
Install Release	60
Installation	50
Versions Available	50
Installed Versions	50
Installing	60
CM	60
Interest	5
Topic	5
Inventory file	84
Downloading	84
Inventory Script	83
Running	83
IP	19, 20, 30, 31, 45, 57, 73–75, 77, 79
downloading	73
enter	30
IP Address	30, 31, 57
IP Address Filter	30
IP Endpoints	84
IP Office	73
IP phone configuration updates	73
gateway devices	73
IP Phones	13, 20, 34, 73–75, 77
Select	34, 74
IP Phones Software Libraries	73, 77
IP Phones Software Libraries dialog	77
IP Phones Targets Table	19
IP Phones View	20, 34
IP Telephony	20

J

Job Date	70
Job Owner	70
Job Summary window	60

L

License	54, 63–66
Assigning	63, 65
License File	54, 65
Line help explains	73
Local Software Library	77
Log	79–81
Clearing	81
Closing	81
Saving	80
Viewing	79
Log file	77, 79
Viewing	77

Log Report	79
LSPs	8, 60, 84

M

Main CM Server	60
sequence	60
Main Server	8
upgrading	8
Major - An	79
Manage IP phone software distribution	73
Manage IP Phones Software	75
Manage Updates	52
Maximum Download Retries	15, 70
specify	70
Media Server	20, 49, 50, 52, 54, 59, 60
Reset - Resets	50
Media Server CD	60
Media Server Details dialog	49
Media Server Hard Disk	60
Media Server License	54
Media Server Operations	50
Media Server Release Management	50
Media Server Software Repository	49
Configuring	49
Media Server Table	50
Media Server Updates	52
Mode_dir	40
Modif	40
Module #/Location	57
Modules	72
Resetting	72

N

Name	45, 57
FTP	45
SCP	45
USB	57
Network Management Console	28
added	28
Network Management Server	44, 73, 75, 77
use	77
Network Management Station	40
New	8
New Targets	28
Detecting	28
New Versions	40
Retrieving	40
NMS	8, 40, 44, 45, 74
enabled	45

NMS CD	59, 60
NMS Library	68, 69
NVRAM	73

O

OK	15, 16, 26–30, 32, 34, 36, 40, 43, 84
Open	5, 54, 65, 68, 69
Help	5
Schedule Download dialog box	68, 69
Open dialog	54, 65, 84
Options dialog	13–15
Other	14

P

Parameters	66
Setting	66
Performing	39
Web Analysis	39
Phones Software Table	74
Platform	60
PN	8
Populate	56, 58, 74
Targets Table	56, 58, 74
Port	15
Port Network	57
Printing	27
Targets Table	27
Product Defaults	43
Setting	43
Product Defaults dialog	43
close	43
Product Filter	30
Product Type	30

R

RAM	73
Ranges	31
Rebooting	50, 66
After Download	66
Refer	45
Avaya	45
Regarding	16
SFAP	16
Release Management	50
Release Management Tab	50
Releases	8, 50, 83
Communication Manager	83
Remote Software Library	45

Defining	45
Remove	71
Reset	70, 72
Modules	72
Reset - Resets	50
Media Server	50
Reset After Download	70
Resize	79
Resized	12
Retrieve From	40
Web	40
Web dialog	40
Retrieve Image From	40
Web	40
Retrieve Sold To's	16
Retrieving	40
New Versions	40
Retry Download	70
Retype FTP Password	45
Retype SCP Password	45
Reverts	52
Unpacked	52
Rom	50
Running	7, 40, 83
Avaya Network Configuration Manager	40
Avaya Network Manager	7
Inventory Script	83

S

S8300 CM	68, 69
S83xx	8
upgrades	8
SAT	50
Save	19, 26, 50, 80
Log	80
Targets Table	19, 26
Save As	26
Save dialog	80
Save Log File	80
Save Translation	50
Sbin	83
Schedule Calendar	70
Schedule Download	68, 69, 71
Cancelling	71
Schedule Download dialog	68–70
Schedule Download dialog box	68, 69
Opening	68, 69
Schedule Download Information	70
Viewing	70
Schedule Download Table	70
Scheduling	68–70, 75

