Avaya Integrated Management

Network Management

Release 5.2 Service Pack 4

Issue 2
March 2010

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the Web site, simply go to http://www.avaya.com/support **and search for the document number in the search box.**

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the following Web site:

http://www.avaya.com/support

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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.

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://www.avaya.com/support

Contents

Integrated Management - Network Management Release 5.2 Service Pack 4 Release Notes

Integrated Management - Network Management Release 5.2 Service Pack 4 Network Management

Integrated Management - Network Management service packs are cumulative. This service pack includes modifications and enhancements specific to this service pack and from earlier service packs, if any.

Table 1: Changes delivered to Network Management Release 5.2 Service Pack 4 on page 8

For information on fixes made in previous service pack releases, refer to Integrated Management Network Management 5.2 prior Service Pack fixes on page 23.

Integrated Management supports IP Office Release 5.0

Avaya is pleased to announce that the support of IP Office Release 5 in Avaya Integrated Management is now available with the delivery of the 1Q 2010 maintenance release for IP Office Release 5.

You can now manage IP Office Release 5 through Avaya Integrated Management applications by following the instructions given in this document.

Product Support Notices

Some problems are also documented as Product Support Notices (PSN). The PSN number defines the related document and appears in the Problem column in the tables.

To read the PSN description online:

1. Go to the Avaya support site at http://support.avaya.com.
2. Scroll down to **PRODUCT INFORMATION** and click on **Product Support Notices**.
3. Type the last four digits of the PSN number into your web browser's "Find on Page" function to search the page for a link to the PSN.
4. Click the PSN title link to open the PSN.

Integrated Management - Network Management 5.2 Service Pack 4 fixes

Avaya now supports client access to Network Management applications using Internet Explorer 8 on Windows 7 Professional (x86 and x64). Avaya does not support any other web browser on Windows 7 Professional (x86 and x64).

Table 1: Changes delivered to Network Management Release 5.2 Service Pack 4

Changes delivered to Network Management	Solution
Network Management Console with VoIP System View	
The **CM Server Passwords** tab in **NMC Options** is enhanced and now supports the export and import of Communication Manager Server data.	

In the previous release, IP discovery did not work correctly under the following conditions: • the interface discovery option is disabled [**Actions > Discover Interfaces**] • a router-based discovery is fired	The issue is fixed in this release.
In the previous release, customers were unable to see the IP phone for the Communication ManagerCommunication Managers in the **Server Separation Mode**, and extensions with port **X** were missing.	The issue is fixed in this release.
In the previous release, the CM server's IP Interface information [in standby mode] did not correctly display in the Interfaces tab.	The issue is fixed in this release.
In the previous release, for some devices SNMP default setting was incorrect.	The issue is fixed in this release.
In the previous release, after logging out the Discover Interfaces checkbox status would be lost. On logging in again, the Discover Interfaces checkbox status would always be set to false.	The issue is fixed in this release. The Discover Interfaces checkbox status is now saved for the corresponding map. For new maps that are created in NMC, the default for Discover Interfaces checkbox status is true.
In the previous release, the phone data would not be discovered if you added Communication Manager with ASG login user.	The issue is fixed in this release.

Network Management Service Pack 4 Installer	
Network Management Service Pack 4 Installer is now enhanced to clean the Java cache on the server for the local administrator account [which is used to install the service pack]. You must still clean the Java cache on the client machine.	
Network Management 5.2 Service Pack 4 supports the latest version of IP Office Manager 7.0 (15).	
In the previous release, Tomcat had a parameter incorrectly set. Due to this, the directory listing was enabled.	The issue is fixed in this release.
In the previous release, after uninstalling Network Management 5.2 some Network Management 5.2 links were still visible.	The issue is fixed in this release. Now after uninstalling no Network Management 5.2 related links are visible.
In the previous release, after uninstalling IP Office Manager 7.0, IP Office Manager 7.0 and related support is still visible.	The issue is fixed in this release. Now after uninstalling no IP Office Manager 7.0 or its related support are visible.

Software Update Manager	
In the previous release, a SFAP user name could only be 30 characters long.	The issue is fixed in this release. SUM now supports a SFAP user name that is longer than 30 characters.

Known Issues and Workarounds

Known Issues	Workarounds
Software Update Manager is not able to connect to the Avaya Support Web site.	In the Network Management Server: 1. Select **Start > All Programs > Avaya > Stop Avaya services**. 2. Select the drive where you installed Network Management. For example C: 3. Go to ***Program Files\Avaya\Network Management\CVS\UServer\resource\compatibility*** 4. Delete the **versions_site.xml** file. 5. Select **Start > All Programs > Avaya > Start Avaya services**.
You may get an error in Software Update Manager if you try to upgrade Small Office Control unit.	Resubmit the job. It is observed that the upgrade is successful if you attempt it the second time.

