Avaya Integrated Management Release 6.0

Network Management Configuration

Issue 1
June 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

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

Preface

This section includes the following topics:

Purpose - A description of the goals of this manual.

Prerequisites - A description of the prerequisite knowledge required to use the Avaya Network Management applications.

Intended audience - The intended audience of this manual.

Conventions used in this book - The typographical conventions used in this manual.

Support resources - A description of the support resources available.

Product documentation - Instructions on how to access the Avaya Integrated Management documents on the web.

Purpose

The purpose of this book is to provide the following information:

- A broad overview of the Avaya Network Management applications.
- Procedures that must be performed after the Avaya Network Management applications are installed.
- Instructions on how to start managing your network using the Avaya Network Management.
- Procedures that must be performed after the Avaya Network Management with IP Office Manager software is installed.
- Instructions on how to get started managing your network using Avaya Network Management with IP Office Manager.
- Instructions on how to provision IP Office devices in your network using Avaya Provisioning and Installation Manager for IP Office.
- Instructions on how to provision media gateways in your network using the Avaya Provisioning and Installation Manager.

Prerequisites

Network managers should be knowledgeable about network-wide tasks, such as monitoring switching, configuring VLANs, and setting up rules to enhance quality of service. The Network managers should also be knowledgeable about managing specific network devices.

Intended audience

This book is written for network managers familiar with network management and its fundamental concepts.

Conventions used in this book

The following typographical conventions are used:

- **Bold** type is used to indicate selections from menus, dialog box, windows, buttons and tabs in a window, and the **Enter** key on the keyboard. It is also used for emphasis.
- **`Courier bold`** font is used to indicate commands that you type.
- ***`Courier bold italic`*** font is used to indicate variable information within the commands that you type.
- `Courier` font is used to indicate information that appears as command results, or ouput.
- Arrows indicate options that you select from cascading menus; for example, Select **File > Open** means choose the **Open** option from the **File** menu.

Support resources

Avaya provides a variety of planning, consulting, and technical services. The following sections describe the resources and services that are available.

Avaya Professional Services

The Avaya Professional Services (APS) team of Avaya Integrated Management (AIM) consultants offers customers the following services:

- Platform-readiness verification
- AIM architectural planning, design, and overview
- Remote turnkey implementation and installation
- AIM server configuration
- Customer acceptance verification
- Custom on-site services
- Onsite and remote knowledge transfer

The APS Data Group consists of the following teams:

- **Avaya Integrated Management Consultants**

  The Avaya Integrated Management (AIM) consulting team offers planning, design, implementation, consulting, and knowledge transfer services for the entire Avaya Integrated Management Suite. This includes ASA, Val Manager, NMC with SUM, MSA, and FPM. The thrust of the APS team is to bring the correct methodology to these complex application deployments that span various regions, and to provide continuity to the overall project. Through proper integration and consulting, our customer can leverage the AIM suite to lower total cost of ownership, and proactively manage their VoIP network comfortably and confidently.

- **Data Network Implementation Engineering**

  The Data Network Implementation Engineering (formerly RNIS) team implements and upgrades or upgrades existing or new data networks. This team analyzes the network design requirements and performance expectations of the customer. The team then creates the hardware and software installation specification used to implement data devices that include Cajun, VPN, Wireless LAN, Secure Gateways, Extreme, Juniper, and multivendor data equipment.

The APS Data Group provides support on a contract basis. Contact your local Avaya Account Team or Business Partner to purchase any implementation offer from the team. For more information, refer to Table 1: Customer-Accessible Resources on page 11, or contact Jon Machak at 248-213-3788 or machak@avaya.com.

Avaya Global Services Delivery

Avaya Global Services Delivery (GSD) provides support to the Avaya Integrated Management client teams, field technicians, and customers. The GSD will bill customers for support on a time and materials basis if the following conditions exist:

- Customers do not provide remote access.
- Customers do not have a current maintenance agreement.
- Customers do not procure and install the required systems and software as defined in the Integrated Management Services Support Plan.
- Customers request support that is outside the purchase agreement.

The GSD does not support hardware or software that customers purchase from third-party vendors.

Avaya Global Technical Services

Avaya Global Technical Services answers customer calls about products in Avaya Integrated Management. The team will either answer your questions directly or connect you with an associate who can answer questions about the products.

Customized Management Solutions for Avaya Integrated Management

The Integrated Management Product Team understands the customer's needs and is focused on customer satisfaction. For information on contact information, see Table 1: Customer-Accessible Resources on page 11. The Product Team will assist customers with Avaya Integrated Management projects and will provide:

- **Project Management** — An Integrated Management project person will work with the customer to access configuration and customization requirements for any or all applications within each Avaya Integrated Management offer. If custom work is required, the evaluation will include a proposed statement of work and price. Note that this offer is *not* intended to provide installation for customers that choose to implement Integrated Management applications using Avaya Services or third-party implementation services.
- **Training** — Basic training can be performed remotely using an interactive medium to display the applications and a conference bridge for audio. On-site training can be customized to meet the customer's needs. Customized training will focus on application functionality that is relevant to the customer and provide focused knowledge transfer to facilitate application-specific training.

Avaya contact information

Table 1 provides contact information that you may use if you need assistance during the process of installing, configuration and setting up Avaya Integrated Management.

Table 1: Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://www.avaya.com/support
Network Management Software Systems Support (NMSSS)	+1 800 237-0016
Avaya Professional Services (APS) Consulting	+1 800 730-9108, prompt 3
Integrated Management Product Team	Send email to: mjk@avaya.com
Toll Fraud Intervention	+1 800 643-2353, prompt 1

Product documentation

The latest version of Avaya Integrated Management product documentation, including this book, is available from the Avaya Support Web site. To view or download these books from the Web, you must have access to the Internet, an Internet browser, and the Adobe Reader. The Adobe Reader is available from http://www.adobe.com. For information on how to view or download these books, see How to access books on the web.

How to access books on the web

To view or download books from the Avaya Support Web site, follow these steps:

1. Go to http://www.avaya.com/support.
2. Click **Documentation**, and then select the document category you want to view.
3. Click the letter **I** in the alphabet listing.
4. Locate **Integrated Management(All Offers)** and click the corresponding link.
5. Select the document you want to view from the available list.

Chapter 1: Overview

Avaya Network Management

The Avaya Network Management is part of the Avaya Integrated Management, which provides a complete set of tools and an applications platform. All of the tools in the Avaya Integrated Management are accessible through a common Web-based user interface to facilitate system and network management.

The Avaya Network Management applications and device managers are SNMP-based network management applications. There are different types of applications to fill different network management needs.

Note:

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Avaya Network Management applications

The Avaya Network Management applications are network-wide applications that allow you to manage Avaya media gateways and Avaya LAN and backbone switches in your network as a whole. These applications allow you to configure Avaya media gateways and VLANs, monitor switching, set up rules to enhance quality of service, and perform other important network tasks. For example, one Avaya Network Management application is the Avaya System Monitoring (SMON) Manager, which provides advanced switch monitoring. (Avaya Integrated Management includes a 90-day trial version of the Avaya SMON Manager, and you can purchase a license to continue use beyond 90 days.) The Avaya SMON Manager monitors the Ethernet switching fabric and gives you a complete top-down view of all switched traffic across your network.

Other network-wide applications includes the Avaya Configuration Backup Restore for backup and restore of network devices and the Avaya Software Update Manager for automatically updating your network devices with the most up-to-date software. A further description of the Avaya Network Management applications is provided in the following sections. For more details about a specific application, refer to the application's user guide.

Note:

The Avaya Network Management applications do not support devices that use Network Address Translation (NAT) addresses. Network Management Console client and server connections, with NAT in between is not supported too. Although the Avaya Network Management Console may detect devices that are configured using NAT, some Network Management framework features are not available. However, IP Office devices behind a NAT server will be supported if the IP Office device is the only device that can access the network and be reachable from the network.

Note:

You cannot install SMON Manager if you perform the first installation with Network Management 6.0. You can get SMON Manager only if you upgrade to Network Management 6.0 from a previous version.

Avaya Software Update Manager

The Avaya Software Update Manager downloads software to managed Avaya devices. The Avaya 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. You can use the Avaya Software Update Manager to retrieve a new release from Avaya's Web site, store it on your hard disk, and subsequently download it to the appropriate device.

Avaya Network Management Console

The Avaya Network Management Console is an application that allows you to view the devices in your network, the voice network hierarchy, and the port connections. Using advanced network searches, the Avaya Network Management Console helps you build, maintain, and display a centralized list of hosts discovered in the network. The list, which you can print or export, provides the host MAC and IP addresses and device port connectivity. The Avaya Network Management Console helps you rapidly locate a host or switch port on the network and find duplicate IP addresses in the network. You can also import connections into the Avaya Network Management Console.

The Avaya Network Management Console provides a platform from which you can launch applications to manage network devices and monitor the traffic on your network. This application uses a client/server architecture, allowing multiple users to access the Avaya Network Management Console simultaneously. Web-based technology provides a method for accessing and managing your network from any computer with Internet access.

Avaya Network Management Console with VoIP System View is the platform and the focal point from which all network management activity is initiated. The Network Management Console with VoIP System View automatically discovers devices on the network and displays them in an intuitive, hierarchical navigation tree. Different views of the tree allow the administrator to view the network by IP subnet, by device type, or logically by voice systems.

Elements in the navigation tree are color coded to indicate fault status. Network Management Console also serves as a focal point for viewing fault event notifications, which are collected and displayed in the Event Browser. The administrator can also configure actions to be executed upon receipt of particular types of notifications.

Network Management Console serves as a launch point for all applications included in the Network Management with IP Office Manager offer. Applications can be easily launched from the menu bar, either globally, or focused on a device selected in the navigation tree. Launching IP Office Manager for a particular device presents additional information not presented in the system view. Network Management Console also provides built-in capabilities to launch a telnet or web browser session on the selected device in the tree.

IP Office Manager

Internet Protocol (IP) Office Manager is an application for viewing and editing an IP Office system configuration. IP Office Manager is an off-line editor. This means that it receives a copy of the current IP Office system configuration. Changes are made to the copy and then sent back to the IP Office system for those changes to become active. This means that changes to the active configuration in the system that occur between Manager receiving and sending back the copy may be overwritten. For example this may affect changes made by users through their phone or voicemail mailbox after the copy of the configuration is received by Manager.

IP Office Manager performs a number of functions for IP Office systems.

- **Configuration Settings Editor** - In configuration mode, Manager is used to edit configuration settings for IP Office systems. Those settings control the call and data function that the IP Office system provides to users and callers. Refer to the Configuration Mode section.
- **Security Settings Editor** - In security mode, Manager is used to edit the security settings of IP Office 3.2+ systems. Those settings are used to control user access to the configuration settings of the IP Office. Refer to the Security Mode section.
- **Upgrade Wizard** - The Upgrade Wizard is a component of Manager used to upgrade the firmware run by the control unit and expansion modules within an IP Office system
- **Embedded Memory Card Management** - For systems with a compact flash card installed, the IP Office 4.2+ Manager can be used to view and manage the files stored on the card. This is accessed through the File | Advanced | Embedded File Management... .
- **BOOTP Server** - Manager acts as a Bootstrap Protocol (BOOTP) server, providing software files in response to BOOTP requests from IP Office systems. This task is required for maintenance. This function can be switched off if not required.
- **Time Server** - Manager acts as an Internet Time server (RFC868), providing the time in response to requests for IP Office systems. This function can be switched off if not required.

Avaya Provisioning and Installation Manager for IP Office

Avaya Provisioning and Installation Manager for IP Office provides the capability to remotely configure IP Office systems on a network-wide basis. It provides integrated network system views that ease centralized configuration tasks, especially provisioning and installing large numbers of IP Office system devices simultaneously.

Through the use of wizards that prompt you for required information, Avaya Provisioning and Installation Manager for IP Office enables you to:

- Create and edit templates and device profiles.
- Import and export device profiles and templates.
- Create a template by importing data from an electronic pre-installation worksheet (EPW).
- Distribute a template through bulk provisioning to a group of devices.
- Send a profile to a device and make a choice to distribute now, schedule for a later, or make pending.
- Provide backup and restore of system configurations.
- Create up to four Auto Attendant templates that define announcements for particular time slots. The Auto Attendant templates can include WAV files.
- Interact with IP Office Manager to define templates
- Define dynamic groups and static groups of devices

Avaya Configuration Backup Restore

The Avaya Configuration Backup Restore allows you to save device and module configurations and apply them to devices and modules across the network. This provides a mechanism for backup and restore of network devices, as well as the ability to replicate device and module configurations onto other devices.

Avaya SMON Manager

You cannot install SMON Manager if you perform the first installation with Network Management 6.0. You can get SMON Manager only if you upgrade to Network Management 6.0 from a previous version.

The Avaya SMON Manager is a collection of applications that work together with the other Avaya Network Management components to provide a full spectrum of in-depth monitoring of switch traffic and network performance. The Avaya SMON Manager consists of a software console application on a workstation and remote monitoring probes in network devices that support SMON.

The Avaya SMON Manager console constantly communicates with the SMON devices on your network. The console uses SNMP to gather information from the devices. The Avaya SMON Manager provides a suite of powerful graphic display tools to view this information.

The Avaya SMON Manager provides you with detailed analysis of the traffic flow on your switched network, from a global view down to a specific host, and from total MAC layer traffic down to a specific application protocol — all in real-time.

SMON monitoring provides the following information:

- A global view of traffic for all switches on the network.
- An overall view of traffic passing through a specific switch.
- Detailed data about the hosts transmitting packets or cells through a switch.
- An analysis of traffic passing through each port connected to a switch.

Avaya Provisioning and Installation Manager for Media Gateways

The Avaya Provisioning and Installation Manager provides the capability to remotely configure Avaya media gateways on a network-wide basis. It provides integrated network system views that ease centralized configuration tasks, especially provisioning and installing large numbers of gateways simultaneously.

Using wizards that prompt you for required information, the Provisioning and Installation Manager enables you to:

- Create templates and device profiles to use later.
- Import and export device profiles and templates.
- Save templates and device profiles with a completed status or incomplete status where non-required information can be added at a later time.
- Copy configuration templates and device profiles to create placeholders for different parameters.
- Create a template from scratch or import data from an electronic pre-installation worksheet (EPW).
- Distribute a template through bulk provisioning to a group of devices.
- Send a profile to a device and make a choice to distribute now, schedule for a later, or make pending.
- Configure G250, G350, G430, and G450 media gateways with Standard Local Survivability (SLS) updates that include parameters such as automatic route selection (ARS) rules and dial plans. Survivability provides basic call processing controller functionality in the event that a main controller or LSP is unavailable.

- Store notes about templates and device profiles.