Downloads	68	Software Libraries dialog	44, 46
Software Downloads	70	Software Libraries Parameters	45
SCP	45	Software Libraries Properties Table	45
enabled	45	Software Type	57
name	45	Software Update Manager	28, 68, 69, 74, 77
SCP Password	45	Software Version	57, 70
SCP Server Path	45	Software Version Selection dialog	43
SCP User Name	45	Sold To	16
Script File Table	74	select	16
Section	73	Sold To's	16
Security Update checkbox	60	Sorting	25
Select	16, 32, 34, 36, 45, 58, 59, 68, 69, 74, 75, 86	Targets Table	25
checkbox	86	Specify	70
CM Software Management	36, 59, 68, 69	Maximum Download Retries	70
Distributed Office	32, 58, 68, 69	SSH	83, 84
IP Phones	34, 74	Standalone Mode	7, 40
Software Libraries	45	Standby Supervisor	66
Sold To	16	Synchronizing	66
Select Actions	27, 49, 56, 58, 59, 68, 69, 71, 72, 74, 75	Start	13, 27
Select Avaya Support Web Site	14	Avaya Software Update Manager	13
Select Copy	50	Detection Process	27
Select Delete	50	State	39
Select Detect	28, 30	updates	39
Select File	26, 27, 80	Status	66, 70
Select Help	5	Status Line	12, 32, 36
Select IP	75	SUM	68, 69
Select Tools	39, 40, 43, 44, 77	SUM 5.2	59, 60
Select View	32, 34, 36, 79, 81	Supports Avaya G430	8
Selected Devices	75	Switches	50
Selected Targets	29	Synchronizing	66
Sequence	60	Standby Supervisor	66
Main CM Server	60		
Server Library	77	T	
Server proxy settings	15	Table	63
Defining	15	Target Details	49, 56, 59, 68, 69, 74
Server station	40	Target Details dialog	56
Setting	43, 66	Targets Table	12, 13, 19, 20, 25–32, 34, 36, 39, 40, 56, 58, 60, 63, 64, 66, 68–70, 72, 74, 75, 79
Default Flash	66	added	28, 30, 66
Parameters	66	Customizing	26
Product Defaults	43	Filtering	31, 32, 34, 36
SFAP	16	populate	56, 58, 74
regarding	16	Printing	27
SFAP Login Parameters	16, 40	save	19
Skip	40	Saving	26
Software	8, 74, 75	Sorting	25
Downloading	74, 75	use	19
Software Downloads	70	views	19
Scheduling	70	Targets Using Filters	30
Software Libraries	44–46, 57, 70, 77	Detecting	30
Configuring	44	Telnet	83
Select	45		

TFTP	8, 45, 59, 68, 69, 73	Use Proxy checkbox	15
contains	73	Use SFAP checkbox	16
TFTP Server Secure Path	45	User Name	16
TN	8	Userver	40
upgrade	8	Using	86
TN Board	57, 58	Group	86
applies	57	Version	86
TN Circuit Packs	84	Using Tooltips	13
Tools	13, 84	Using Wildcards	31
ToolTip	13	V	
Tooltips	13	Var	52, 83, 84
Topic	5	Version	86
Interest	5	using	86
Txt	84	Versions Available	50
Type	52	Installation	50
U		View Tabs	12
Unpacked	52	Viewing	13, 19, 46, 64, 70, 77, 79
reverts	52	assigned license	64
Update ID	52	files available	46
Update Manager	77	Log	79
Updates	29, 39, 60, 65, 68, 69	Log Files	77
Communication Manager	60	Schedule Download Information	70
Information	29	Targets Table	19
State	39	W	
Upgrades	8, 60	Waiting	70
Main Server	8	Want	84
S83xx	8	ASCA HTML	84
TN	8	Web	40
URL	50, 60	Retrieve From	40
Hard Disk	50	Retrieve Image From	40
USB	57	Web Analysis	39
name	57	Performing	39
USB Flash Drive	57	Web dialog	40
Use	19, 20, 77	Retrieve From	40
CM Software Management	20	Web Site	14
Distributed Office	20	Website	13, 14, 40, 45
Network Management Server	77	Website download parameters	14
Targets Table	19	Defining	14

