Avaya Solution & Interoperability Test Lab

Configuring Avaya Integrated Management Network Management for Centralized Administration of Avaya IP Office to Support the Avaya Chain Store Management Solution – Issue 1.0

Abstract

These Application Notes describe the procedures required for configuring selected applications from the Avaya Integrated Management Network Management suite to centrally manage Avaya IP Office systems in a distributed network environment. Specific applications in the Avaya Integrated Management Network Management suite are used to support the Avaya Chain Store Management solution for Avaya IP Office.

Avaya Network Management Console, Avaya Secure Access Administration and Avaya Software Update Manager are standalone applications from the Avaya Integrated Management Network Management suite that are provisioned in these Application Notes for managing Avaya IP Office systems at multiple locations. These Application Notes will encompass administration tasks for each standalone application to perform software upgrades for Avaya IP Office systems in a sample network configuration.

1. Introduction

These Application Notes describe the procedures required for configuring selected applications from the Avaya Integrated Management Network Management suite to centrally manage Avaya IP Office systems in a distributed network environment. Specific applications in the Avaya Integrated Management Network Management suite are used to support the Avaya Chain Store Management (CSM) solution for Avaya IP Office. Avaya Network Management Console (NMC), Avaya Secure Access Administration (SAA) and Avaya Software Update Manager (SUM) are standalone applications from the Avaya Integrated Management Network Management suite that are provisioned in these Application Notes for managing Avaya IP Office systems at multiple locations.

The NMC application performs the network discovery of managed devices and establishes the SNMP parameters used for accessing Avaya IP Office. The NMC also serves as a launch point for all applications that are part of the Integrated Management Network Management suite in which both the SAA and SUM applications are launched. SAA is a centralized application for defining login credentials for authorized users and assigning privileges for accessing applications from the Avaya Integrated Management Network Management suite. SUM is an application that stores the latest software obtained from the Avaya Support web site and performs software upgrades for managed Avaya devices discovered by the NMC. The SUM application also analyzes the current software versions in use by managed devices and notifies the system administrator whenever a newer version is available. The Avaya IP Office Manager is installed with the Avaya Integrated Management Network Management suite and is used to administer SNMP parameters for the Avaya IP Office 406v2 and Avaya IP Office 412.

The diagram in **Figure 1** illustrates the network environment used to verify these Application Notes. The Main location contains a server hosting the Avaya Integrated Management Network Management suite that was installed to upgrade the Avaya IP Office systems at the Branch 1 and Branch 2 locations. Branch 1 hosts an Avaya IP Office 406v2 and Branch 2 hosts an Avaya IP Office 412 with WAN access to the Main at each location. The Main, Branch 1 and Branch 2 locations communicate through a Multi-Protocol Label Switched (MPLS) network simulating the WAN. The testing approach for these Application Notes is to confirm the upgrade for the Avaya IP Office 406v2 and Avaya IP Office 412 at the respective Branch locations using the Avaya Integrated Management Network Management suite over a simulated WAN.

With the exception of the components mentioned above, any configuration related to the underlying network infrastructure will not be covered. Also, these Application Notes provide a sample of administrative tasks that can be performed by the specified application in the Avaya Integrated Management Network Management suite and do not cover all their features and capabilities. Please see **Section 7** for additional references on configuration of CSM applications.