Issue with JRE 1.6.0.11 If you are using JRE 1.6.0.11, sometimes all the open Internet Explorer browsers crash if you open the online help of any one of the Network Management applications, and then close the application browser.	1. Launch the application window again. OR 2. Install JRE 1.6.0.16 on your client. The Network Management 5.2 Service Pack 4 installation provides JRE 1.6.0.16.
If you have Network Management 5.2 Custom (with only Integrated Management launch page, Network Management Console, Software Update Manager, and Configuration Backup Restore) + SP3 **with IP Office support installed**, the system does not display the link for **Provisioning and Installation Manager for IP Office** in the launch page.	1. In the Network Management server, select **Start > Programs > Avaya > Tools > Configure Integrated Management**. The system displays the **Configure Utility** dialog box. 2. Perform some changes in this dialog box. For example, you can clear any checkbox, and then select it again. 3. Click **Save**. 4. Click **Exit**. 5. Refresh the Integrated Management launch page. You can now see the link for Provisioning and Installation Manager for IP Office.

The Adobe Flash Player for Internet Explorer 8 that comes with the Network Management application does not work if you are using Windows 7 Professional operating system. This issue effect the following Network Management aplications: • Branch Central Manager • User Administration • Change Password	From the Adobe site (http://get.adobe.com/flashplayer/) download and install the latest Adobe Flash Player. After Adobe Flash Player is successfully installed, the effected Network Management applications will work properly.
The IP Office System Status auto-login feature does not work when you open IP Office System Status from the Network Management Console.	For the selected IP Office device, manually enter the admin username and password.
If the Network Management Console is installed on a 64 bit OS, you cannot create a device profile and run the job in PIMIPO.	1. Stop **Avaya Services**. 2. On the Network Management Console server, open the command prompt. 3. Run the following two commands in the order given. **Note:** The commands are listed in a Note after the table. 4. Start **Avaya Services**.

Note:

Listed below are the commands to run if the Network Management Console is installed on a 64 bit OS, and you cannot create a device profile and run the job in PIMIPO.

```
%PIM_JBOSS%\bin\AvayaJBossPIMIPO.exe -uninstall AvayaJBossPIMIPO


%PIM_JBOSS%\bin\AvayaJBossPIMIPO.exe -install AvayaJBossPIMIPO %CV_PATH%\
..\JRE\1.6.0_11\bin\client\
jvm.dll -Xrs -Dnmc.service.
ip=127.0.0.1 -Xms128m -Xmx512m -Djava.library.path=%CV_PATH%\..\IPOffi~1\\
Manager -Djava.class.path=%CV_PATH%\..\private\SSO\;%CV_PATH%\..\JRE\
1.6.0_11\lib\tools.jar;%PIM_JBOSS%\bin\run.jar;%CV_PATH%\CVS\gen\resources\
resources.jar;%CV_PATH%\CVS\gen\resources\private\
adminResource.jar -start org.jboss.
Main -params -c pimipo -stop org.jboss.
Main -params -c pimipo -method systemExit -out %PIM_JBOSS%\
bin\PIMIPOout.txt -current %PIM_JBOSS%\bin
```

WARNING:
Each of the two commands above must be copied to a separate line.

Though you see line breaks in the second command, when you copy this command make sure that there are no line breaks, and you enter the command in one line.

Third-party software license

- This product includes software developed by the Apache Software Foundation http://www.apache.org/). The licenses can be found at http://www.apache.org/licenses/.

- The adobe flash player is distributed under the adobe flash player end user license agreement (http://www.adobe.com/products/eulas/).

  Adobe® Flash® Player Copyright © 1996 - 2008. 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.

Using Network Management on Microsoft Windows Vista Operating System

Follow the instructions given below only if you are using Microsoft Windows Vista Operating System in which the UAC (User Account Control) mode is enabled.

Tip:
For more information on the UAC mode, see http://technet.microsoft.com/en-us/library/cc709691.aspx.

Network Management uses applications such as Telnet Client which are provided along with the operating system. You must configure it in Windows Vista before using it.

To use the Telnet Client in Vista, you must enable it from the Control Panel. On Windows Vista, you can use the Windows Features tool to install optional components.

To install Telnet Client on Windows Vista:

1. Click **Start**, and then click **Control Panel**.
2. On the **Control Panel Home** page, click **Programs**.
3. In the **Programs and Features** section, click **Turn Windows features on or off**.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. In the **Windows Features** list, select **Telnet Client**, and then click **OK**.