The Provisioning and Installation Manager supports the following media gateways:

- Avaya G250
- Avaya G250–BRI
- Avaya G250-DS1
- Avaya G250-DCP
- Avaya G350
- Avaya G430
- Avaya G450
- TMG550

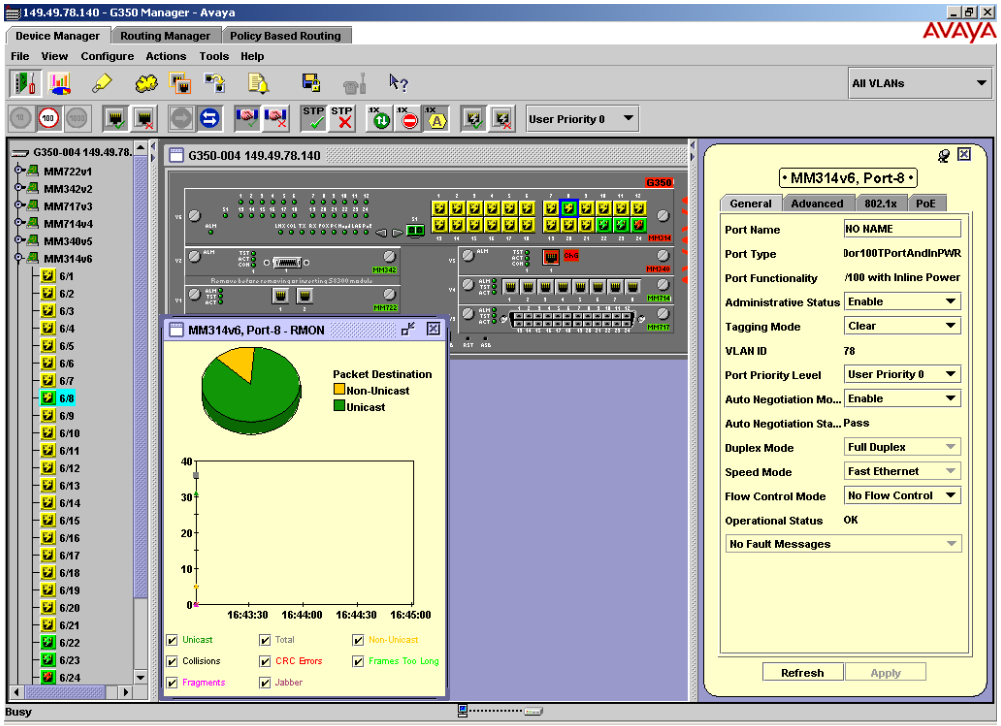
You can perform initial gateway configuration in the following ways:

- In a staging environment using a Local Area Network (LAN) to simulate the customer LAN
- On the customer premises with the assumption that either LAN connectivity exists to Provisioning and Installation Manager or Wide Area Network (WAN) connectivity has been provided through an external router to the Provisioning and Installation Manager.

Device Managers

Device managers are applications that are tailored to manage and monitor Avaya media gateways and LAN and backbone switches. Device managers allow you to set up, configure, monitor, manage, and diagnose all Avaya network devices. The Device Manager provide a real-time view of each device, called the “chassis view.” The chassis view uses color coding to indicate individual port, module, and LAG status. You can use the device manager to configure port, LAG, and VLAN settings, port security, redundancy modes, and all other device parameters. An example of an Avaya device manager is shown in Figure 1.

Figure 1: Avaya Device Manager



• MM314v6, Port-8 •

General | Advanced | 802.1x | PoE

Port Name: NO NAME
Port Type: 0or100TPortAndInPWR
Port Functionality: /100 with Inline Power
Administrative Status: Enable
Tagging Mode: Clear
VLAN ID: 78
Port Priority Level: User Priority 0
Auto Negotiation Mo...: Enable
Auto Negotiation Sta...: Pass
Duplex Mode: Full Duplex
Speed Mode: Fast Ethernet
Flow Control Mode: No Flow Control
Operational Status: OK
No Fault Messages

Refresh | Apply

In addition, each device can be monitored using Avaya's Device SMON applications. Device SMON provides switch monitoring capabilities, as well as graphs and pie charts displaying traffic types on ports, VLANs, and switches.

NM Backup Utility

The NM Backup Utility is used to back up multiple configuration files, database and application data of the Network Management Console, IP Office Manager, and Provisioning and Installation Manager (PIM) for Gateways and PIM for IP Office applications. You can choose to back up one or more applications as part of a backup job. This wizard helps you to setup a new backup job or edit an existing one.

You can run the backup job immediately or schedule it to run later. When the backup operation is complete, the utility creates a compressed archive and a text file with essential information about the contents of the archive. The text file is only for your convenience and is not needed during restore operation. You can choose to store the backup archive on a FTP server or locally on the NM server while setting up the job.

The utility backs up various configuration files and application data which are essential to restore the NM server in case of an unrecoverable error. You need not recreate all the administered settings when you bring up the NM server. Instead you can restore the information from the backup archive stored on the NM or remote FTP server. Also, if you are installing a Service Pack, it is recommended that you take a backup before installing the Service Pack.

For NMC, back up includes discovery configurations, Network Map Definitions, CM Server passwords and licensing information and various other files. The NMC backup also includes the settings for the Secure Access Administration, Configuration Backup Restore and Software Update Manager applications.

PIM for Gateways and PIM for IP Office back up add their configuration files as well. The database back up includes the Network Management Console, AIM-Admin, PIM, and User Admin databases.

Installation specific information such as SSO Configuration files, licensing information, IM application jobs, environment and binary files (software libraries) are also bundled with the backup archive.

For information on the NM Backup Utility, see *Avaya Integrated Management Release 6.0 Network Management Console User Guide*.

NM Easy Restore Utility

The NM Easy Restore Utility is used to restore the backup taken by the NM Backup Utility. Enter the path of the backup archive stored either on the NM or FTP server during backup to restore the data present in it.

For information on how to use the NM Backup Utility and NM Easy Restore Utility, refer to the *Avaya Integrated Management Release 6.0 Network Management Console User Guide*.

Chapter 2: Post installation tasks for Avaya Aura™ Communication Manager

Overview

This chapter provides information on the tasks you should perform after installing the Avaya Network Management applications.

- Configuring the Avaya Aura™ Communication Manager Servers – Information on configuring the Avaya Aura™ Communication Manager servers to view them properly on Network Management Console.
- Configuring SNMP options in Network Management – Information on configuring SNMP for the Avaya Network Management.
- Entering the Avaya SMON Manager license – Information on entering SMON licenses for the Avaya Network Management applications.
- Configuring Proxy settings (Optional) – Information on configuring the Avaya Network Management to work through a proxy server.
- Configuring the Web Server (Optional) – Information on configuring a custom web server to work with the Avaya Network Management.
- Configuring the Web Server for Polycom GMS support (Optional) - Information on configuring the web server to support Polycom GMS.
- Configuring FTP (Optional) – Information on configuring an FTP server to work with the Avaya Network Management.
- Changing the Port Numbers used by the Network Management applications – Information on how to change the TCP port numbers of the Network Management server and client applications.
- Configuring the Software Update Manager for domain users – Information on configuring domain users in the Software Update Manager.

For instructions on how to install the Avaya Network Management applications on a Windows server, refer to the *Avaya Integrated Management, Release 6.0, Network Management Installation and Upgrade* document.

Configuring the Avaya Aura™ Communication Manager Servers

You must configure each Communication Manager in order to see the Communication Manager servers properly within the Avaya Network Management Console. The Avaya Network Management Console provides a simplified, wizard-driven process to automate this setup. The Network Discovery Wizard is offered during the installation process and may also be activated at any time from the Avaya Network Management Console menu under **Actions**. The wizard ensures that SNMP is properly configured and activated on the Communication Manager servers and that the appropriate credentials for accessing these servers are stored within the Avaya Network Management Console for use during the discovery process and beyond.

Use of the Network Discovery Wizard is strongly encouraged. For information on running the Network Discovery Wizard, see Discovering the Voice Network on page 35. However, if you choose to perform the configurations manually, follow the instructions provided under Communication Manager 3.1 and later or Communication Manager 3.0 and earlier below.

Communication Manager 3.1 and later

Perform the following steps for each Communication Manager Release 3.1 and later:

1. From the Internet Explorer, enter the IP address of the Communication Manager server, and press **Enter**.
2. Log into the Communication Manager server.
3. Click **Launch Maintenance Web Interface**.

   The system displays the **Integrated Management Maintenance Web Pages** page.
4. Click **SNMP Agent Status** in the left panel.

   The system displays the **SNMP Agent Status** page.
5. On the SNMP Agent Status page, ensure that the Master Agent is **Down**. If it is not, click **Stop** to turn the Master Agent off.
6. Click **SNMP Agents** in the left panel.

   The system displays the **SNMP Agents** page.
7. On the SNMP Agents page, do the following:

   a. Under the **IP Addresses for SNMP Access** section, do one of the following:

      - Select the **Any IP address** option for all IP addresses to have SNMP access.
      - Select the **Following IP addresses** option, and enter the IP addresses to which you want to give SNMP access.

b. Under the **SNMP Users/Communities** section, do one of the following:

  - Check **Enable SNMP Version 1**, and enter the community names.
  - Check **Enable SNMP Version 2c**, and enter the community names.
  - Check **Enable SNMP Version 3**, and enter the user name and password for the read-only user and read-write user.

c. Click **Submit**.

8. Click **SNMP Traps** in the left panel.

   The system displays the **SNMP Traps** page.

9. Click **Add**.

   The system displays the **Add Trap Destination** page.

10. On the Add Trap Destination page, do the following:

    a. Ensure that the check box for **Check to enable this destination** is selected.

    b. Enter the IP address of the management station, and then do one of the following:

      - Check the **SNMP version 1** option, and enter the community name.
      - Check the **SNMP version 2c** option, ensure **notification type** is **trap**, and enter the community name.

    c. Click **Add**.

11. Click **SNMP Agent Status** in the left panel.

    The system displays the **SNMP Agent Status** page.

12. Click **Start** to turn the Master Agent on.

13. Click **Test Trap** in the left panel.

    The system displays the **Test Trap** page.

14. Click **Test** to generate a test trap.

15. Click **Firewall** in the left panel.

    The system displays the **Firewall** page.

16. On the Firewall page, do the following:

    a. Ensure the input and output check boxes for port 161 and port 162 are selected.

    b. Click **Submit**.

17. Open the Network Management Console application.

18. Select **File > Options**.

19. Select the **CM Servers Passwords** tab.

20. Enter the IP address, user name, and password for each Avaya Aura™ Communication Manager server.

21. Select the **SNMP Access** tab.

22. Set up the SNMP rule for the Avaya Aura™ Communication Manager server IP addresses.

    Note:

    The SNMP time-out value must be set to 60 seconds (60000), and the retries value must be set to 1.

23. Ensure that the test trap generated in Step 14 was received by the Network Management Console.
24. Run Network Discovery. For information, see Discovering the Voice Network on page 35.

Communication Manager 3.0 and earlier

Perform the following steps for each Communication Manager Release 3.0 and earlier:

1. From the Internet Explorer, enter the IP address of the Communication Manager server, and press **Enter**.
2. Log into the Communication Manager server.
3. Click **Launch Maintenance Web Interface**.

   The system displays the **Integrated Management Maintenance Web Pages** page.
4. Click **SNMP Agents** in the left panel.

   The system displays the **SNMP Agents** page.
5. On the SNMP Agents page, do the following:

   a. If the **Master Agent status** is **Down**, click **Start** to turn the Master Agent on.

   b. Under the **IP Addresses for SNMP Access** section, do one of the following:

      - Select the **Any IP address** option for all IP addresses to have SNMP access.
      - Select the **Following IP addresses** option, and enter the IP addresses to which you want to give SNMP access.

   c. Under the **SNMP Users/Communities** section, do one of the following:

      - Check **Enable SNMP Version 1**, and enter the community names.
      - Check **Enable SNMP Version 2c**, and enter the community names.
      - Check **Enable SNMP Version 3**, and enter the user name and password for the read-only user and read-write user.

   d. Under the **Communication Manager SNMP Agent** section, select **Enable Agent**, and enter any string, such as abcdefgh, for the **Agent ACP Login** password.

   e. Click **Submit**.
6. Click **SNMP Traps** in the left panel.

   The system displays the **SNMP Traps** page.

7. Click **Add**.

   The system displays the **Add Trap Destination** page.

8. On the Add Trap Destination page, do the following:

   a. Ensure the check box for **Check to enable this destination** is selected.

   b. Enter the IP address of the management station, and then do one of the following:

      - Check the **SNMP version 1** option, and enter the community name.
      - Check the **SNMP version 2c** option, ensure **notification type** is **trap**, and enter the community name.
      - Check the **SNMP version 3** option, ensure **notification type** is **trap**, and enter the user name and password.

   c. Click **Add**.

9. Click **Firewall** in the left panel.

   The system displays the **Firewall** page.

10. On the Firewall page, do the following:

    a. Click **Advanced Setting**.

    b. Ensure the input and output check boxes for port 161 and port 162 are selected.

    c. Click **Submit**.

11. Open the Network Management Console application.

12. Select **File > Options**.

13. Select the **CM Servers Passwords** tab.

14. Enter the IP address, user name, and password for each Avaya Aura™ Communication Manager server.

15. Select the **SNMP Access** tab.

16. Set up the SNMP rule for the Communication Manager server IP addresses.

    Note:

    The SNMP time-out value must be set to 60 seconds (60000), and the retries value must be set to 1.

17. Run Network Discovery. For information, see Discovering the Voice Network on page 35.

Configuring SNMP options in Network Management

The Avaya Network Management Console must be configured with SNMP parameters in order to successfully discover and communicate with devices in your network. SNMPv1 uses community strings to authorize read-only or read-write access to a device. SNMPv3 is more secure and validates users with a user name and password. In addition, SNMPv3 offers the option of encrypting all data transferred between the applications and the network devices.

For details on configuring SNMPv1 and SNMPv3 credentials for use with your network devices, see the *Avaya Network Management Console User Guide*. If you use SNMPv3 in your network devices, you should also refer the *Avaya Secure Access Administration User Guide*.

Entering the Avaya SMON Manager license

The Avaya Network Management offer provides a 90-day trial version of the Avaya SMON Manager. You have the option of purchasing the SMON Manager license key. This key is required to fully activate and use the Avaya SMON Manager beyond the 90-day trial period on a permanent basis.

The first time you launch Avaya SMON Manager, you are prompted for the license key. The license key allows unlimited use of Avaya SMON Manager. Enter the license key if you have purchased one. If you have not purchased a license key, press **Enter** when you are prompted for the license key. You will be able to use Avaya SMON Manager for the 90-day trial period.

To purchase a license key, contact your Avaya representative.

Configuring Proxy settings (Optional)

If your network has a non-permissive firewall, you must configure Avaya Network Management to work with your proxy server. This enables the Avaya Software Update Manager’s Analyze and Retrieve capability from the Web functions.

The process to configure Avaya Network Management to work with your proxy server was simplified beginning in Avaya Network Management Release 4.0. It is no longer necessary to edit property files. Instead, the proxy parameters are conveniently located in the Options dialog box available in the Software Update Manager menu. For more information, see the *Avaya Software Update Manager* online help.

Configuring the Web Server (Optional)

The Avaya Integrated Management installs the Apache HTTP server and configures it for use with the Avaya Integrated Management applications. For installations using a custom HTTP server, insert the definitions script into the HTTP server’s configuration file.

To use Voice Integration services, do the following:

1. Open the file **/etc/profile**.
2. Add entries for **AIM_FPM=<fpm_ip_address>** and **AIM_MSA=<msa_ip_address>** where **fpm_ip_address** is the IP address of the server running Avaya Fault and Performance Manager and **msa_ip_address** is the server running Avaya MultiSite Administration.
3. After you add the **AIM_FPM** and **AIM_MSA** entries, add an entry **export AIM_FPM AIM_MSA** to enable the server to use the values you configured.