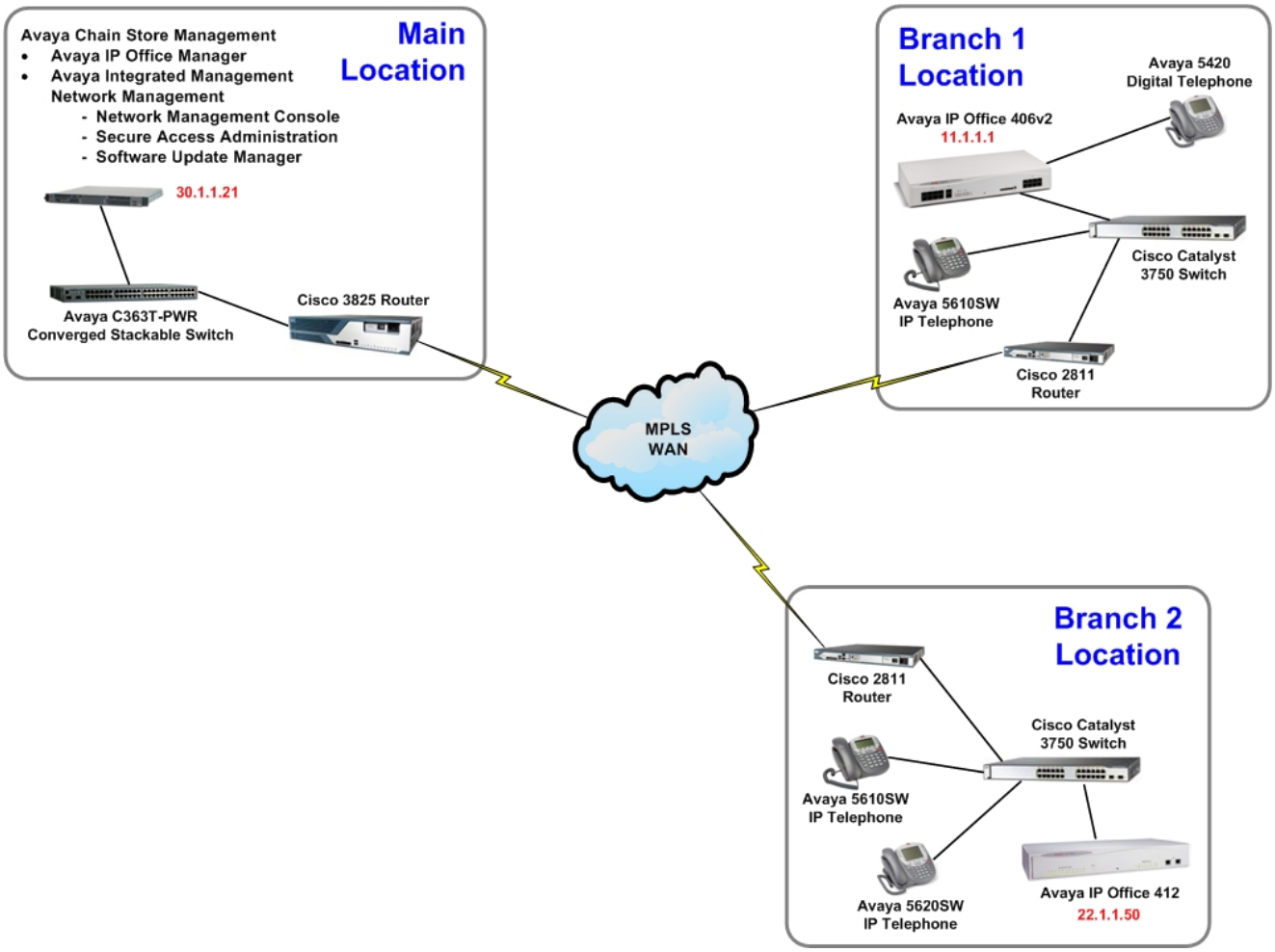


Figure 1: Network Configuration

2. Equipment and Software Validated

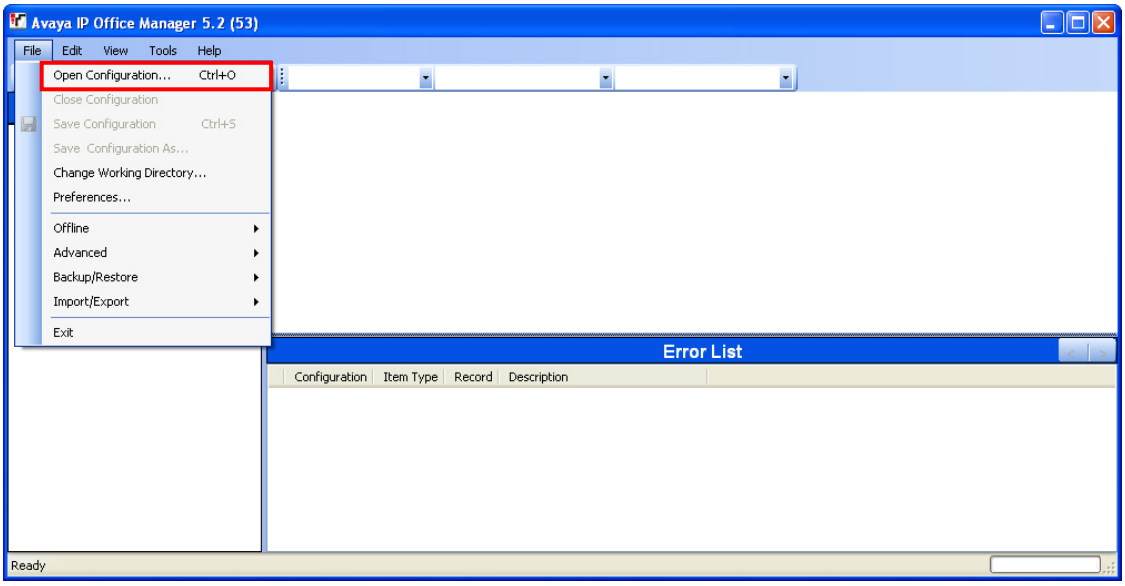
The following equipment and software were used for the sample configuration provided:

Equipment	Software	
Avaya Chain Store Management • Avaya Integrated Management Network Management ➢ Network Management Console (NMC) ➢ Secure Access Administration (SAA) ➢ Software Update Manager (SUM) • Avaya IP Office Manager	• Release 3.3.15 ➢ 3.3 ➢ 3.3.06 ➢ 3.3.09R1 • 5.2(53)	
Avaya IP Office • 406v2 • 412	**Starting Version** • 3.2(54) • 3.2(54)	**Ending Version** • 4.0(309) • 4.0(309)
Avaya 5610SW IP Telephone (2)	2.3	
Avaya 5620SW IP Telephone	2.3	
Avaya 5420 Digital Telephone	n/a	
Avaya C363T-PWR Converged Stackable Switch	4.5.14	
Cisco Catalyst 3750 Switch (2)	12.4	
Cisco 3825 WAN Router	12.4	
Cisco 2811 Access Router (2)	12.4	

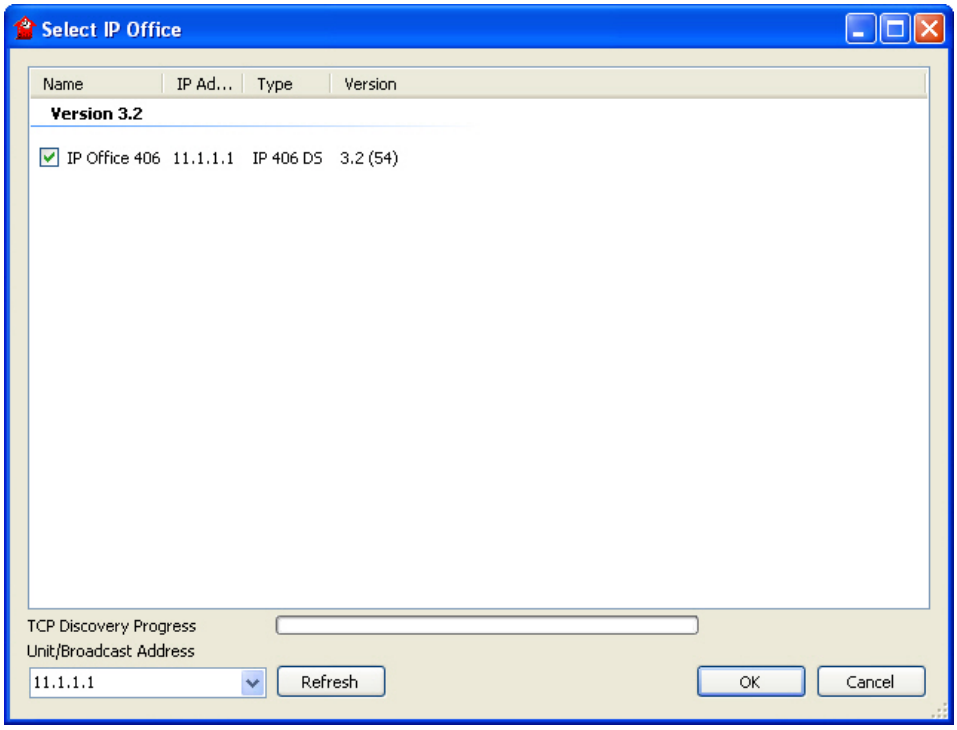
3. Configure Avaya IP Office

The following are the steps used to provision each Avaya IP Office system at the Branch locations from the Main location illustrated in **Figure 1**. The Avaya IP Office systems will be enabled for SNMP connectivity to support management functions performed by CSM applications. For brevity, this section will assume the viewer of these Application Notes has a basic understanding of Avaya IP Telephony and will not cover details regarding the initial configuration for Avaya IP Office.