Tip:
For more information see, http://technet.microsoft.com/en-us/library/cc771275.aspx#bkmk_installvista.

Important:
In the Microsoft Windows Vista, you must run the ENM applications as an *administrator*.

For example, when you select **Start Avaya services**, **Stop Avaya services**, or **ENM Easy Restore** from the start menu, right-click and then select **Run as administrator**.

Note:
You can configure **NM Easy Restore** to automatically run as administrator each time you start it. To configure, you can use the procedure described in the Web site, http://support.microsoft.com/kb/922708.

You must set the proper Compatibility mode for the application to run as administrator by default.

Using Network Management on Microsoft Windows 7 Professional Operating System

Network Management uses the Telnet Client application provided with the Microsoft Windows 7 Professional operating system. You must configure the Telnet Client application in Windows 7 before you can use it.

You can enable Telnet Client from the Control Panel using the Windows Feature tool.

To enable Telnet Client in Microsoft Windows 7 Professional operating system, follow these steps:

1. Click **Start**, and then click **Control Panel**.
2. On the **Control Panel Home** page, click **Programs**.
3. In the **Programs and Features** section, click **Turn Windows features on or off**.
4. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

5. In the **Windows Features** list, select **Telnet Client**, and then click **OK**.

Tip:
The installation might take several minutes.

Note:
For more information see, http://windows.microsoft.com/en-US/windows-vista/Telnet-frequently-asked-questions.

Installing the IP Office Manager 7.0 (18) patch

This patch provides fixes and enhancements to IP Office Manager 7.0. Installing this patch enables you to manage IP Office Release 5 from the Network Management applications.

WARNING:
You must have Network Management 5.2 and Network Management 5.2 Service Pack 4 installed on your system.

Installing the IP Office Manager 7.0 (18) patch on a server

To install IP Office Manager 7.0 on a server, follow these steps:

1. From the Avaya support site (http://support.avaya.com) download **`IPOfficeManager7.0(18).exe`** to your system.

2. Stop Avaya Services.

Note:
To stop Avaya Services, follow these steps:

1. Click **Start**.

2. Select **All Programs > Avaya > Stop Avaya Services**.

3. Run **`IPOfficeManager7.0(18).exe`**.

4. Select **Yes**, when the **IP Office Manager** dialog box states "**This setup will perform an upgrade of 'IP Office Manager'. Do you want to continue?**".

5. To continue the installation, click **Next**, in the **IP Office Manager - InstallShield Wizard** dialog box.

6. Click **Finish**, when the **IP Office Manager - InstallShield Wizard** dialog box states **InstallShield Wizard Completed**.

7. Rename **`IPOfficeManager7.0(18).exe`** to **`IPOfficeManager.exe`**.

8. Copy **`IPOfficeManager.exe`** to the **`<NM_install_path>\Avaya\Network Management\CVS\IPO\`** path on the NM server.

9. Start Avaya Services.

Note:
To start Avaya Services, follow these steps:

1. Click **Start**.

2. Select **All Programs > Avaya > Start Avaya Services**.

Installing the IP Office Manager 7.0 (18) patch on a client machine

To install IP Office Manager 7.0 on a client machine, follow these steps:

1. Click the **Avaya IP Office Manager 7.0** link, from the Intergrated Management launch page (located on the server).

2. Download the latest version of IP Office Manager to your machine, and install.

Upgrading the phone firmware

Some phones might not connect to IP Office after using Network Management 5.2 to upgrade the IP Office firmware to 5.0 1Q 2010. These phones need a firmware upgrade.

Prerequisite

From the Avaya support site (http://support.avaya.com), download the IP Office Release 5.0 1Q 2010 Administration CD, and install it on a computer.

WARNING:
You can only install IP Office Release 5.0 1Q 2010 on a computer that does *not* have Network Management 5.2 Service Pack 4 installed on it.

Note:
The IP Office Release 5.0 1Q 2010 Administration CD contains IPO Manager with the required phone firmware.

Note:
A running IP Office Manager can act as a TFTP server and provide files from its configured binaries directory.

Important:
To upgrade the phone firmware your computer must use an IPO Manager that runs the TFTP server, and IPO can be used as a TFTP-HTTP relay.

Installing phone firmware on IP phones

To install the phone firmware on IP phones, follow these steps:

1. Launch IP Office Manager, and for the IP Office phones that are not working, open the IP Office configuration.

   Important:
   IP Office must be upgraded to IP Office firmware Release 5 1Q 2010.

2. Select **System** node in the **Navigation** window.

3. Set the **TFTP Server IP Address** to the IP Address of the machine where the TFTP Server will run.

   Note:
   Enter the IP Address of the IP Office Manager computer or 0.0.0.0, if your computer is running IP Office Manager as a TFTP Server.