Following is an example of a configuration script for an Apache web server running with Avaya Network Management in the standalone mode on a Windows server:

```
PassEnv AIM_FPM
PassEnv AIM_MSA
PassEnv CV_PATH
#Aliases:
Alias /launch    "C:/Program Files/Avaya/Network Management/CVS/Launch"
<Directory "C:/Program Files/Avaya/Network Management/CVS/Launch">
AddHandler cgi-script .cvpl
Options +ExecCGI
AllowOverride None
Order allow,deny
Allow from all
</Directory>

Alias /nm    "C:/Program Files/Avaya/Network Management/CVS
Alias /nm    "C:/Program Files/Avaya/Network Management/CVS
<Directory "C:/Program Files/Avaya/Network Management/CVS">
AddHandler cgi-script .cvpl
Options +ExecCGI
AllowOverride None
Order allow,deny
Allow from all
</Directory>
#Access restriction:
<Directory "C:/Program Files/Avaya/Network Management/CVS/Gen/resources/
private">
Deny from all
</Directory>
```

Configuring the Web Server for Polycom GMS support (Optional)

Polycom GMS runs under the Microsoft IIS Web Server on the same server as the Network Management server.

To support Polycom GMS:

1. Open the Apache configuration file. This file is usually called **httpd.conf** and it resides under the Apache bin directory.
2. Add the following lines:

   ```
   #Polycom Support
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_connect_module modules/mod_proxy_connect.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ProxyRequests Off
   ProxyPass /pwx http://127.0.0.1:<IIS Port>//pwx
   ProxyPassReverse /pwx http://127.0.0.1:<IIS Port>//pwx
   #End Polycom Support
   ```

   Note:

   Replace **<IIS Port>** with the port number used by Microsoft IIS Web Server.
3. Save your changes.

Configuring FTP (Optional)

FTP is supported by the Avaya Software Update Manager and the Avaya Configuration Backup Restore for certain network switches and gateways.

To configure FTP service on your Windows server, follow these steps:

1. Create a user on the Windows server.
2. Select **Start > Control Panel > Administrative Tools > Internet Services Manager**.
3. Select **Default FTP Site**.
4. Select the **Home Directory** tab.
5. Under **FTP Site Directory**, select **Read** and **Write**.

6. Click **Apply** to save changes.
7. Close the Control Panel.
8. Open Avaya Software Update Manager.
9. Select **File > Options**. The system displays the **Options** dialog box.
10. In the **FTP Global Use** field, select **Enabled**.
11. In the **FTP User Name and Password** field, enter the user name and password you created.
12. In the **FTP Server Page** field, enter the path of the FTP Site Directory on your server.
13. Click **Apply** to save the changes. The FTP server is configured to work with Avaya Software Update Manager.

    Note:

    The procedure is identical for the Avaya Configuration Backup Restore.

Changing the Port Numbers used by the Network Management applications

You can change the TCP port numbers of the Network Management server and client applications. You can use a firewall to block incoming and outgoing TCP connections to port numbers that are not used in the Network Management applications. You can set the firewalls on the Network Management server station and on any client station that is used to remotely access the server. The firewall on the web server port (the default installation is set to port 80) is required to allow http connections.

The port numbers are listed in the **cv.prop** file in the following location:

<Avaya application location>\Network Management\private\gen\(in standalone mode)

The **cv.prop** file contains a list of properties. Most of the properties define fixed port numbers used by the Network Management applications. Two of the properties (**.rmiport.min=2900** and **.rmiport.max=2950**) define a range of 50 port numbers.

To change the port numbers, follow these steps:

1. Stop the Network Management server (or HP OpenView server).
2. Change the ports in the **cv.prop** file.
3. Run the **updateResources.bat** batch file that resides in the same directory as the **cv.prop** file.
4. Restart the server.

Configuring the Software Update Manager for domain users

The Avaya Software Update Manager automatically upgrades TN board versions. The upgrade is done when the SCP client on the TN board downloads the image file from the Network Management Console/Software Update Manager SCP server. During the upgrade process, the Software Update Manager sets the user name and password on the TN board for the download process. By default, when the Network Management Console is installed, a local Windows user is specified for the SCP process. You can then configure the Software Update Manager for domain users instead of a specific local Windows user. To do this, you must:

1. Ensure that:
    - Network Management Console is registered to a domain.
    - You can log in to Windows with the domain user that you want to use.
2. Configure the COPSSH Server.
3. Configure the Software Update Manager.

Configuring the COPSSH Server

Perform the following steps to set up Software Update Manager for a domain user:

1. Log in to Windows with the domain user.
2. Open a command prompt window and run the following command:

    net user <domain_user> /domain
3. Check the command printout and make sure that under **Global Group Memberships**, the group **Domain Users** appears.
4. Change your work directory to **C:\Program Files\copSSH\bin** and run the following command:

    mkpasswd -d -c -u <domain user>

    For example: **C:\Program Files\copSSH\bin>mkpasswd -d -c -u jdoe**

    ```
    jdoe:unused_by_nt/2000/xp:132577:10513:Doe, John (John),U-GLOBAL\
    jdoe,J-1-5-21-790525478-1343024091-1801674531 -122577:/home/jdoe:/
    bin/switch
    ```
5. Open the directory **C:\Program Files\copSSH\etc**. Open the file **passwd** for editing and add the ouput of the command in step 4 to the file.

6. In the command prompt window run the following command:

   C:\Program Files\copSSH\bin>mkgroup -d >> domain.txt

   The command looks for the domain groups. The run time of the command can take some time depending on the number of groups in the domain. The output of the command is printed in the file **domain.txt**. When the command is finished running, open the file **domain.txt** and locate the line for the group Domain Users. It should look like:

   ```
   Domain Users:S-1-5-21-790525478-1343024091-1801674531-513:10513
   ```

7. Open the directory **C:\Program Files\copSSH\etc**. Open the file **group** for editing and add the ouput of the command in step 6 to the file.
8. In the directory **C:\Program Files\copSSH\etc** open the file **sshd_config** for editing. Locate the line **#IgnoreRhosts yes** and replace this line with **IgnoreRhosts no**.
9. Open the services window and stop the **copSSH Server** service. Then start the **copSSH Server** service.

The COPSSH Server is now configured and can be tested by using Putty or WinSCP to log in to the COPSSH Server.

Configuring the Software Update Manager

To enable the domain user you created in the Software Update Manager in the procedure Configuring the COPSSH Server, perform the following steps:

1. From the Network Management Console, select **Tools > Software Libraries**. You can also click on the Software Libraries icon.

   The system displays the **Software Libraries** properties dialog box in the lower window pane.
2. In the **Type** field, select **scp&tftp** from the drop-down menu.
3. In the **SCP User Name** field, enter the user name you created in the procedure Configuring the COPSSH Server.
4. In the **SCP Password** field, enter the password for the user you created.
5. In the **Retype SCP Password** field, enter the password again.
6. In the **SCP Server Path** field, enter the path for the domain user you created. The default path is **C:\Documents and Settings\username**.
7. Click **Add**.

The domain user is now able to use the Software Update Manager for TN circuit pack firmware downloads.

Chapter 3: Discovering the Voice Network

This chapter provides the procedure to run the Network Discovery Wizard to discover your voice network. The Network Discovery Wizard is provided during the Network Management installation. If you did not run the Network Discovery Wizard during installation, the first time you open the Avaya Network Management Console, you must discover your voice network.

Starting the Network Management Console

After installing Avaya Network Management, perform the following steps to start Avaya Network Management Console:

1. Ensure that the Avaya Network Management Server is running. The Avaya Network Management Server is a Windows service and should start automatically when you boot the server station.

   To check the status of the Avaya Network Management Server, select **Start > Programs > Avaya > Tools > Avaya Network Management Server Status**. The system displays a dialog box with the current Avaya Network Management Server status.

   If the Avaya Network Management Server is not running, start the Avaya Network Management Server by selecting **Start > Programs > Avaya > Start Avaya Services**.

2. Start the Avaya Network Management Console as follows:

   - If you are logged into the server where the Avaya Integrated Management applications are installed, do the following:

     a. Double-click the Windows desktop shortcut to the Avaya Integrated Management Launch Products page.

     The system displays the **Avaya Integrated Management Launch Products** page.

     b. Click the link **Avaya Network Management Console**.

     The system displays the **Login** dialog box. It prompts you for the User Name and Password you specified during installation.

     c. Enter your User Name, and press **Enter**.

     d. Enter your Password, and click **Login**.

     The system displays the **Avaya Network Management Console** window.

   - If you are at a remote PC, perform the following steps:

     a. Open Internet Explorer.

b. Enter the IP address of the server where the Avaya Integrated Management applications are installed, and then press **Enter**.

   The system displays the **Avaya Integrated Management Launch Products** page.

c. Click the link **Avaya Network Management Console**.

   The system displays the **Login** dialog box. It prompts you for the User Name and Password you specified during installation.

d. Enter your User Name, and press **Enter**.

e. Enter your Password, and click **Login**.

   The system displays the **Avaya Network Management Console** window.

Note:

If you receive a security certificate error message in your web browser window when launching the Integrated Management Products page, accept it and continue to the Integrated Management Products page. This error appears because Network Management is distributed with a self-signed certificate. This default certificate is an Apache Web Server certificate that is installed in the folder Program Files\Apache Group\Apache2\conf\ssl on the Network Management server.

If you do not want to see this security certificate error message, you must install a new certificate that is signed by your Certificate Authority (CA).

Using the Network Discovery Wizard to discover your voice network

To run the Network Discovery Wizard, do the following:

1. Access the Avaya Integrated Management Launch Products page.
2. Click the link **Avaya Network Management Console**.

   The system displays the **Login** dialog box. It prompts you for the User Name and Password you specified during installation.
3. Enter your User Name, and press **Enter**.
4. Enter your Password, and click **Login**.

   The system displays the **Avaya Network Management Console** window.

   For information on how to start the Avaya Network Management Server and launch the Network Management Console, see Starting the Network Management Console on page 35

5. From the **Actions** menu, select **Network Discovery Wizard**.

   The system displays the **Welcome** dialog box for the Avaya Network Management Configuration Wizard. This wizard will help you configure your VoIP media servers and gather information required to properly discover and manage your voice network with this network management station.

6. Click **Next**.

   The system displays the **Configure CM Servers** dialog box.

7. In the Configure CM Servers dialog box, perform the following steps:

   a. Click **Add CM** to add the Avaya Aura™ Communication Manager servers you want to manage.

   b. Enter the IP Address and login for the Communication Manager server.

   c. Do one of the following:

      - Click **Password**, and then enter the password.
      - Click **ASG key**, and then enter the ASG key.

   d. Select the appropriate protocol from the menu.

   e. Click **Next**.

   f. Select one of the following options:

   - If you want of use an existing SNMPv3 user to communicate with the Communication Manager server, click **Existing SNMPv3 User**, and then select the user from the associated drop-down box.
   - If you want to create a new SNMPv3 user to communicate with the Communication Manager server, click **New SNMPv3 User**, and then do the following:

      1. In the **User Name** field, enter the name of the new SNMPv3 user.
      2. In the **Authentication Password** field, enter the password. This password must consist of 8 to 32 characters.
      3. In the **Verify Authentication Password** field, re-enter the password.
      4. From the **Authentication Scheme** field, select the type of authentication.

   Note:

   For the Communication Manager servers, the SNMPv3 Authentication Scheme must be **MD5**.

      5. In the **Privacy Password** field, enter the privacy password. This password must consist of 8 to 32 characters.
      6. In the **Verify Privacy Password** field, re-enter the privacy password.

   g. Click **Next**.

h. Validate the server certificate, and then click **Yes**.

The new Avaya Aura™ Communication Manager server appears in the **Configure CM Servers** dialog box.

i. Repeat Steps a through h for each Communication Manager server you want to add. When you are finished adding Communication Manager servers, click **Next**.

The system displays the **Configure Global SNMP Parameters** dialog box. You can add one or more sets of SNMP parameters to be used for network discovery and management access to your network devices.

8. To add one or more sets of SNMP parameters:

a. Click **Add SNMP Rule**, and choose one of the following options:

- If the SNMP parameters are for an existing user, click **Existing SNMPv3 User**, and then select the user from the **Select User** menu.
- If the SNMP parameters are for a new user, click **New SNMPv3 User**, and then perform the following steps:

1. In the **User Name** field, enter the user name.
2. In the **Authentication Password** field, enter the password.
3. In the **Verify Authentication Password** field, re-enter the password.
4. From the **Authentication Scheme** field, select the scheme.

Note:

For the Communication Manager servers, the SNMPv3 Authentication Scheme must be **MD5**.

5. In the **Privacy Password** field, enter the privacy password.
6. In the **Verify Privacy Password** field, re-enter the privacy password.

- If you want to configure the SNMPv1 Community, click **SNMPv1 Community**, and then perform the following steps:

1. In the **Read Community** field, enter the Read Community string.
2. In the **Read/Write Community** field, enter the Read/Write Community string.

b. Click **Next**.

The new SNMP parameters appear in the Configure Global SNMP Parameters dialog box.

c. Repeat steps a and b for each set of SNMP parameters you want to add.

d. When you are finished configuring the global SNMP parameters, click **Next**.

The system displays the **Configure Network Subnet to Discover** dialog box.

9. In the Configure Network Subnet to Discover dialog box, perform the following steps:

a. Click **Add Subnet** to add the IP network you want to discover.

b. In the **Subnet IP** field, enter the subnet IP Address.

c. Perform one of the following steps:

   - Click **Subnet Mask**, and then enter the subnet mask.
   - Click **Router**, and then enter the router for this subnet.

d. Click **Next**.

   The system displays the new IP network in the Configure Network Subnet to Discover dialog box.

e. Repeat Steps a through d for each IP network you want to discover. When you are finished adding IP networks, click **Next**.

   The system displays the **Configuration Complete** dialog box.

For more information on how to use Avaya Network Management Console's Discovery feature, refer to Chapter 10 of the *Avaya Integrated Management Release 6.0 Network Management Console User Guide.*

Chapter 4: Provisioning Media Gateways in the network

Overview

To perform initial provisioning of the Avaya media gateways in your network, complete the following tasks:

- Starting the Avaya Provisioning and Installation Manager on page 41
- Creating a Template on page 43
- Creating a Device Profile on page 43
- Creating a Group on page 45
- Scheduling a job on page 45
- Performing a backup on page 46

Starting the Avaya Provisioning and Installation Manager

You can start the Provisioning and Installation Manager from the Windows server where the application is installed or through Internet Explorer from a remote PC.

Note:

You can also start the Provisioning and Installation Manager for a specific device from the Network Management Console. See the *Avaya Network Management Console User Guide*, document number 14-300169 for more information.

From the Server

To start the Avaya Provisioning and Installation Manager from the Windows server where the application is installed, do the following:

1. Double-click the Windows desktop shortcut to the Avaya Integrated Management Launch Products page.

   The system displays the **Avaya Integrated Management Launch Products** page.

2. Click the link **Avaya Provisioning and Installation Manager**.

   The system displays the **Login** dialog box. It prompts you for the User Name and Password you specified during installation.

3. Enter your User Name, and press **Enter**.
4. Enter your Password, and click **Login**.

   The system displays the **Avaya Provisioning and Installation Manager** window.

From a remote PC

To start the Avaya Provisioning and Installation Manager from a remote PC, do the following:

1. Open Internet Explorer.
2. Enter the IP address of the server where the Avaya Integrated Management applications are installed, and then press **Enter**.

   The system displays the **Avaya Integrated Management Launch Products** page.

3. Click the link **Avaya Provisioning and Installation Manager**.

   The system displays the **Login** dialog box. It prompts you for the User Name and Password you specified during installation.

4. Enter your User Name, and press **Enter**.
5. Enter your Password, and click **Login**.

   The system displays the **Avaya Provisioning and Installation Manager** window.

Creating a Template

When you create a template, you can specify configuration parameters manually or by importing template data from an XML file.

To create a template, do the following:

1. From the Provisioning and Installation Manager main window, click **Templates** in the left panel.

   The system displays the **Templates** page.

2. Click **New**.

   The system displays the **Templates** wizard.

3. Select the type of template you want to create, or select **Import from an XML file** and then specify the file path.
4. Continue through each page of the Template wizard. Click **Help** for help with each wizard page.

After you create a template, you can schedule the data to be uploaded to the devices. For more information on scheduling a job, see Scheduling a job on page 45.

Creating a Device Profile

When you create a Device Profile, you can enter the IP address manually, select it from the Avaya Network Management Console, import it from the electronic pre-installation worksheet, or import it from an XML file.

When you create a Device Profile, you can also associate templates that have already been created to the Device Profile. When you associate templates to a Device Profile, the configuration parameters defined in the templates are applied to the Device Profile.

Note:

> When you create a Device Profile, you can configure the Survivability feature for the device. The Device Profile wizard prompts you for Survivability parameters, such as automatic route selection (ARS) and dial strings. Survivability is supported for G250, G250-DS1, G250- DCP, G250- BRI, G350, G430 and G450 media gateways. For more information about Survivability, see the online help that is included with the Provisioning and Installation Manager application.

To create a device profile, do the following:

1. From the Provisioning and Installation Manager main window, click **Device Profiles** in the left panel.

   The system displays the **Device Profiles** page.

2. Click **New**.

   The system displays the **Device Profile** wizard.

3. Enter the IP address of the device in one of the following ways:

   - Enter manually.
   - Select a device from the Network Management Console.
   - Import from the electronic pre-installation worksheet.
   - Import from an XML file.

4. Continue through each page of the Device Profile wizard. Click **Help** for help with each wizard page.

   Note:

   A Device Profile may define multiple IP interfaces. One of the IP interfaces that you define must be set as primary management interface (**PMI**). The IP address of the PMI interface is used by the Avaya Provisioning and Installation Manager to communicate with the device and as the device identifier in the Avaya Aura™ Communication Manager server.

After you create a device profile, you can schedule the data to be uploaded to the devices. For more information on scheduling a job, see Scheduling a job on page 45.

Creating a Group

A Group is a collection of devices and is used in conjunction with templates to make it easy to apply a template to multiple devices at a time.

To create a group, perform the following steps:

1. From the Provisioning and Installation Manager main window, click **Groups** in the left panel.

   The system displays the **Groups** page.

2. Click **New**.

   The system displays the **Groups** wizard.

3. Enter the Group Name for this group.
4. Continue through each page of the Groups wizard. Click **Help** for help with each wizard page.

For more information on applying a Template to a Group for bulk provisioning, see Scheduling a Template job on page 46

Scheduling a job

After you create a Device Profile or Template, you need to schedule the Job for the configuration parameters defined in the Device Profile or Template to be uploaded to the devices. You schedule a Job through the Jobs wizard, which you access from the first page of the Device Profile wizard and the first page of the Template wizard. You can also access the Job wizard from the left panel of the Provisioning and Installation Manager main window. You can schedule the Job to run now, at a specified date and time, or later.

Scheduling a Device Profile job

To schedule a Device Profile Job, perform the following steps:

1. From the Provisioning and Installation Manager main window, click **Device Profile** in the left panel.

   The system displays the **Device Profile** page. This page provides a list of Device Profiles that have been created.

2. Select the Device Profile for which you want to schedule a Job.

3. Click **Job** at the top of the Device Profile page.

   The system displays the **Jobs wizard** page.
4. Continue through each page of the Jobs wizard. Click **Help** for help with each wizard page.

Scheduling a Template job

To schedule a Template Job, perform the following steps:

1. From the Provisioning and Installation Manager main window, click **Template** in the left panel.

   The system displays the **Template** page. This page provides a list of Templates that have been created.
2. Select the Template for which you want to schedule a Job.
3. Click **Job** at the top of the Template page.

   The system displays the **Jobs wizard** page.
4. Continue through each page of the Jobs wizard. Click **Help** for help with each wizard page.

   Note:

   When you schedule a Template job, you can apply the template to a group of devices for bulk provisioning.

Performing a backup

During a backup session, files are archived in a zip file. The following Provisioning and Installation Manager application files are included in a backup session:

- Profiles
- Templates
- Groups
- Authorization sets
- Jobs in the job queue or log— except running jobs
- System settings such as job queue, log retention, and system log file size
- Survivability extract data

The backup session also provides a list of files and the Provisioning and Installation Manager version.

To backup PIM data data and settings, use the Network Management Backup Utility.

To restore PIM data and settings, use the Network Management Easy Restore utility.

Chapter 5: Upgrading Avaya Aura™ Communication Manager devices

Use this procedure to update the Communication Manager devices using the Avaya Software Update Manager.

Follow these steps to upgrade the Communication Manager devices:

1. From the Avaya Network Management Console window, select **Tools > Avaya Software Update Manager**.
2. Select **File > Options**. The system displays the **Options** dialog box. Perform the following one-time setup instructions:
   a. In the Server Proxy Setting area, select the **Use Proxy** check box.
   b. In the **Host** field, enter the IP address or DNS name for the web proxy server.
   c. In the **Port** field, enter the TCP listening port used by the web proxy server.
   d. In the SFAP Login Parameters area, select the **Use SFAP** check box.
   e. In the **User Name** field, enter your user name.
   f. In the **Password** field, enter your password.
   g. In the **Confirm Password** field, reenter your password.
   h. Click **Retrieve Sold To's**. The system displays a list of Sold To's 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.
   i. From the **Sold To** drop-down list, select the Sold To you want to use.
   j. Click **OK** to save the changes and close the dialog box.

      Or

      Click **Apply** to save the changes and keep the dialog box open.
3. Select **Actions > Download Targets Detection**.

   The system displays the **Download Targets Detection** dialog box.
4. Select **Detect using filter**.
5. In the Product Filter area, select the Communication Manager devices you want to update.
6. Click **OK**.

   The system displays a warning dialog box.

7. Click **Continue**.

   The system displays a message box stating that the Avaya Software Update Manager will update the Download View table.

8. Click **OK**.

   All of the current information (software version and firmware version) for the discovered devices in the Avaya Network Management Console is displayed.

   The Avaya Software Update Manager connects to the Avaya Support Web site and compares the firmware on your Avaya Aura™ Communication Manager devices with the current Communication Manager firmware available on the Web site. The Avaya Software Update Manager then displays a status icon in front of each Communication Manager device.

   - If the icon is red, the device does not have the latest version of the firmware, and you do not have the latest version on your server.
   - If the icon is yellow, the device does not have the latest version of the firmware, but you have the latest version on your server.
   - If the icon is green, the device has the latest version of the firmware.
   - If the icon is purple, a new version is available on the Avaya site, but you are not entitled to download it.

9. Select **Tools > Retrieve From the Web**.

   The system displays a dialog box.

   Note:

   > It may take up to two minutes for the Avaya Software Update Manager to connect and log in.

10. Click **OK**.

    The files are downloaded to your server.

11. Select the devices you want to update.
12. Select **Actions > Download Now**. You can choose to download immediately or schedule it to a later date.
13. Select the check box **Reset after download**.
14. Click **Submit**.

For more information on the Software Update Manager, refer to the *Avaya Integrated Management Software Update Manager* online help.

Upgrading using the CM Software Management dialog box

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

Note:

> The CM Software Upgrade/Update dialog box is only accessible from the CM Software Management tab in the Software Update Manager Target table.
>
> The CM Software Upgrade/Update tab enables you to copy a release from an HTTP server to the hard drive of one or more CM 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.

Upgrading and updating Media Server releases

1. From the Avaya Network Management Console window, select **Tools > Avaya Software Update Manager**.

   The Avaya Software Update Manager automatically attempts to connect to the Avaya Support Web site. If the Avaya Software Update Manager connects to the Avaya Support Web site, the Avaya Software Update Manager window appears and displays the Targets table in the Download View tab. The Targets Table displays a status icon for each managed device to indicate the status of the software currently running on the associated device. This status icon also indicates whether an upgrade or update is available. Go to Step 2.

   If the Avaya Software Update Manager does not connect to the Avaya Support Web site, an error message box appears stating that the Web site is unreachable. Click **OK**. Perform the following steps:

   a. Select **File > Options**.

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

   b. In the Server Proxy Setting area, select the **Use Proxy** check box.

   c. In the **Host** field, enter the IP address or DNS name for the web proxy server.

   d. In the **Port** field, enter the TCP listening port used by the web proxy server.

   e. In the SFAP Login Parameters area, select the **Use SFAP** check box.

   f. In the **User Name** field, enter your user name.

   g. In the **Password** field, enter your password.

   h. In the **Confirm Password** field, reenter your password.

i. Click **Retrieve Sold To's** to specify the information you want to download.

j. When finished, click **Apply**.

k. Click the **OK**.

2. Select the **CM Software Management** tab.
3. Select **Actions > Target Details**. The CM Software Management dialog box appears.
4. Click the **CM Software Upgrade/Update** tab in the CM Software Management dialog box. Choose one of the following options:

l **To install a release on one or more Media Servers:**

a. Select one or more of the targets that you want to upgrade in the Targets Table.

b. Select the **CM Release Location** check box.

c. Click one of the following sources from which you want to download the software release:

- **NMS CD**
- **Media Server Hard Disk**
- **Media Server CD**
- **URL** - specify the URL from which you want to download the software.

d. From the drop-down list next to the selected media source, choose the software version you require.

e. Select one of the following actions:

- **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.

f. Click **Download** to begin. The system displays the **Job Summary** window in the CM Software Management dialog box, displaying a summary of the download currently being performed.

Note:

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

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

l **To Install a CM Service update:**

a. Select one or more of the targets that you want to upgrade in the Targets Table.

b. Select the **CM Service Packs** check box. The system displays a list of CM Service Packs in the CM Service Packs table.

c. Select the service update you want to install.

d. Click **Download**. The system displays the **Job Summary** window in the CM Software Management dialog box, displaying a summary of the download currently being performed.

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

- **To install a platform/security update:**

a. Select one or more of the targets in the Targets Table that you want to upgrade.

b. Select the **Platform/Security Update** check box.

c. Select the service update you want to install.

d. Click **Download**. The system displays the **Job Summary** window in the CM Software Management dialog box, displaying a summary of the download currently being performed.

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

For information on how to install license or authentication files to the software repository on the CM Server, refer to the *Avaya Integrated Management Software Update Manager* online help.

Chapter 6: Post installation tasks for IP Office devices

Overview

This chapter describes the tasks you should perform after installing Avaya Network Management with IP Office. Initial configuration consists of the following steps:

1. Enable SNMP for each IP Office device.
2. Add IP Office devices to Avaya Network Management Console.
3. Configure access parameters for IP Office devices.
4. Upgrade the IP Office devices using Avaya Software Update Manager.

Step 1: Enable SNMP on the IP Office devices

Before you can use Avaya Network Management Console to discover the IP Office devices automatically in your network, you must configure the community string in IP Office Manager for each IP Office device in your network.

Note:

> If you have IP Office Release 2.1 or earlier, go to Step 2. SNMP is not supported in these releases.

Using IP Office Manager, perform the following steps for each IP Office device:

- Configure the SNMP community string and set the port to 161.
- Enable trap destinations. Enter the IP address of the Windows server where Avaya Network Management is installed, select all of the trap check boxes, set the port to 162, and configure the SNMP community string.

Step 2: Add IP Office devices to Avaya Network Management Console

Use this procedure to populate all of the IP Office devices in your network in Avaya Network Management Console.

You can populate Avaya Network Management Console using the following methods:

- discover devices automatically

  Use this method if your IP Office devices are accessible through the web and answer to SNMP.
- add devices manually

  Use this method if you want to enter each IP Office device one at a time.
- import a CSV file

  Use this method if your IP Office devices are accessible through the web, but do not answer to SNMP. (You can ping or access these devices via IP Office Manager.)

Discovering devices automatically

Use this procedure if your IP Office devices are accessible through the web and answer to SNMP.

To discover IP Office devices automatically, perform the following steps:

1. Log into Network Management Console. For more information on how to start the Avaya Network Management Server and launch the Network Management Console, see Starting the Network Management Console on page 35.
2. Select **Actions > IP Discovery**.

   The system displays the **Discovery** window.

   Note:

   If **IP Discovery** is disabled, select **Actions > Get Write Permission**. After the Write Permission Request dialog box closes, repeat Step 2.
3. Select **Edit > Add**.

   The system displays the **Add New Subnet** dialog box.
4. In the **Subnet IP** box, enter the IP address of the subnet you want to add.
5. In the **Subnet Mask** box, enter the subnet mask.
6. Click **Apply**.
7. Click **Close**.
8. Repeat Steps 3 through 7 to add more subnets. When finished, go to Step 9.

9. Select **Actions > Start Network Discovery**.

   The system displays a progress bar displaying the progress of the discovery process. When the process is complete, the devices appear in the left panel.

Adding devices manually

If your IP Office devices answer to SNMP and you want to discover them manually, perform the following steps:

1. Log into Network Management Console. For more information on how to start the Avaya Network Management Server and launch the Network Management Console, see Starting the Network Management Console on page 35.
2. Select **File > New > Device**.

   The system displays the **Add Device** dialog box. The Basic Information tab is selected.
3. Enter the parameters for the IP Office device.
4. Click the **SNMP Access** tab.
5. Enter the SNMP parameters for the IP Office device.
6. When finished, click **Apply** to add the device to the Network Map.
7. Click **Close**.
8. Repeat Steps 2 through 7 for each IP Office device you want to add.

Importing a CSV file

If your IP Office devices are accessible through the web, but do not answer to SNMP, you must import a CSV file into Avaya Network Management Console. This CSV file must contain the following information for each IP Office device in your network:

- type
- IP address
- subnet mask
- MAC address
- name
- read community string
- write community string
- timeout interval
- retry interval

Table 2describes the fields in each record of the CSV file.