4. Set the **HTTP Server IP Address** to the IP Address of the machine where the HTTP Server will run.

   Note:
   Give the IP Address of the IP Office control unit, if IP Office is running as the HTTP Server.

5. Select **Manager** for **Phone File Server Type**.

   Note:
   In IP Office Manager, the HTTP Server's default IP Address is 0.0.0.0 (Disabled) and it is available in software level = 4.2+.

Note:
If an address is entered here, Avaya IP phones using IP Office DHCP use that address to request software and settings files.

6. In the **Manager PC IP Address** field enter the IP Address of the computer where IP Office Manager is running.

   Note:
   The default value for the **Manager PC IP Address** field in IP Office Manager is 0.0.0.0 (Broadcast).

7. Click **Save**.

8. Click **OK** on the **System node** page in IP Office Manager.

9. To save the new IP Office configuration, select **File > Save**.

10. Select **Immediate** for the **Configuration Reboot Mode** field - in the the **Send Configuration** dialog box.

11. Click **OK** in the **Send Configuration** dialog box.

    Note:
    IP Office now reboots. This process takes a few minutes. The phones connected to IP Office automatically upgrade after the reboot is complete.

Tip:
Phones are functional only after successfully upgrading the phone firmware.

Installing phone firmware on digital phones

You can upgrade digital phones using a TFTP Server. Using IP Office Manager configure the TFTP Server IP Address on the IP Offie control unit.

Note:
The IP Office Manager TFTP Server's default IP Address is 0.0.0.0 (Broadcast).

If your computer is running IP Office Manager as a TFTP Server, it can also provide files from its configured binaries directory.

You can disable IP Office Manager from acting as a TFTP Server using EnableBootP and TFTP Servers command.

To install the phone firmware on digital phones, follow these steps:

1. Launch IP Office Manager, and for the IP Office phones that are not working, open the IP Office configuration.
2. Select **System** node in the **Navigation** window.
3. Set the **TFTP Server IP Address** to the IP Address of the machine where the TFTP Server will run.

   Note:
   Enter the IP Address of the IP Office Manager computer or 0.0.0.0, if your computer is running IP Office Manager as a TFTP Server.

4. Click **OK** on the **System node** page in IP Office Manager.
5. To save the new IP Office configuration, select **File > Save**.
6. Select **Immediate** for the **Configuration Reboot Mode** field - in the the **Send Configuration** dialog box.
7. Click **OK** in the **Send Configuration** dialog box.

   Note:
   IP Office now reboots. This process takes a few minutes. The phones connected to IP Office automatically upgrade after the reboot is complete.

Tip:
Phones are functional only after successfully upgrading the phone firmware.

Appendix A: Integrated Management Network Management 5.2 prior Service Pack fixes

Integrated Management - Network Management 5.2 Service Pack 3 fixes

The following name changes are done to applications in the Avaya Integrated Management product.

Old Name	New Name
Enterprise Network Management	Network Management
Avaya Communication Manager	Avaya Aura™ Communication Manager
Avaya Communication Manager Branch Edition	Avaya Aura™ Communication Manager Branch
Communication Manager Branch Edition - Central Manager	Branch Central Manager
Configuration Backup and Restore Manager	Configuration Backup Restore
System Management	Performance and Administration
Administration Tools	Site Administration
ENM Backup Utility	NM Backup Utility
ENM Easy Restore Utility	NM Easy Restore Utility
ENM Log Viewer	NM Log Viewer

Table 2: Changes delivered to Network Management Release 5.2 Service Pack 3

Changes delivered to Network Management	Solution
Network Management Console with VoIP System View	
Support for Avaya Aura™ Communication Manager Release 5.2.1. Network Management Console supports the following functions on Communication Manager Release 5.2.1: • Discovery and display of devices in the Device Type view • Proper correlation of devices in the VoIP System View • Basic administration tasks such as Adding, Deleting, and Modifying devices • Network Discovery Wizard	
This release supports Avaya Aura™ Communication Manager running on the Next Gen S8800 server platform in simplex and duplex modes. • Support for the new platform Next Gen S85xx server • Support for the new platform Next Gen S87xx server **Note:** In the simplex mode, the Network Management Console displays the S8800 as S85XX, and in the duplex mode as S87XX.	

This release reinstates the IP Office support similar to the Network Management Release 5.0. Specifically, this release provides IP Office 5.0 support to the following applications: • Discovery, including VoIP SystemView • Port Connections • Secure Access Administration • Fault Monitoring • Software Update Manager • Provisioning and Installation Manager for IP Office • IP Office System Status	
Support for IP Office Manager 7.0 You can start IP Office Manager 7.0 on an IP Office device to see detailed information not presented in the System View. A new instance of IP Office manager opens each time you start the application from the Network Management Console.	
G860 related changes: The G860 AudioCodes SysOID is replaced by Avaya SysOID. The G860 AudioCodes Trap OIDs is replaced by Avaya Trap OIDs.	
Support for Microsoft Windows Vista with Service Pack 2.	
In this release, Network Management Console does not display the **Phone Extension** column in the **Interfaces** table as it did in previous releases.	

In the previous release, when you closed the **IP Discovery** window, Network Management Console raised an exception in the Java console.	This issue is fixed in this release, Network Management Console does not raise an exception after you close **IP Discovery** window.
In previous releases, you could initiate an IP discovery without providing any subnet or router IP addresses in the **IP Discovery** dialog box. You could not use the **Stop Discovery** option after you initiated the discovery.	This issue is fixed in this release. Now, you cannot run the discovery without entering discovery data.
In the previous release, if you selected SNMP version V3 in the **SNMP** tab of the **Options** dialog box, the user dropdown also displayed CLI users. When you select SNMP V3, the system should only display the SNMP V3 enabled users.	This issue is fixed in this release. Now, the system does not display CLI users in the SNMP V3 user dropdown list.
In the previous release, after the discovery process, Network Management Console did not display the IP phones information under the **Registered Endpoints** tab. **Note:** This issue was not observed consistently.	This issue is fixed in this release. Now, you can view the IP phones information under the **Registered Endpoints** tab.
In this release, the sequence of the discovery process has changed. This helps in enhancing the speed of the IP Phone data discovery. The new discovery sequence is: 1. IP discovery 2. System View discovery 3. IP phone data discovery 4. Port connection discovery	

In this release, the **Discover** check box in the Network Management Console's **File > Options > CM Servers Password** tab has been renamed to **Discover Phones**. The label **Discover** was misleading. This check box is used to discover phones associated with Communication Manager. Even if you do not select the check box, the Communication Manager is discovered and displayed in the Network Management Console view. **Note:** The state of the check box does not affect Software Update Manager's operation.	
From this release discovering interfaces has been made optional. A new check box is added to discover interfaces. If you want to include interfaces in the discovery, select **Actions > Discover Interfaces** in the Discovery window. The interfaces won't be discovered if you do not select the **Discover Interface** check box.	

From this release, you can configure a maximum of five user-defined applications or tools links to appear on the Integrated Management launch page. To add links: 1. In the Network Management Server, select **Start > All Programs > Avaya > Tools > Configure Integrated Management**. 2. Click the **Other URL Information** tab. 3. In the **Name** field, enter the name of the application/tool you want to add to the launch page. 4. In the **URL:** field, enter the URL of the application/tool. 5. Click **Save**. 6. Click **Exit**. You can view the link on the Integrated Management launch page under the section, **Other Operations and Links**.	
NM Backup and NM Easy Restore Utility	
Support for IP Office in the NM Backup and the NM Easy Restore Utility This release supports backup and restore of IP Office related files using the NM Backup and the NM Easy Restore Utility tools. The NM Backup utility also saves the configuration files of Provisioning and Installation Manager for IP Office.	

Software Update Manager	
In previous releases the end user license agreement is not displayed prior to downloading files.	The issue is fixed in this release. After selecting the **Retrieve From Web** option, you will see and must accept the end user license agreement.
In this release the Software Update Manager supports kernel updates for the Communication Manager release.	
In this release the Software Update Manager supports Avaya Aura™ Communication Manager running on Next Gen S8800 server platform in duplex modes running software duplication.	
Software Update Manager now supports Communication Manager release 5.2.1.	
Software Update Manager now supports IP Office upgrades to firmware for IPO 4.0 and 5.0 releases.	
In previous releases after selecting **Activate** or **Deactivate**, the Status columns in the **CM Software Management** tab and the Manage Updates tab in the **Media Server Details** panel did not immediately correlate with one another.	The issue is fixed in this release.
In previous releases the Software Update Manager did not validate the SCP Server Password and special characters (!@#$%^) are not accepted by the Communication Manage leading to errors in the TN upgrade.	The issue is fixed in this release; Software Update Manager validates the password entered by the user.
In previous versions Software Update Manager associated incompatible (wrong hardware) versions for TN upgrades. Scenario occurred especially for TN Boards having different hardware compatibility for the same firmware version.	The issue is fixed in this release. To allow the users to view the correct hardware compatibility for a particular firmware version, a new column named **Hardware** is added to the **Files** tab in the **Software Libraries** panel.