Table 2: CSV Import File Fields

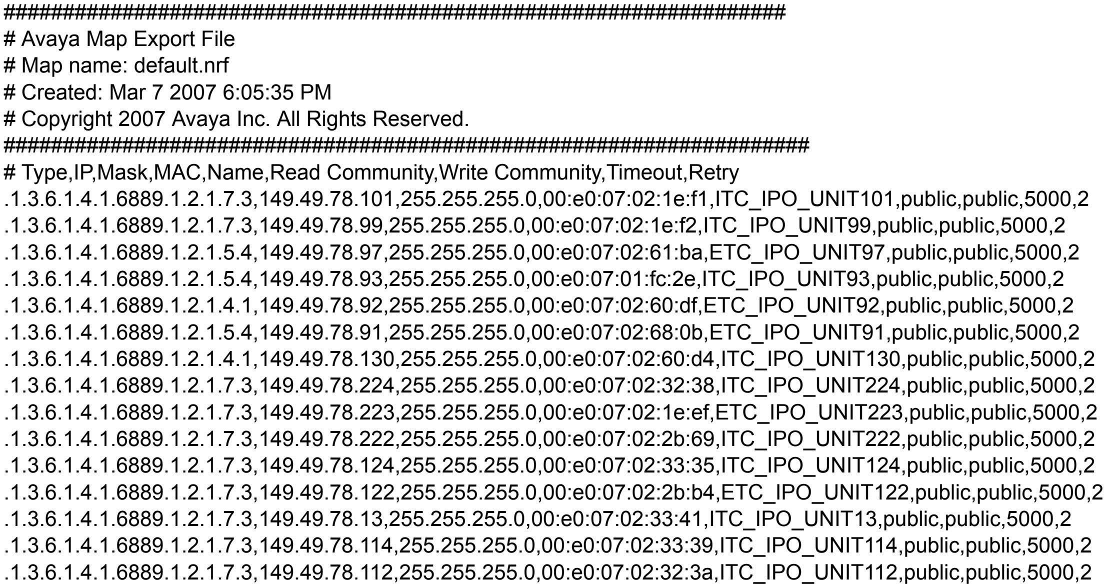
Field	Description
Type	The sysObjectID of the IP Office device. Table 3 shows the sysObjectIDs of the supported IP Office devices.
IP	The IP address of the IP Office device.
Mask	The IP subnet mask of the IP Office device.
MAC	The MAC address of the IP Office device.
Name	The name of the IP Office device.
Read Community	The read community string of the IP Office device.
Write Community	The write community string of the IP Office device.
Timeout	The number of milliseconds an application will poll the IP Office device without receiving a response before timing out. The recommended value is 5000 ms.
Retry	The number of times an application will poll the IP Office device without receiving a response before timing out. The recommended value is 2.

Table 3: sysObjectIDs of Supported IP Office Devices

Device	Symbol ID	SysObjectID
IP406-V2	IPOFFICE_406V2	1.3.6.1.4.1.6889.1.2.1.7.3
IP412	IPOFFICE_412	1.3.6.1.4.1.6889.1.2.1.4.1
IP500	IPOFFICE_500	1.3.6.1.4.1.6889.1.2.1.9.1
IP500-V2 (IP Office mode)	IPOFFICE_500V2	1.3.6.1.4.1.6889.1.2.1.10.1
Small Office 2T+4A	SMALL_OFFICE_4A	1.3.6.1.4.1.6889.1.2.1.5.1
Small Office 4T+8A	SMALL_OFFICE_8A	1.3.6.1.4.1.6889.1.2.1.5.2
Small Office 4T+4A+8DS	SMALL_OFFICE_8D	1.3.6.1.4.1.6889.1.2.1.5.4
IP500-V2	IPOFFICE_500V2	1.3.6.1.4.1.6889.1.2.1.10.1

Figure 2 shows a sample CSV file that contains 15 IP Office devices.

Figure 2: Sample CSV File



```
###################################################################
# Avaya Map Export File
# Map name: default.nrf
# Created: Mar 7 2007 6:05:35 PM
# Copyright 2007 Avaya Inc. All Rights Reserved.
#####################################################################
# Type,IP,Mask,MAC,Name,Read Community,Write Community,Timeout,Retry
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.101,255.255.255.0,00:e0:07:02:1e:f1,ITC_IPO_UNIT101,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.99,255.255.255.0,00:e0:07:02:1e:f2,ITC_IPO_UNIT99,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.5.4,149.49.78.97,255.255.255.0,00:e0:07:02:61:ba,ETC_IPO_UNIT97,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.5.4,149.49.78.93,255.255.255.0,00:e0:07:01:fc:2e,ITC_IPO_UNIT93,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.4.1,149.49.78.92,255.255.255.0,00:e0:07:02:60:df,ETC_IPO_UNIT92,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.5.4,149.49.78.91,255.255.255.0,00:e0:07:02:68:0b,ETC_IPO_UNIT91,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.4.1,149.49.78.130,255.255.255.0,00:e0:07:02:60:d4,ITC_IPO_UNIT130,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.224,255.255.255.0,00:e0:07:02:32:38,ITC_IPO_UNIT224,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.223,255.255.255.0,00:e0:07:02:1e:ef,ETC_IPO_UNIT223,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.222,255.255.255.0,00:e0:07:02:2b:69,ITC_IPO_UNIT222,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.124,255.255.255.0,00:e0:07:02:33:35,ITC_IPO_UNIT124,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.122,255.255.255.0,00:e0:07:02:2b:b4,ETC_IPO_UNIT122,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.13,255.255.255.0,00:e0:07:02:33:41,ITC_IPO_UNIT13,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.114,255.255.255.0,00:e0:07:02:33:39,ITC_IPO_UNIT114,public,public,5000,2
.1.3.6.1.4.1.6889.1.2.1.7.3,149.49.78.112,255.255.255.0,00:e0:07:02:32:3a,ITC_IPO_UNIT112,public,public,5000,2
```

To import a CSV file, perform the following steps:

1. Log into Network Management Console. For more information on how to start the Avaya Network Management Server and launch the Network Management Console, see Starting the Network Management Console on page 35.
2. Select **File > Import map**.

   The system displays the **Import Map** dialog box.
3. Select the CSV file you want to import, and then click **Open**.

   The devices in the CSV file are imported into the current Network Map. The devices appear in the Device Type View and the Subnet View.

Step 3: Configure the Access parameters for IP Office devices

You must provide user names and passwords to the Avaya Network Management server to access IP Office devices. These user names and passwords must match the security administrator name and password in the IP Office device.

In this section, you will:

1. Create a new IP Office User in Avaya Secure Access Administration.

   This IP Office user and password must match the IP Office security administrator name and password. There can be only one IP Office user per IP Office device in Avaya Secure Access Administration. For more information about IP Office security administration, see the IP Office documentation.

   Once you assign an Avaya Secure Access Administration IP Office User, Avaya Secure Access Administration will create a user (AIMAdmin) who has complete administration capabilities.

2. Assign the IP Office User to IP Office devices.

The steps you perform depend on the firmware release of the IP Office device.

IP Office devices running Firmware earlier than 4.0.307

If any of the IP Office devices are running firmware earlier than 4.0.307, perform the procedures in this section.

Step 1: Creating users

Perform the following steps:

1. From the Avaya Network Management Console window, select **Actions > Avaya Secure Access Administration**.

   The system displays the **Avaya Secure Access Administration** window.

2. Select **Action > New > New IP Office User**.

   The system displays the **New IP Office User** dialog box.

3. In the **Name** field, enter the name for the IP Office User. This user and password will be used only after you upgrade the IP Office device to version 4.0.307 or later.

4. In the **Password** field, enter the password for this user. This password must match the password of the Security Administrator as currently configured in the IP Office system. This password will only be used after you upgrade.

5. In the **Confirm Password** field, reenter the password for this user.
6. In the **TFTP Password** field, enter the TFTP password for the IP Office device being administered. This password must match the system password for the IP Office device. This password will be used to upgrade the IP Office device.
7. In the **Confirm TFTP Password** field, reenter the TFTP password.
8. Click **Apply** to add the Secure Access Administration IP Office user.
9. Click **Close**.

Step 2: Assigning users

In this section, you will use Avaya Secure Access Administration to map the IP Office system password to the IP Office devices.

Perform the following steps:

1. Select **Action > Assign Users to IP Office Devices**.

   The system displays the **Assign IP Office Security Administration** dialog box.
2. Select all of the IP Office devices running firmware earlier than 4.0.307.
3. From the **User Name** field, select the user you just created in the previous section.
4. From the **Select Action Type** field, select **Don't synchronize with devices**.

   ⚠ **Important:**
   You must select **Don't synchronize with devices**.
5. Click **Apply**.
6. Click **Close**.
7. At this point, you must use **Avaya Software Update Manager** to upgrade your IP Office devices. Go to Step 4: Upgrade the IP Office devices using Avaya Software Update Manager on page 64. Avaya Software Update Manager will use the TFTP password for each IP Office device. After you upgrade your IP Office devices, go to Step 8.
8. After you upgrade the IP Office devices with Avaya Software Update Manager, open **Avaya Secure Access Administration**.
9. Select **Action > Assign Users to IP Office Devices**.

   The system displays the **Assign IP Office Security Administration** dialog box.
10. Select all of the IP Office devices that were running firmware earlier than 4.0.307.
11. From the **User Name** field, select the user you created in the previous section.
12. From the **Select Action Type** field, select **Apply All**.

13. Click **Apply**.

    Avaya Secure Access Administration will try to contact the IP Office devices, change the TFTP password on each device, and define a service user called **AIMAdmin**.

    Note:

    The AIMAdmin password is common to all IP Office devices. You can change this password using **File > Options** in Avaya Secure Access Administration.

14. Click **Close**.
15. Close **Avaya Secure Access Administration**.

IP Office devices running Firmware 4.0.307 or later

If any of the IP Office devices are running firmware 4.0.307 or later, perform the procedures in this section.

Step 1: Creating users

Perform the following steps:

1. From the Network Management Console window, select **Actions > Avaya Secure Access Administration**.

   The system displays the **Avaya Secure Access Administration** window.

2. Select **Action > New > New IP Office User**.

   The system displays the **New IP Office User** dialog box.

3. In the **Name** field, enter the name for the IP Office User. This name must match the name of the Security Administrator of the IP Office device to which this user will be assigned.
4. In the **Password** field, enter the password for this user. This password must match the password of the Security Administrator as currently configured in the IP Office system.
5. In the **Confirm Password** field, reenter the password for this user.
6. In the **TFTP Password** field, enter the TFTP password for the IP Office devices being administered. After the user is assigned to the IP Office device, Avaya Secure Access Administration will change the TFTP password. (The TFTP password is referred to as the System password in the IP Office device.)
7. In the **Confirm TFTP Password** field, reenter the TFTP password.
8. Click **Apply** to add the Secure Access Administration IP Office user.
9. Click **Close**.

Step 2: Assigning users to IP Office devices

Perform the following steps:

1. Select **Action > Assign Users to IP Office Devices**.

   The system displays the **Assign IP Office Security Administration** dialog box.

2. Select all of the IP Office devices running firmware 4.0.307 or later that you want to assign to an IP Office user.
3. From the **User Name** field, select the user you just created in the previous section.
4. From the **Select Action Type** field, select **Apply changes**.
5. Click **Apply**.

   Avaya Secure Access Administration will try to contact the IP Office devices and change the TFTP password on each device and define a service user called **AIMAdmin**.

   Note:

   > The AIMAdmin password is common to all IP Office devices. You can change this password from **File > Options** in Avaya Secure Access Administration.

6. Click **Close**.
7. Close **Avaya Secure Access Administration**.

Step 4: Upgrade the IP Office devices using Avaya Software Update Manager

In this section, you will start Avaya Software Update Manager and update all of the IP Office devices.

> ⚠ **Important:**
>
> For Avaya Software Update Manager to update IP Office devices, the IP Office devices must be assigned to an IP Office user in Avaya Secure Access Administration.

Perform the following steps to upgrade the IP Office devices:

1. From the Avaya Network Management Console window, select **Tools > Avaya Software Update Manager**.

   Avaya Software Update Manager automatically attempts to connect to the Avaya Support web site. If Avaya Software Update Manager connects to the Avaya Support web site, the Avaya Software Update Manager window appears and displays the Targets table in the Download View tab. The Targets Table displays a status icon for each managed device to indicate the status of the software currently running on the associated device. This status icon also indicates whether an upgrade or update is available. Go to Step 3.

   If Avaya Software Update Manager does not connect to the Avaya Support web site, an error message box appears stating that the web site is unreachable. Click the **OK** button. You must configure the proxy server. Perform the following steps:

2. Select **File > Options**. The system displays the **Options** dialog box. Perform the following one-time setup instructions:

   a. In the Server Proxy Setting area, select the **Use Proxy** check box.

   b. In the **Host** field, enter the IP address or DNS name for the web proxy server.

   c. In the **Port** field, enter the TCP listening port used by the web proxy server.

   d. In the SFAP Login Parameters area, select the **Use SFAP** check box.

   e. In the **User Name** field, enter your user name.

   f. In the **Password** field, enter your password.

   g. In the **Confirm Password** field, reenter your password.

   h. Click **Retrieve Sold To's**. The system displays a list of Sold To's 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.

   i. From the **Sold To** drop-down list, select the Sold To you want to use.

   j. Click **OK** to save the changes and close the dialog box.

3. Select **Actions > Download Targets Detection**.

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

4. Select the **Detect using filter** option button.

5. In the Product Filter area, select the IP Office devices you want to update.

6. Click **OK**.

   The system displays a warning dialog box.

7. Click **Continue**.

   The system displays a message box stating that Avaya Software Update Manager will update the Download View table.

8. Click **OK**.

   All of the current information (software version and firmware version) for the discovered devices in Avaya Network Management Console is displayed.

9. Select **Tools > Image Analyzer**.

   Avaya Software Update Manager connects to the Avaya Support web site and compares the firmware on your IP Office devices with the current IP Office firmware available on the web site. Avaya Software Update Manager then displays a status icon in front of each IP Office device:

   - If the icon is red, the device does not have the latest version of the firmware, and you do not have the latest version on your server.

   - If the icon is yellow, the device does not have the latest version of the firmware, but you have the latest version on your server.

   - If the icon is green, the device has the latest version of the firmware.

   - If the icon is purple, the associated device is an expansion module that has the latest version of the firmware.

10. Select the IP Office devices that have red status icons.

11. Select **Tools > Retrieve From the Web**.

    The system displays a dialog box.

12. Click **OK**.

    The files are downloaded to your server.

13. Select **Tools > Image Analyzer**.

    All of the red status icons will turn yellow, indicating that the latest firmware versions are now on your server.

14. Select the devices you want to update.

15. Select **Actions > Download Now**.

    The selected IP Office devices are updated.

16. After all of the devices have been updated successfully (see the Current Version column), select **Tools > Image Analyzer**.

    All of the status icons should be green or purple.

Go to Accessing IP Office Systems on page 67 to start managing the IP Office devices from Avaya Network Management Console.

Chapter 7: Managing IP Office devices in your network

Overview

This chapter provides procedures for managing your IP Office devices from Avaya Network Management Console.

Accessing IP Office Systems

Avaya Network Management Console shows the connected and registered endpoints associated with each of your IP Office devices. From the Avaya Network Management Console window, you can:

- view all ports in the network
- quickly locate a station by user name, extension, or IP address
- view the status of each device on your network.
- use Event Manager to view a historical log of all traps received from the devices on your network. You can also configure Event Manager to send you an email message, run a script, or play a WAV file when certain events occur.
- use Avaya Software Update Manager to retrieve the latest firmware versions from the Avaya Support web site and update the following devices in your network:
  - control units
  - expansion units
  - VCM and slide-in modules
  - license dongles

  Using the Job Scheduler, you can set
  - the devices for which you want Avaya Software Update Manager to retrieve the latest firmware version
  - when you want Avaya Software Update Manager to retrieve the latest firmware version for the selected devices

You can launch IP Office Manager for a specific IP Office device by double-clicking on the associated IP Office icon on the map in the Avaya Network Management Console window.

Backing Up the configurations of all the IP Office devices

You should back up the configurations of all your IP Office devices before making any configuration changes.

To back up the configurations of all the IP Office devices, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.
2. Click the **Device Profiles** folder in the left panel.

   The system displays the **Device Profiles** page.
3. Click **Backup**.

   The system displays the **General** dialog box. The Job Name box displays a default name for this back up job. You can change this name.
4. In the Notes field, enter any notes about this backup job.
5. Click **Next**.