In previous versions of Software Update Manager, some users were having compatibility issues with Communication Manager software and Gateway (GW) firmware versions. Software Update Manager User Interface was recommending latest GW firmware version irrespective of the Communication Manager versions to which it was registered.	Avaya recommends using like gateway firmware version series and Communication Manager releases. The following gateway firmware series are recommended with the following Communication Manager software releases: • Gateway firmware version series 25.xx.xx with Communication Manager 3.x.x software releases. • Gateway firmware version series 26.xx.xx with Communication Manager 4.x.x software releases. • Gateway firmware version series 27.xx.xx with Communication Manager 5.0.x software releases. • Gateway firmware version series 28.xx.xx with Communication Manager 5.1.x software releases. • Gateway firmware version series 29.xx.xx with Communication Manager 5.2.x software releases. Avaya does not support newer Communication Manager software releases running with older gateway firmware versions. **Note:** Gateway with incompatible firmware can result in a service affecting scenario. Software Update Manager recommendation is most appropriate.
Secure Access Administration	
This release reinstates the IP Office User support similar to the Release 5.0	

Branch Central Manager (formerly known as Communication Manager Branch Edition - Central Manager)	
Support for 1692 and 9650 handsets in the Branch Central Manager user interface.	
The following labels have been changed in the station template. • **Avaya 4690** to **Avaya 1692/4690** • **Avaya 9630** to **Avaya 9630/9650** In the Branch Central Manager user interface the phone names are changed as given below. • **9630-SIP** to **9630/9650-SIP** • **4690-H323** to **1692/4690-H323**	

Integrated Management - Network Management 5.2 Service Pack 2 fixes

Table 3: Changes delivered to Network Management 5.2 Service Pack 2

Changes delivered to Network Management	Solution
In the previous release, when you tried to uninstall Network Management Release 5.2, the system prompted you with a message requesting a CD image. You had to insert the Network Management 5.2 CD to complete the uninstallation.	With this release, you do not require the CD.
In the previous release, when you tried to uninstall Network Management Release 5.2 installed on Windows Vista, the system displayed the **Modify Firewall** screen in the uninstallation wizard.	In this release the system does not show the **Modify Firewall** screen during uninstallation.

Network Management now supports Microsoft Windows Vista Service Pack 2.	
Network Management Console (NMC) with VoIP System View	
NMC no longer uses the native ping to discover devices. In keeping with the modified design, you can discover devices in the subnet using just SNMP.	With this release, the application does not use the native ping step as a required input value to the SNMP discovery step. **Note:** The NMC map shows the status of the devices as **Unreachable** for those devices that are IP reachable but not SNMP reachable.
In the previous release, the **SNMP** user option in the **Add/Modify Device** dialog box in NMC displayed the default user **root**. The CLI user **root** is a default user preconfigured in Secure Access Administration. Therefore the user role was carried over to the SNMP users option in the **Add/Modify Device** dialog box. This must not happen because **root** is not a SNMP V3 user, unless you configure it explicitly.	This has been fixed in this release.
From this release, you cannot switch between maps in NMC when discovery is in progress.	
In the previous release, the **Quick Log Viewer** in NMC did not show the correct logged-in user in the **User** column.	The logged-in user now appears in the **User** column.
In the previous release, Network Management did not close the two SSH sessions that NMC established during the IP Phone Data discovery phase. So, if you ran 7-8 discoveries without restarting the cvserver, the Communication Manager login sessions got exhausted as the maximum number of sessions allowed is 16. **Workaround**: You had to restart the cvserver before the start of the next discovery.	This has been fixed in this release.

In the previous release, if you right-clicked any device from the **Device Type** or **VoIP System View** tab of NMC, the system highlighted both the menu items, the **Device Manager** and the **Web** option in the popup menu. NMC highlighted the **Device Manager** option in the popup menu for devices that did not support device manager. For example, Communication Manager servers. NMC also highlighted the **Web** option in the popup menu for devices that did not support web. For example, Media Gateways.	In this release, NMC highlights the Device Manager and Web options only for supported devices.
In this release, NMC discovers the **9670G** phone connected to the Communication Manager. NMC displays the phone information in the **Port Connection Table** when you select the Communication Manager device from the System View, the Device Type View, or the Subnet View.	
In this release, NMC supports **I55** release **IEE6**.	
In the previous release, sometimes the VoIP System View did not respond during the discovery process. The problem was observed during the phone discovery phase.	This has been fixed in this release
Support for new I55 device type and new I55 alarms • Network Management Console supports the a new I55 device type, **ACB IEE3** • Network Management Console supports new traps of the I55 software	
Software Update Manager (SUM)	
In previous releases, Software Update Manager did not block the download of unsupported firmware like 96xx phones and 96xx settings file on Gx50.	Now Software Update Manager blocks the download of unsupported firmware and settings file.
In previous releases, the Software Library Files table could not be sorted like in the device table.	You can now sort the Files on the Software Library table.