   The system displays the **Device Filter** dialog box. From this dialog box, you can specify whether you want to back up all devices or a subset of devices.
6. Select the **All devices** option button.
7. Click **Next**.

   The system displays the **Devices** dialog box. The **Available Devices** list box shows all of the available devices.
8. Click **>>** to back up all the devices.

   The system displays the selected devices in the **Selected Devices** box.
9. Click **Next**.

   The system displays the **Schedule** dialog box. From this dialog box, you can set the back up to be performed now or at a later time.
10. Select the **Run now** option button, and then click **Next**.

    The system displays the **Summary** dialog box.
11. Click **Next** to start the back up.

    The system displays a progress dialog box. When the back up is complete, the **Finish Up** dialog box appears.
12. Click the **Finish** button.
13. Click the **Jobs** folder in the left panel to determine whether the back up was successful.

Working with templates

You can create and use templates to manage and maintain branches that have similar configurations. With templates, you can make your changes in one file and then propagate this file to a group of branches.

Note:

> To create templates, IP Office Manager must be installed on the PC you are using.

When you create a template, you can specify configuration parameters manually. You can create the following templates:

- **General**

  General templates contain the following information:

  - account codes
  - time profiles
  - firewall profiles
  - directories
  - automatic route selection (ARS)

- **Hardware**

  Hardware templates contain the following information:

  - hardware configuration (control unit and expansion modules)
  - short codes
  - system parameters (LAN/WAN IP addresses, SNMP configuration, alarm notifications, and basic telephony parameters)
  - line/trunk settings
  - E911
  - extensions
  - wireless parameters (Small Office only)

- **Auto Attendant**

  Auto Attendant templates contain the following information:

  - time profiles
  - short codes
  - incoming call routes

  - associations of WAV files from the Voice Files library to time profiles. Avaya Provisioning and Installation Manager for IP Office enables you to upload WAV files from PCs to the Voice Files library. (You manage the Voice Files library from Avaya Provisioning and Installation Manager for IP Office.)

- **Users**

  Users templates contain the following information:

  - users and extensions
  - hunt groups
  - time profiles
  - firewall profiles
  - incoming call routes
  - user rights. User rights is a template within a template. With user rights, you can define classes of users and associate defaults for the following settings in each class:
    - short codes
    - basic telephony parameters
    - button programming
    - Phone Manager

Creating a General template

To create a General template, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click **Templates** at the top of the window.

   The system displays the **Select Template Type** wizard.

3. From the IPO Templates box, select the **IPO-General** option button, and then click **Next**.

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

4. In the **Name** field, enter the name for this template.

5. in the **Notes** field, enter any notes.

6. Click **Next**.

   The system displays the **IPO Manager** dialog box, and IP Office Manager starts in template mode. The IP Office Manager window appears.

7. Using IP Office Manager, complete the General template. Use the online help for more information about the General template.
8. When you are finished creating the General template in IP Office Manager, select **File > Save Template and Exit**.

   The system closes the IP Office Manager window, and displays the **Summary** dialog box.
9. Click **Next**.

   The system displays the **Finish Up** dialog box.
10. Click **Finish**.

Creating a Hardware template

To create a Hardware template, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the Provisioning and Installation Manager window.
2. Click **Templates** at the top of the window.

   The system displays the **Select Template Type** wizard.
3. From the IPO Templates box, select the **IPO-Hardware** option button, and then click **Next**.

   The system displays the **General** dialog box.
4. In the **Name** field, enter the name for this template.
5. in the **Notes** field, enter any notes.
6. Click **Next**.

   The system displays the IPO Manager dialog box and IP Office Manager starts in template mode. The Create Offline Configuration Wizard dialog box appears.
7. Complete each dialog box in the wizard. Click the Help button for information about the dialog box.

   After you complete the Create Offline Configuration Wizard, the IP Office Manager window appears.
8. Using IP Office Manager, complete the Hardware template. Use the online help for more information about the Hardware template.
9. When you are finished creating the Hardware template in IP Office Manager, select **File > Save Template and Exit**.

   The system closes the IP Office Manager window, and displays the **Summary** dialog box.

10. Click **Next**.

    The system displays the **Finish Up** dialog box.

11. Click **Finish**.

Creating an Auto Attendant template

Before creating an Auto Attendant template, you must upload the Auto Attendant voice files (WAV files) to Provisioning and Installation Manager for IP Office. To upload voice files, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click **+** in front of the **Administration** folder in the left panel of the window.

   The system displays the **Administration** options.

3. Click **Voice Files**.

   The Voice Files List page appears and lists all of the WAV files in Provisioning and Installation Manager for IP Office.

4. Click **Add**.

   The system displays the **PIM - Upload Voice File** dialog box.

5. Using the **Browse** button, select the WAV file you want to upload to Provisioning and Installation Manager for IP Office.
6. Click **Upload file**.
7. Repeat Steps 2 through 6 for any other WAV files you want to upload to Provisioning and Installation Manager for IP Office.

To create an Auto Attendant template, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click **Templates** at the top of the window.

   The system displays the **Select Template Type** wizard.

3. From the IPO Templates box, select the **IPO-Auto Attendants** option button, and then click **Next**.

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

4. In the **Name** field, enter the name for this template.
5. in the **Notes** field, enter any notes.

6. Click **Next**.

   The IPO Manager dialog box appears, and IP Office Manager starts in template mode. The IP Office Manager window appears.

7. Using IP Office Manager, complete the Auto Attendant template. Use the online help for more information about the Auto Attendant template.

8. When you are finished creating the Auto Attendant template in IP Office Manager, select **File > Save Template and Exit**.

   The system closes the IP Office Manager window, and displays the **Summary** dialog box.

9. Click **Next**.

   The system displays the **Finish Up** dialog box.

10. Click **Finish**.

Creating a Users template

To create a Users template, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click **Templates** at the top of the window.

   The system displays the **Select Template Type** wizard.

3. From the IPO Templates box, select the **IPO-Users** option button, and then click **Next**.

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

4. In the **Name** field, enter the name for this template.

5. in the **Notes** field, enter any notes.

6. Click **Next**.

   The IPO Manager dialog box appears, and IP Office Manager starts in template mode. The IP Office Manager window appears.

7. Using IP Office Manager, complete the Users template. Use the online help for more information about the Users template.

8. When you are finished creating the Users template in IP Office Manager, select **File > Save Template and Exit**.

   The system closes the IP Office Manager window, and displays the **Summary** dialog box.

9. Click **Next**.

   The system displays the **Finish Up** dialog box.

10. Click **Finish**.

Distributing templates

To distribute templates, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click the **Templates** folder in the left panel of the window.

   The **Templates** page appears and displays the existing templates.

3. Click the option button of the template you want to distribute.
4. Click **Job** at the top of the window.

   The system displays the **General** dialog box. A default name is provided for this job. You can change the job name.

5. Enter any notes.
6. Select the **Save The Job** check box if you want to save this job so you can use it at a later time.
7. Click **Next**.

   The system displays the **Device Filter** dialog box.

8. Select the devices you want to configure with the selected template, and then click **Next**.

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

9. From the Available list box, select the device(s) you want to configure with the selected template, and then click **>**. The selected devices appear in the Selected list box.

   If you want to select all of the devices from the Available list box, click **>>**.

10. Click **Next**.

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

11. Specify when you want to run this job, and then click **Next**.

    The system displays the **Job Options** dialog box.

12. Specify how you want to run this job, and then click **Next**.

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

13. Click **Next**.

    The job is created, and the system displays the **Finish Up** dialog box.

14. Click **Finish**.

The job runs at the time you specified.

Working with device Profiles

When Avaya Network Management Console discovers an IP Office device, it automatically creates a device profile. The device profile contains the following information:

- the name of the device
- the IP address of the device
- the type of device
- any notes entered about the device
- the Feature License Key data of the device

You may associate a device profile with existing templates (that is, General, Hardware, Auto Attendant, and Users).

Creating a device Profile

When you create a device profile, you can enter the IP address manually or select it from the Avaya Network Management Console. You can create a profile for the following devices:

- IP406-V2
- IP412
- IP500
- IP500-V2 (IP Office mode)
- Small Office 2T+4A
- Small Office 4T+8A
- Small Office 4T+4A+8DS

To create a device profile, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click **Profiles** at the top of the window.

   The system displays the **Device Profile Wizard** dialog box.

3. Make sure the **IPO device** option button is selected, and then click **Next**.

   The system displays the **Device Profile Wizard** dialog box.

4. Perform one of the following steps:

   - If you want to enter the IP address manually:

     a. Click the **Enter manually** option button, and then click **Next**.

        The system displays the **Device Type** dialog box.

     b. Select the device type for which you want to create a profile, and then click **Next**.

        The system displays the **Profile Details** dialog box.

     c. Enter the appropriate information for the selected device, and then click **Next**.

        The system displays the **Template Associations** dialog box.

     d. Go to Step 5.

   - If you want to select a device from Avaya Network Management Console:

     a. Click the **Select a device from NMC** option button, and then click **Next**.

        The system displays the **IP Address Filter** dialog box.

     b. Enter the IP address of the device for which you want to create a profile or specify the filter criteria from which you want to select the IP address.

     c. Click **Next**.

        The system displays the **IP Address** dialog box.

     4. Select the IP address of the device, and then click **Next**.

        The Device Details dialog box appears and shows the name, type, and IP address of the selected device.

     e. Click **Next**.

        The system displays the **Template Associations** dialog box.

     f. Go to Step 5.

5. If you want to associate a template type with this device profile, click the check box for the appropriate template type, and then select the appropriate template from the template selection drop-down list box.

6. Repeat Step 5 for each template type you want to associate with this device profile.

7. When finished associating templates, click **Next**.

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

8. Enter the licenses for the device, and then click **Next**.

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

9. Click **Next**.

   The device profile is created, and the system displays the **Finish Up** dialog box.

10. Click **Finish**.

Working with Groups

A group is a collection of devices and is used in conjunction with templates to make it easy for you to change multiple devices at a time. There are two types of groups:

- Static group

  A static group enables you to manage your branch offices logically. You can create static groups according to arbitrary criteria such as geographic location, device type, and type and/or size of the branch office.

- Dynamic group

  A dynamic group enables you to select specific branch offices by building a query. You build a logical expression combining static groups that are manually administered. For example, if you choose AND, only the devices that are in both groups will be selected for the dynamic group. If you choose OR, all of the devices in both groups will be selected for the dynamic group.

Creating a Static Group

To create a static group, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click **Groups** at the top of the window.

   The system displays the **Select Group Type** dialog box.

3. Select the **Static Group** option button, and then click **Next**.

   The system displays the **General Information** page.

4. In the **Name** field, enter the name for this group.

5. In the **Notes** field, enter any notes for this group.

6. Click **Next**.

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

7. Select the criteria you want to use to filter the eligible devices for this group. For example, if you are only interested in IP Office devices on a specific subnet, select that subnet from the Subnet box.

8. Click **Next**.

   The system displays the **Select Devices** dialog box.

9. From the Available list box, select the device(s) you want to add to the group, and then click **>**. The selected devices appear in the Selected list box.

   If you want to select all of the devices from the Available list box, click **>>**.

10. Click **Next**.

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

11. Click **Next**.

    The static group is created, and the **Finish Up** dialog box appears.

12. Click **Finish**.

Creating a Dynamic Group

Before you can create a dynamic group, you must have already created static groups.

To create a dynamic group, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click **Groups** at the top of the window.

   The system displays the **Select Group Type** dialog box.

3. Select the **Dynamic Group** option button, and then click **Next**.

   The system displays the **General Information** page.

4. In the **Name** field, enter the name for this group.

5. In the **Notes** field, enter any notes for this group.

6. Click **Next**.

   The system displays the **Query builder** dialog box.

7. From the Group Name box in the first row, select the static group you want to use.

8. From the Condition box in the next row, select the condition you want to use to build the dynamic group. Choices are:

   - AND
   - AND_NOT
   - OR

9. From the Group Name box in the row, select the static group you want to use.

10. If you want to add another condition, click **Add Row**.

    A new row appears.

11. From the Condition box in the new row, select the condition you want to use.
12. From the Group Name box in the new row, select the static group you want to use.
13. If you want to include parentheses around two or more groups, click **(** and **)** on the appropriate rows.

    The text box at the bottom of the dialog box shows the query you have built so far.
14. Repeat Steps 10 through 13 to add more conditions to this query.
15. When finished, click **Next**.

    The system displays the **Summary** dialog box.
16. Click **Next**.

    The dynamic group is created, and the system displays the **Finish Up** dialog box.
17. Click **Finish**.

Importing Licenses

You can import a CSV file that contains the license information for IP Office devices. Each record in the CSV file must contain the following information for each device:

- IP address
- the list of license keys for the device

To import licenses, perform the following steps:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.

2. Click the **Import Licenses**.

   The system displays the **General** dialog box. The Job Name box displays a default name for this import job. You can change this name.

3. In the **Notes** field, enter any notes about this job.

4. Click **Next**.

   The system displays the **Import Licenses Wizard** dialog box.

5. Use the **Browse** button to select the CSV file that contains the licenses you want to import.

6. Click **Next**.

   The system displays the **Add Templates** dialog box.

7. If you want to distribute templates with the licenses, select the appropriate template types. The last template of the selected type that was sent to this device will be resent with the licenses. (The IP addresses in this license file will be matched to the existing IP Office devices in Avaya Network Management Console.)

8. Click **Next**.

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

9. Specify when you want to run this job, and then click **Next**.

   The system displays the **Job Options** dialog box.

10. Specify how you want to run this job, and then click **Next**.

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

11. Click **Next** to start the import.

    A progress dialog box appears. When the job is complete, the Finish Up dialog box appears.

12. Click the **Finish** button.

Backing up Provisioning and Installation Manager files

During a backup session, files are archived in a zip file. The following Provisioning and Installation Manager for IP Office application files are included in a backup session:

- Profiles
- Templates
- Groups
- Jobs in the job queue or log— except running jobs
- System settings such as job queue, log retention, and system log file size

The backup session also provides a list of files and the Provisioning and Installation Manager for IP Office version.

To perform a backup:

1. From the Avaya Network Management Console window, select **Tools > Avaya Provisioning and Installation Manager For IPO Devices**.

   The system displays the **Provisioning and Installation Manager** window.
2. Click **+** in front of the **Administration** folder in the left panel.
3. Click **Backup/Restore**.

   The system displays the **Backup/Restore** page.
4. Click **Backup Now**.

   The system displays the **File Download** dialog box.
5. Click **Save**.

   The system displays the **Save As** dialog box.
6. Select the folder and filename for the backup file, and click **Save**.

   The system displays the **Download complete** dialog box.
7. Click **Close**.

Chapter 8: Backup and Restore of device configurations

The Avaya Configuration Backup Restore is an application that allows you to backup and restore device configurations and configure multiple devices. The Avaya Configuration Backup Restore uses Secure Copy Protocol (SCP), File Transfer Protocol (FTP), or Trivial File Transfer Protocol (TFTP) to exchange information with the devices in the network.

To use the FTP or SCP protocols, install an appropriate server on an accessible management station, and the username, password, and path to the server must be specified in the File Transfer Protocols tab of the Options dialog box.

This chapter includes the following topics:

Note:

In this chapter, ‘uploading’ always refers to information being copied from the device to the application, and ‘downloading’ always refers to information being copied from the application to the devices.

Starting the Avaya Configuration Backup Restore

To start the Avaya Configuration Backup Restore from the server on which Avaya Configuration Backup Restore is installed, select **Tools > Avaya Configuration Backup Restore**.

To start the Avaya Configuration Backup Restore from a web browser:

1. Using Microsoft Internet Explorer, go to the Integrated Management Launch page, and click **Configuration Backup Restore** in the Maintenance section.

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

2. In the **User Name** field, enter your user name.
3. In the **Password** field, enter your password.

4. Click **Login**.

   The system displays the **Avaya Configuration Backup Restore** window.

Setting the Avaya Configuration Backup Restore options

Using the **Options** dialog box, you can configure the Avaya Configuration Backup Restore options.

1. Start the Configuration Backup Restore. For information on how to start the Configuration Backup Restore, see Starting the Avaya Configuration Backup Restore on page 83.
2. Select **File > Options**. The system displays the **Options** dialog box to the General tab.
3. Click **Default Report Path** and browse to the directory in which you want the Avaya Configuration Backup Restore to save reports.
4. Select the desired report format from the **Format Of Report File** pull-down list box. The Avaya Configuration Manager can create text reports in **CSV (Comma Separated Value)** and **Tab Delimited Format**.
5. Select the desired default action from the **Default Action When Downloading** pull-down list box. The possible actions are:
   - **Request Confirmation** - A confirmation dialog box appears asking you to confirm the download.
   - **Do Not Request Confirmation** - The Avaya Configuration Backup Restore will start the download without requesting confirmation.
6. Click **...** in the **Path to Diff Program** section and browse to the directory with the software you want Avaya Configuration Backup Restore to use to compare configuration files.
7. Click **File Transfer Protocols** on the options dialog box and enter the fields in the tab. The following table provides a list of the fields in the File Transfer Protocols tab of the **Options** dialog box and their descriptions.

Table 4: The Configuration Backup Restore - Options

Field	Description
SCP Global Use	The state of SCP usage for Avaya Configuration Backup Restore. Possible values: • **Enabled** - SCP is used for devices that support SCP. Devices that do not support SCP use FTP if FTP Global Use is enabled, otherwise TFTP is used. • **Disabled** - SCP is not used. FTP is used for all devices if FTP Global Use is enabled, otherwise TFTP is used.
SCP User Name	A user name defined on the SCP server. This is the SCP user that the Avaya Configuration Backup Restore will use.
SCP Password	The password defined on the SCP server for the configured SCP user.
Retype SCP Password	The password defined on the SCP server for the configured SCP user. Retype the SCP Password.
SCP Server Secure Path	The path to the root of the secure path configured on the SCP server.
FTP Global Use	The state of FTP usage for Avaya Configuration Backup Restore. Possible values: • **Enabled** - If SCP is disabled, or SCP is not supported, then FTP is used for devices that support FTP. Devices that do not support FTP use TFTP. • **Disabled** - FTP is not used. If SCP is disabled, or a device does not support SCP, then TFTP is used.
FTP User Name	A user name defined on the FTP server. This is the FTP user that the Avaya Configuration Backup Restore will use.
FTP Password	The password defined on the FTP server for the configured FTP user.
Retype FTP Password	The password defined on the FTP server for the configured FTP user. Retype the FTP Password.
FTP Server Path	The path to the root of the secure path configured on the FTP server.

Click **Apply** to save the changes made in the File Transfer Protocols tab of the Options dialog box.

Click **Refresh** to undo all changes made in the Options dialog box. All unsaved changes to the dialog box are discarded.

Saving device configurations

This section explains how to save the device configurations. The Avaya Configuration Backup Restore enables you to manually save the configurations of selected devices and to create backup jobs for automatically saving the configuration of all or some of the devices listed in the Device Table. The Device Table lists discovered devices and displays information about them.

This section includes the following topics:

- Saving a device configuration - Instructions on how to manually save a voice network device's configuration to a file.
- Creating a backup job - Instructions on using the Backup Wizard.

Saving a device configuration

To save a device's configuration to a file in the library:

1. Start the Avaya Configuration Backup Restore.
2. Click the **Backup** tab to display the Device table.
3. Select a device in the Device Table.

   Note:

   You can upload the configurations of several devices by selecting them before you open the Upload dialog box.
4. Select **Actions > Upload**. The system displays the **Upload** dialog box showing one row for each configuration type found in the selected device.
5. Select the configuration types you want to upload.
6. Click **Upload**. The system displays a progress bar above the Upload button, and the upload begins.

The progress bar next to each configuration type shows the progress of the upload of that configuration. The progress bar that appears above the Upload button shows the progress of the entire upload.

Creating a backup job

The Backup Wizard provides a simple method of backing up the configurations of all or some of the devices in your network. In addition, using the Backup Wizard, you can schedule periodic automated backups. This can help you maintain an archive of your devices' configurations over time.

Note:

If you configure a backup job from a workstation working via remote access, the backup files are saved on the server.

To create a new backup job:

1. Start the Avaya Configuration Backup Restore.
2. Click **Backup** Tab to display the Device table.
3. Select the Avaya Aura™ Communication Manager device from the table.
4. Select **Action > Backup**. The system displays the **Welcome** screen.
5. Click **Next**. The system displays the **Device to upload from** screen. Choose Selected devices option to backup the configuration of the Communication Manager devices selected in the Device Table.
6. Click **Next**. The system displays the **File types to upload** screen. Select the configuration types you want to back up. To select or deselect a configuration type, click on the row displaying the configuration type.
7. Click **Next**. The system displays the **Immediate or Delayed** screen. Choose one of the following options:
   - **Immediate** - The current backup is performed once, and the backup job's options are not saved.
   - **Periodic** - The current backup will be performed at user defined periods, and the backup job's options are saved.
8. When you have selected a job type, click **Next**.

   If you selected **Immediate** the Summary Screen appears. Go to step 12.

   If yo selected **Periodic**, the Job Name screen appears. Go to step 9.
9. Enter a name of the backup job in the **Job Name** field.
10. Click **Next**. The system displays the **Period Parameters** screen. To configure the frequency and time of backups:

    a. Select an hour from the **Start hour** pull-down list box to configure the start time for the backup job.

    b. Choose one of the following options in the Recurrence Pattern section of the dialog box to configure the basis of the recurrence pattern:
       - **Daily** - The backup job will be performed every x days.
       - **Weekly** - The backup job will be performed every x weeks.
       - **Monthly** - The backup job will be performed every x months.

    c. Finish configuring the recurrence pattern by doing one of the following:
       - If you selected **Daily** option, enter a number in the **Every x day(s)** field.
       - If you selected **Weekly** option:

1. Enter a number in the **recur every x week(s) on** field.
2. Select the check boxes next to the days of the week on which you want the backup job to run.

- If you selected **Monthly** option:

1. Enter a number in the **Day x** field. This is the day of the month on which the backup job will run. If the day does not exist in a given month, (example, the 30th day of February), the last day of the month will be substituted.
2. Enter a number in the **Every y month(s)** field.

d. Enter a starting date in the **Start date** field.

e. Select an end of the recurrence range for the backup job. Possible range ends are:

- **No end date** - The backup job runs until it is deleted.
- **End after x occurrences** - Enter a number. The backup job runs x times, where x is the number entered.
- **End by** - Enter a date. The backup job runs until the date entered.

11. Click **Next**. The system displays the **Summary** screen.
12. Click **Submit**.

Downloading configuration files

This section explains how to download configuration files to the devices in the Device Table. It includes the following topics:

- Downloading - Provides instructions on how to download a configuration file to a device.
- Creating a restore job - Provides instructions on how to create a restore job for delayed downloading.

Downloading

Note:

When you download a file, the protocol used appears in the log. For information about configuring the download protocol, see Setting the Avaya Configuration Backup Restore options on page 84.

To download a configuration file to one or more devices:

1. Start the Avaya Configuration Backup Restore.
2. Click **Restore** Tab to display the Library table.

3. Select the configuration file you want to download to one or more devices.
4. Select **Action > Download**. The **Download** dialog box displays the file name and source and possible destinations of the file.
5. Select the modules or devices to which you want to download the selected configuration file.

   The **Possible Destinations** list contains a list of all modules and devices to which it is appropriate to download the selected configuration file. The configuration file is only downloaded to modules and devices in the **Selected Destinations** list. You can add modules or devices to Selected Destination list from the Possible Destinations list. You can also remove modules or devices from Selected Destination list. For more information, refer to the *Avaya Integrated Management Configuration Backup Restore* online help.
6. Configure the reset after download option.

   Some devices need to be reset after a download in order for the downloaded configuration to take effect. Using the Download dialog box, you can instruct the device to be reset when the download is completed.

   - To automatically reset the device after the download, select the **Reset After Download** check box.
   - If you do not want the device to reset after the download, clear the **Reset After Download** check box.
7. Click **Download**. The system displays the **Download Confirmation** dialog box.

   Note:

   > If **Default Action When Downloading** is configured to **Do Not Request Confirmation**, the **Download Confirmation** dialog box does not open.

   - If the modules or device in the **Selected Destinations** list match the module or device from which the configuration file was uploaded exactly, a confirmation dialog box appears with information about the configuration file and the selected devices.
   - If the modules or devices in the **Selected Destinations** list do not exactly match the module or device from which the configuration file was uploaded exactly, a warning message appears at the bottom of the dialog box. For example, this can occur when the device types are the same, but the modules or devices have different expansion modules or when a configuration file has been edited manually.
   - To download the configuration file to the selected device, click **Proceed**. The selected configuration file is downloaded to the modules or devices in the **Selected Destination** list.

   Note:

   > Once the download process begins, it cannot be stopped.

   CAUTION:

   > If an inappropriate configuration file is downloaded to a module or a device, you may lose contact with the device's agent.

- To edit the configuration file with the Configuration Editor, click **Edit file**. The Configuration Editor appears. After editing the file, you can initiate the download process from the Configuration Editor. For more information on the Configuration Editor, refer to the section **Editing Configuration Files** of the *Avaya Integrated Management Configuration Backup Restore* online help.
- To cancel the download, click **Cancel**. The download is cancelled.
- If the configuration was manually edited, the system displays the **Download Warning** dialog box. To download the file, click **Yes**. The file is downloaded to the selected devices.

Creating a restore job

The Restore Wizard provides a simple method of restoring the configurations of one or more of the devices in your network. You can perform immediate restores to solve problems or schedule delayed restores during convenient off hours.

Note:

If you configure a restore job from a workstation working via remote access, the backup files must have been saved on the server.

To create a new restore job:

1. Start the Avaya Configuration Backup Restore.
2. Select **Action > Restore**. The system displays the **Welcome** screen.
3. Click **Next**. The system displays the **Search Devices** screen.
4. Choose one of the following options:
   - Specify **Device Name**, **IP Address**, and/or select a group from the **Select Group** drop-down list for the devices.
   - Specific **Device Type** by checking the devices.
5. Click **Next**. The system displays the **Search files to restore** screen. Enter a **Backup Job Name** to select files from that backup. Select files by date if desired. Check the **File Types** to restore.
6. Click **Next**. The system displays the **Select File** screen. Select the version of files to be restored.
7. Click **Next**. The system displays the **Execution Details** screen. Enter a name for the restore job in the **Job Name** field. (A name will be generated if you do not specify one.) Select an immediate or scheduled execution time. Click on "..." to set date and time for scheduled execution. Clear the check box for Reset if you do not want to automatically apply the changes when downloaded.
8. Click **Nex**t. The system displays the **Summary** screen.

9. Click **Finish**.

For more information on topics like Device table, Library table, Editing Configuration files, Comparing Configuration files, Generating reports, Filtering tables and Managing jobs, refer to *the Avaya Integrated Management Configuration Backup Restore* online help.

Chapter 9: Backup and Restore of administered data of Network Management applications

Overview

This Chapter provides instructions on how to backup your Network Management Console and Provisioning and Installation Manager database and administered data and settings using the NM Backup Utility and restoring the backup using NM Easy Restore Utility. For more information, see NM Backup Utility on page 20.

This Chapter includes the following topics:

- Backing up the data using the NM Backup Utility wizard on page 93
- Restoring the data using NM Easy Restore Utility on page 96

You can also refer *to* the *Avaya Integrated Management Release 6.0 Network Management Console User Guide* for more information.

Backing up the data using the NM Backup Utility wizard

To backup your Network Management Console and Provisioning and Installation Manager database and administered data and settings:

1. Launch the Avaya NM Backup Utility.

   Click **NM Backup Utility** on the launch page

   Or

   Select **Tools > Avaya NM Backup Utility** from the Network Management Console window. The system displays the **NM Backup Utility** window.

   For information on how to start the Network Management Console, see Starting the Network Management Console on page 35.

2. Perform steps 2 to 5 if you want to set default FTP/NM server parameters. These parameters will be used as defaults while setting up the backup job. Steps 2 to 5 are optional.

3. Select **File > Options** from the NM Backup Utility User Interface. The system displays the **Options** dialog box.

4. Enter the Server parameters in the **Options** dialog box.
5. Click **Apply**. The parameters are saved. These parameters will be used as defaults while setting up a backup job.

   For information on the fields in the Options dialog box, refer to Table 5

Table 5: NM Backup Utility Options Dialog Box Parameters

Parameter	Description
FTP Server IP Address	IP address of the FTP server
FTP Port	The port number
User Name	FTP user name
Password	FTP password
Retype Password	Retype the password as in **Password** field.
FTP Backup Directory Path	Path relative to the FTP home directory on the server, where you want to save the backup archive on the FTP server.
NM Backup Directory Path	Absolute path of the directory where you want to save the backup archive on NM server.

6. Select **Action > Backup**. The system displays the **NM Backup Wizard**.
7. Click **Next**. The system displays the **Configure Backup Items** dialog box.

   a. Enter a name for the Backup in the **Backup Name** field.

   Note:

   > The name of the backup archive will be formed as: **Backupname_MMMMM.dd.yyyy.HHmmss**. For example, if you enter the backup name as '**test**' then the name of the backup archive will be **test_July.28.2008.123244.zip** where the date and time reflects the date and time when the backup job executes.

   b. Select **NMC Data and Settings**, **PIM Data and Settings**, and **PIM for IPO Data and Settings**.By default all three applications are selected. You can clear the **PIM for IPO Data and Settings** checkbox if you have not installed PIM for IPO.

8. Click **Next**. The system displays the **Select Backup Destination** dialog box.
9. By default, the parameters configured in the Options dialog box appear here. You can change the parameters if you want to save the backup to a different location.
10. Click **Next**. The system displays the **Select Job Type** dialog box.
11. You can schedule the backup job to run immediately or periodically.

    To run the backup immediately:

    a. Select **Immediate**.

b. Click **Next**. Go to step 12.

To run the job periodically:

a. Select **Periodic**.

b. Click **Next**. The system displays the **Schedule Backup Job** dialog box.

c. Select the time when you want to start the backup from the `Start hour` drop-down list under the **Job Start time** section of the dialog box.

d. Perform one of the following steps under the Recurrence Pattern section of the dialog box:

- If you want to schedule the backup daily, select **Daily**.

  If you want to schedule the backup at fixed intervals (days), enter a value in the **Every day(s)** field. For example, If you want to schedule the backup every two days, enter **2**.

- If you want to schedule the backup weekly, select **Weekly**.

  Choose the day of the week on which you want to schedule the backup. If you want to schedule the backup to run at fixed intervals (weeks), enter a value in the **recur every week(s)** field. For example, if you want to schedule the backup every two weeks, enter **2**.