The Versions.xml file has been updated with the latest phone releases.	Now ASCA reports shows correct recommendations for IP Phones.
In previous releases, when a Communication Manager service pack or patch was attached to the Software Update Manager Library, you had to associate that particular Communication Manager server type to it.	This problem has been fixed.
Software Update Manager supports Connection Preserving COLD Updates (CPU) on Communication Manager duplex servers.	Communication Manager 5.2.1 supports COLD patch, SUM has been enhanced to support this feature in Communication Manager.
Software Update Manager should also work with e-mail ID instead of Global SSO (single sign on) for the Software and Firmware Access Policy (SFAP).	Now SUM works with e-mail ID for SFAP.
In previous releases, Software Update Manager displayed the wrong details about the firmware in the Software Library.	SUM now displays only the correct details.
Secure Access Administration	
In the previous release, online help was not available for Sync Passwords.	Online help is now available for Sync Passwords.
Device Manager	
The **Protocol Status** tab in the G430 and G450 Device Manager needs to have the **ARP Inspection** field.	The **ARP Inspection** field has been added to the **Protocol Status** tab.
Communication Manager Branch Edition – Central Manager (CMBE - CM)	
In the previous release, if you tried to restart a job after stopping it in between, it did not run immediately. The job status changed from **ANNULATED** to **ACTIVE**, but the execution of the job took around 45 minutes.	This has been fixed in this release.
In the previous release, the **Log Viewer** and the **Alarm Manager** GUI pages took a long time to load. This issue mostly happened after server restart.	This has been fixed in this release.

In the previous release, if you added an **Abbreviated Dialing Group** in the Communication Manager Branch Local Manager, or if you made any changes from Communication Manager Branch Local Manager, the **Incremental Synchronization** failed for that object.	This has been fixed in this release.
In this release, the number of **OLG** members for i120 and G450 branches has increased from 40 to 96.	
In this release, the length of the **farEndDomain** used in SIP trunk has changed from 40 to 63.	
From this release, you can see the logout and session expiration logs in the **Log Viewer** utility of the CMBE-CM application.	
In this release, CMBE-CM supports the **Trunk Flash Hook** button. CMBE-CM supports **Flash** in **Station** and **Feature Access Codes** templates. In the Station template, the **Flash** button is added to the relevant set-types. **Flash FAC** has been added to the **Flash Access Codes** templates **Note:** The **Flash** button is not supported on **SIP** phone.	
In the previous release, CMBE-CM did not register various actions in the Log Viewer (audit logs).	In this release the CMBE-CM registers the following events in the Log Viewer (audit logs) • Full sync starting • Full sync finished • Occurrence of incremental sync with details of the changes made • User-initiated operations • Start of a user-initiated job • End of a user-initiated job

In this release CMBE-CM supports expansion module for **9630** phones.	
In this release CMBE-CM supports a new call-type **Operator** in the **Dial Plan** template.	
In the previous release, CMBE-CM displayed incorrect values for the **Max Concurrent Call** field in the **SIP Trunk template**.	This has been fixed in this release. The CMBE-CM now displays the correct values as: • **1-180** for G450 • **1-30** for i40 and i120

Integrated Management - Network Management 5.2 Service Pack 1 fixes

Table 4 lists the changes delivered to Integrated Management - Network Management 5.2 Service Pack 1.

Table 4: Changes delivered to Network Management 5.2 Service Pack 1

Changes delivered to Network Management	Solution
In the previous release, if you upgraded from Network Management 5.0 SP3 with **Communication Manager & Branch Gateway only** installation to Network Management 5.2, the filters for Distributed Office were seen in the Configuration Backup and Restore Manager (CBR) application.	This has been fixed in this release. The filters are not visible in this release.
In the previous release, if you upgraded to Network Management 5.2 **Communication Manager Branch Edition only** installation (upgrade path: 4.0 > 5.0 > 5.2), the Provisioning and Installation Manager for Branch Gateways link was visible on the Integrated Management launch page. This link should not have been present.	This has been fixed in this release. The link does not appear now.

Network Management Console (NMC) with VoIP System View	
In the previous release, when you added CM from the **CM Servers Passwords** tab of **File > Options** window the port shown was 5022, but in the cmxml.xml file it was being written as 5023.	This has been fixed in this release
The launching mechanism has changed for EPICenter 7.0. The new launch mechanism is JWS (Java Web Start) based.	To accommodate this, the launching mechanism of EPICenter from Network Management Console has been changed in this release.
In the previous release, the Polycom GMS link was missing from the **Tools** menu of the Network Management Console application after some upgrade paths. If you were upgrading ENM from 4.0 (upgrade path: 4.0 > 5.0 > 5.2) the link was present in 5.2, but if you were upgrading from 5.0 (upgrade path: 5.0 > 5.2), the link was not present in 5.2.	This has been fixed in this release.
Support SSO for EPICenter 7 This release supports the SSO (Single Sign-On) mechanism for EPICenter 7. The SSO mechanism uses the existing Network Management Console session for authentication.	
ENM Backup Utility	
In the previous release, the backup name was not validated before submitting the job in the ENM Backup Utility application. For example, if you provided an invalid name, such as ***** in the **Backup Name** field, and clicked **Submit**, the backup failed because of the invalid name. The name was not validated before you submit the job.	This has been fixed in this release. If you enter an invalid backup name, the **Next** button remains inactive and you cannot proceed unless you give a valid name for the backup.
In this release, a new button **Set as Default Options** is added to the **Select Backup Destination** screen of the ENM Backup Utility application. You can use this button if you have not set the default backup options in the **File > Options** window in the ENM Backup Utility. The parameters entered in the **Select Backup Destination** screen is set as default when you click the **Set as Default Options** button.	

Device Manager	
In the previous release, the Welcome page link for G430 was broken. The link opened to an unrelated support site instead of the appropriate page.	This has been fixed in this release. The hyperlink on the launch page now points to the G430 page on the Avaya Support Site.
In the previous release, the **DHCP Config Pool** tab in the G430 Device Manager closed when you selected the refresh button.	A fix is included for the GUI Refresh of the **DHCP Pool Config** tab. DHCP Config. pages now get refreshed without closing or minimizing abruptly.
In the previous release, the **configuration** tab of the DHCP Pool in the G430 Device Manager was not visible when you clicked over it.	This has been fixed in this release. The configuration tab is now visible when you click over any of the pool created.
In the previous release, the context sensitive help (Help-On) was not working for the following topics in G430 Device Manager: – Get/Set toolbar – Switch Connected Addresses – Port Redundancy Dialog – Port Mirroring – VLAN conf dialog – Port redundancy wizard The system displayed an Http 404 NOT Found Error.	The context sensitive help for following components in G430 Device Manager is now available for: – Get/Set Toolbar – Port Redundancy Dialog – Port Mirroring – VLAN Configuration Dialog **Note:** Context Sensitive help is not available for “Port Redundancy Wizard” and “Switch Connected Addresses.”.
In the previous releases of G450 Device Manager, the hardware vintage Suffix for G450CR was not validating the version and this affected detection of difference between G450 and G450CR.	Verification of Hardware Suffix is done in G450 Device Manager to detect G450-CR.

Software Update Manager	
In the previous release, when you tried to upgrade the failed Communication Manager, the **Status** column displayed the failure message even after the Software Update Manager had updated the version information.	This has been fixed in this release.
In the previous release, the **Last Refresh Time** column failed to get updated when you clicked the **Refresh selected download targets** column on the **Communication Manager branch Edition, Gateways, Data Switches and TN Circuit Packs** tab.	This has been fixed in this release.
In the previous release, the usage of memory and CPU went up heavily when the **Retrieve from web** tab was used to retrieve the multiple firmware or softwares.	This has been fixed in this release.
In the previous release, the **Reset after download** check box was often overlooked while upgrading the Media Gateways	The **Reset after download** check box has been placed next to the **Submit** Job button on the **Schedule Download** panel. You will not fail to select this check box now.
In the previous release, the Software Update Manager used the **SSO Key** and **SFAP Key** for Certificate validation.	The Certificate validation in SUM will not depend on pre-installed keys.
In the previous release, when you clicked the **Add Image** button, the **software type** dropdown displayed the **Cornerstone** and **Audix** patch in the Software Update Manager.	This has been fixed in this release. These patches are for the ASCA Report which supports the CMM. Avaya recommended that you use the latest patch.
In the previous release, when you download the TN boards the proxy list displayed the non administered C-LAN boards in the Software Update Manager.	This has been fixed in this release.

Secure Access Administration	
In the previous release, the SNMPv3 user **initial** was being displayed in the user list of the Secure Access Administration application. This user when used for discovering devices could cause incorrect discovery results.	This user has been removed from Secure Access Administration. However this user can be explicitly added later, if needed.
In the previous release, the Secure Access Administration logs were not created in the Network Manager Console's Quick Log.	Now the Secure Access Administration creates the logs for important activities and events in the Quick Log.