- If you want to schedule the backup monthly, select **Monthly**.

  Type the day of the month on which you want to schedule the backup in the **Day** field. For example, if you want to schedule the backup to run on the first of every month enter **1**. If you want to schedule the backup to run at fixed intervals (months), enter a value in the `of` **every month(s)** field. For example, if you want to schedule the backup on day one after every two months then enter **1** in the **Day** field and **2** in the **of every months(s)** field.

e. Click **Start Date** under the **Range of recurrence** section of the dialog box. The calendar is displayed. Select the start date for the backup.

f. Perform one of the following steps under the **Range of recurrence** section of the dialog box:

- If you want to end the schedule for backup after a fixed number of occurrences, select **End after occurrences**. Enter the number or occurrences in this field. For example, if you want to end the schedule after 15 occurrences, enter **15** in this field.

- If you want to end the schedule for backup on a particular date, select **End by**. Click **End Date**. The calender is displayed. Select the end date.

- If you do not want to specify an end date for the schedule, select **No end date**. By default this option is selected.

g. Click **Next**. Go to step 12

12. Once you choose the options to schedule the backup, click **Next**. The system displays the **Summary** dialog box.

    The summary dialog box displays the following information:

- **Backup Name** – This displays the name of the Backup you entered in the Configure Backup Items dialog box.
- **Application Types** – This displays the application you choose to backup in the Configure Backup Items dialog box.
- **Backup Destination** – This displays the backup destination you choose in the Select Backup Destination dialog box.
- **Schedule Information** - This displays the schedule information you choose in the Schedule Backup Job dialog box.

13. Click **Submit**. The wizard is closed and a row is added for this backup job in the jobs list appearing on the left of the screen.

    The job will run at scheduled intervals and the progress percentage will be updated in the status column. When the job is complete, the status column will be updated with message **’Job Succeeded. Stored in archive: test_July.28.2008.123244.zip’.**

    If the job fails the status message will say **‘Job Failed:** reason for failure’

    When the job succeeds, the archive is created at the backup location you entered while setting up the backup job. There is also a text file present at the location with the same name of archive (for example, test_July.28.2008.123244.txt), which lists the applications which are backed up in the archive, the NM version and other useful information for future reference.

    This text file is not required during restore. You can safely delete it if you wish. The archive need not be at the same location for restore to succeed and it is safe to move archive to different locations, if required.

    WARNING:

    Please do not modify the contents of the archive. Even if you just unzip and recompress the archive without any modifications, the restore may fail.

Restoring the data using NM Easy Restore Utility

Do the following to restore your backup.

Note:

The restore can only be done on the same NM Server from where backup was taken.

Only Windows Administrators can restore the data.

1. Select **Start > All Programs > Avaya > Tools > NM Easy Restore Utility** from the NM server. The system displays the **NM Easy Restore** Utility window.

Note:

The NM Easy Restore Utility can be launched only from the NM Server.

2. Depending on the server you chose to store the backup file you can choose to restore the data using the NM Easy Restore Utility.
   - To restore the backup from the file stored on the NM server:
   - To restore the backup from the file stored on the FTP server:

To restore the backup from the file stored on the NM server:

1. Select **NM Server** from the NM Easy Restore Utility window.
2. Click **Browse** and navigate to the directory where you saved the recent backup zip file and select the Backup Zip file.
3. Check **Recover PostgresSQL database using write ahead logs (WAL)** only if you have selected the most recent backup zip file for restore. For more information on the Recover PostgresSQL database using write ahead logs (WAL), see Recovering the PostgreSQL database using write ahead logs (WAL) on page 97.
4. Click **Restore**. The restore operation will start. The status will be updated in the log window. Once the restore operation is completed successfully, you can close the restore utility and start Avaya services from **Start > Program Files > Avaya > Start Avaya Services**.

To restore the backup from the file stored on the FTP server:

1. Select **FTP Server** from the NM Easy Restore Utility window.
2. The FTP parameters entered during the Backup process are displayed.
3. Select the Backup Zip file that you want to restore from the directory where you saved it.
4. Check **Recover PostgreSQL database using write ahead logs (WAL)** only if you have selected the most recent backup zip file for restore. For more information on Recover PostgreSQL database using write ahead logs (WAL), see Recovering the PostgreSQL database using write ahead logs (WAL) on page 97.
5. Click **Restore**. The restore operation will start. The status will be updated in the log window. Once the restore operation is completed successfully, you can close the restore utility and start Avaya services from **Start > Program Files > Avaya > Start Avaya Services**.

   Note:

   If Avaya Services are already running then it is stopped when you click **Restore**. You can start it after the restore operation is completed successfully.

Recovering the PostgreSQL database using write ahead logs (WAL)

The Recover PostgresSQL database using write ahead logs (WAL) option is used to restore the PostgreSQL database to the current state with all the entries in it.

The Network Management Console (NMC) use the PostgreSQL database to store the data. The database gets installed automatically during the Network Management installation. When you backup the data using the NM Backup Utility the data from the PostgreSQL database also gets backed up.

When you restore the backed up data using the NM Easy Restore utility, all the data entered in the database after the backup operation is not included in the restore. It is lost. However, it is possible to recover this data using the PostgreSQL database feature called WAL (Write Ahead log) archiving.

Using this feature, PostgreSQL remembers the date and time you took the last backup and all the data entered thereafter is maintained separately in a log file called “write ahead log” (WAL) in its internal directories.

During restore, if ‘**Recover PostgresSQL database using write ahead logs (WAL)**’ is selected, the NM Easy Restore utility attempts to restore this data using the latest WAL file along with the backed up data bringing the database to the current state with all the entries in it.

Following conditions should be met for successful restore using the Recover PostgresSQL database using write ahead logs (WAL) option:

- The backup archive you restore from should be the latest backup taken. This is necessary because the current WAL files are with respect to the latest backup date and time. If you choose an old backup archive the entries in the WAL file cannot be restored.
- The application should not be reinstalled after the backup. If you reinstall the application anytime after backup, the WAL files stored by database get deleted and hence you will not be able to restore the database in the current state. In such case, the database will be restored to the same state as it was during backup. The restore utility does not report any error even if the WAL files are not in expected sequence.

Note:

You can use the NM Backup Utility to take backup of data and settings of Network Management Console, Provisioning and Installation Manager for Gateways, and Provisioning and Installation Manager for IP Office applications. Of these only Network Management Console uses the PostgreSQL database. Recover PostgresSQL database using write ahead logs (WAL) option has no significance for Provisioning and Installation Manager (PIM) applications restore.

Do not select the option "**Recover PostgresSQL database using write ahead logs (WAL)**" if the last restore attempt failed.

Appendix A: Supported Devices

Table 6 provides a list of Avaya Network Management applications and shows the devices that are supported by each application.

Table 6: Supported Devices for the Avaya Network Management Applications

Application	Supported Devices
Avaya Network Management Console	**Communication Manager:** Avaya Aura(TM) Communication Manager, Avaya Communication Manager Express, Avaya HS20, Avaya S8100, Avaya S8300, Avaya S8400, Avaya S8500, Avaya S8700, Avaya VAL, CLAN, Definity Audix, Intuity Audix, SES. **Media Gateways and Switches:** C360, C360 Router-if, G250, 250BRI, 250DCP, G250DS1, G350, G430, G450, G700, G860 LpMedia 5000, G860 LpMedia 8000, G860 Lpat 5000, G860 Lpat 8000, G860 Mediant 5000, G860 Mediant 8000, P330, P330 Router-if, TGM550. **IP Office:** IP406-V2, IP412, IP500, IP500 V2, Small Office 2T+4A, Small Office 4T+4A+8DS, Small Office 4T+8A. **Phones:** Avaya 1603, Avaya 1608, Avaya 1616, Avaya 16CC, Avaya 4601, Avaya 4602, Avaya 4606, Avaya 4610, Avaya 4611, Avaya 4612, Avaya 4616, Avaya 4620, Avaya 4621, Avaya 4622, Avaya 4624, Avaya 4625, Avaya 4626, Avaya 4627, Avaya 4630, Avaya 4690, Avaya 9610, Avaya 9620, Avaya 9630, Avaya 9640, Avaya 9650, Avaya 9670G, Avaya SIP9620, Avaya SIP 9630, Avaya SIP 9640. **Partner Devices:** Juniper J2320, Juniper J2350, Juniper J4350, Juniper J6350, Polycom MGC 100, Polycom MGC 100 PLUS, Polycom MGC 25, Polycom MGC 25 PLUS, Polycom MGC 50, Polycom MGC 50 PLUS, Polycom RMX 2000, Polycom VSX, CISCO2501, CISCO2502, CISCO2503, CISCO2504, CISCO2505, CISCO2506, CISCO2507, CISCO2508, CISCO2509, CISCO2510, CISCO2511, CISCO2512, CISCO2513, CISCO2514, CISCO2515, CISCO2516, CISCO2517, CISCO2518, CISCO2519, CISCO2520, CISCO2521, CISCO2522, CISCO2523, CISCO2524, CISCO2525, CISCO2610, CISCO2611, CISCO2612, CISCO2620, CISCO2621, CISCO2650, CISCO2651, CISCO3620, CISCO3640, CISCO3661, CISCO3662, CISCO7204, CISCO7206, CISCO7505, CISCO7507, CISCO7513, CISCO7576, Extreme Alpine 3802, Extreme Alpine 3804, Extreme Alpine 3808, Extreme Black Diamond 6800, Extreme Black Diamond 6804, Extreme Black Diamond 6808, Extreme Black Diamond 6816, Extreme BlackDiamond 10808, Extreme BlackDiamond 12802, Extreme BlackDiamond 12804, Extreme BlackDiamond 8806, Extreme BlackDiamond 8810, Extreme Summit 200 stack, Extreme Summit 200-24, Extreme Summit 200-48, Extreme Summit 300-24 POE,

Table 6: Supported Devices for the Avaya Network Management Applications (continued)

Application	Supported Devices
Avaya Network Management Console	**Partner Devices:** Extreme Summit 300-48, Extreme Summit 400-24f Extreme Summit 400-24p, Extreme Summit 400-24t, Extreme Summit 400-48t, Extreme Summit 450-24t, Extreme Summit 450-24x, Extreme Summit Stack, Extreme Summit WM200, Extreme Summit X150-24p, Extreme Summit X150-24t, Extreme Summit X150-48t, Extreme Summit X250-24x, Extreme Summit X250e-24p, Extreme Summit X250e-24t, Extreme Summit X250e-48p, Extreme Summit X250e-48t, Extreme Summit X450a-24tDC, Extreme Summit X450a-24x, Extreme Summit X450a-24xDC, Extreme Summit X450a-48tDC, Extreme Summit X450e-48p, Extreme Summit1, Extreme Summit1iSX, Extreme Summit1iTX, Extreme Summit2, Extreme Summit24, Extreme Summit24e2SX, Extreme Summit24e2TX, Extreme Summit24e3, Extreme Summit3, Extreme Summit4, Extreme Summit48, Extreme Summit48i, Extreme Summit48si, Extreme Summit4fx, Extreme Summit5i, Extreme Summit5iLX, Extreme Summit5iTX, Extreme Summit7iSX, Extreme Summit7iTX, Extreme SummitPx1, Extreme SummitX450a-24t, Extreme SummitX450e-24p, Motorola SCCAN Server. **Others:** ATM-if, Generic Media Controller, I55 ACB Compact I55 ACB IEE3, 55 ACB Standard, LU's Xedia AP, X330W-2DS1, X330W-2USP.
Avaya SMON Manager	**P330:** Avaya G700, Avaya P332G-ML, Avaya P332GT-ML, Avaya 332MF, Avaya 333R, Avaya 333T-PWR, Avaya P334T, Avaya P334T-ML. **G250:** G250, G250BRI, G250DSI, G250DCP. **C360:** C363T, C364T, C363T-PWR, C364T-PWR.

Table 6: Supported Devices for the Avaya Network Management Applications (continued)

Application	Supported Devices
Avaya Configuration Backup Restore	**P330:** Avaya G700, Avaya P332G-ML, Avaya P332GT-ML, Avaya 332MF, Avaya 333R, Avaya P333RLB, Avaya P333T, Avaya 333T-PWR, Avaya P334T, Avaya P334T-ML. **C360:** C363T, C364T, C363T-PWR, C364T-PWR. **G250:** G250-BRI, G250-DS1, G250-DCP. **G350:** Avaya G350. **G430:** Avaya G430. **G450:** G450. **TGM 550** TGM 550. **WAN** X330W-2DS1, X330W-2V35, X330W-4V35, X330W-2USP.

Table 6: Supported Devices for the Avaya Network Management Applications (continued)

Application	Supported Devices
Avaya Software Update Manager	**P330:** Avaya G700, Avaya P332G-ML, Avaya P332GT-ML, Avaya 332MF, Avaya 333R, Avaya 333T-PWR, Avaya P334T, and Avaya P334T-ML. **G250:** G250-BRI, G250-DS1, G250-DCP. **G350:** Avaya G350, Avaya Integrated Analog, Avaya MM312, Avaya MM710, Avaya 710B, Avaya MM711, Avaya MM714, Avaya MM714B, Avaya MM716, Avaya MM717, Avaya MM720, and Avaya MM722. **G430:** Avaya G450, Avaya MM710, Avaya MM710B, Avaya MM711, Avaya MM712, Avaya MM714, Avaya MM714B, Avaya MM716, Avaya MM717, Avaya MM720, Avaya MM722, Avaya MP10, Avaya MP70, Avaya MP80. **G450:** Avaya G450, Avaya MM710, Avaya MM710B, Avaya MM711, Avaya MM712, Avaya MM714, Avaya MM714B, Avaya MM716, Avaya MM717, Avaya MM720, Avaya MM722, Avaya MP10, Avaya MP70, Avaya MP80. **C360:** C363T, C364T, C363T-PWR, C364T-PWR. **G700:** Avaya G700-MGP, Avaya G700-VOPI, Avaya MM710, Avaya MM710B, Avaya MM711, Avaya MM712, Avaya MM714, Avaya MM714B, Avaya MM716, Avaya MM717, Avaya MM720, Avaya MM22, Avaya MM60. **Media Servers** Avaya Aura(TM) Communication Manager, S8300, S8300C, S8300D, S8400, S8500, S8500B, S8500C, S8510, S8700, S8710, S8720, S8730, S8800. **TN Boards:** TN2214CP, TN2224CP, TN2302AP, TN2312AP, TN2312BP, TN2313AP, TN2464BP, TN2464CP, TN2501AP, TN2602AP, TN2793B, TN464GP, TN464HP, TN744FP, TN771DP, TN793CP, TN797AP, TN799DP, TN8400AP, TN8412AP. **IP Office:** IP406-V2, IP412, IP500, IP 500-V2, Small Office 2T+4A, Small Office 4T+8A, Small Office 4T+4A+8DS.

Table 6: Supported Devices for the Avaya Network Management Applications (continued)

Application	Supported Devices
Avaya Provisioning and Installation Manager for Gateways	G250, G250-DCP, G250-BRI, G250-DS1, G350, G430, G450, TMG550.
Avaya Provisioning and Installation Manager for IP Office	**IP Office:** IP406-V2, IP412, IP500, IP 500-V2, Small Office 2T+4A, Small Office 4T+8A, Small Office 4T+4A+8DS, IP406-V2, IP412, IP500, IP500 V2, Small Office 2T+4A, Small Office 4T+4A+8DS, Small Office 4T+8A.

Index