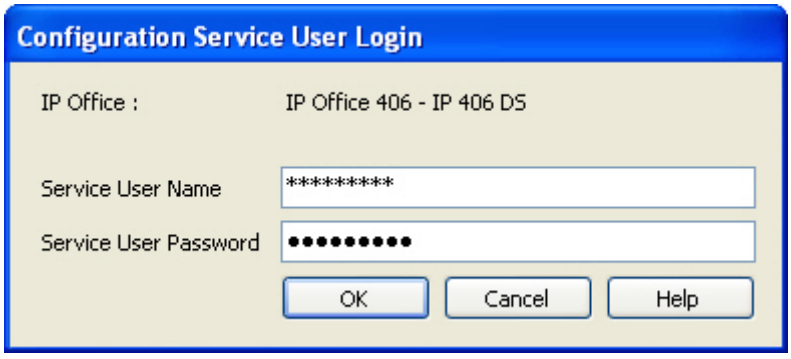
1. Open the Avaya IP Office Manager application from the server at the Main location. From the Avaya IP Office Manager, select the **File** option from the top menu and scroll to the **Open Configuration…** selection. This will open a new window displaying the Avaya IP Office systems available to the Avaya IP Office Manager.



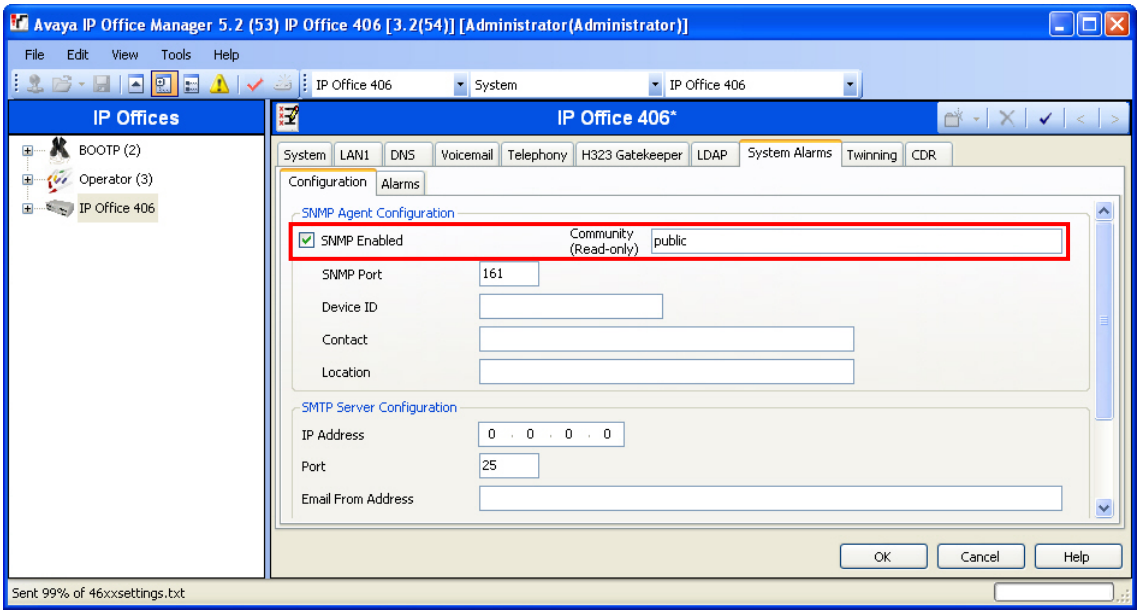
2. In the new window, mark the checkbox for the Avaya IP Office system slated for configuration. Click the **OK** button to display the authentication prompt for accessing the selected Avaya IP Office.



3. Enter valid login credentials at the authentication prompt. Click the **OK** button to display the opening page of the Avaya IP Office Manager application for the selected system.



4. At the opening page of the Avaya IP Office Manager, click **IP Office 406** from the left pane to display tabs for administering configuration parameters for the selected system. Click the **System Alarms** tab to display the default parameters used for SNMP configuration. Mark the checkbox for **SNMP Enabled** to enable the SNMP service and enter an ASCII string in the **Community (Read-only)** field to assign a SNMP community string for the selected system. Leave the remaining parameters at the default settings and click the **OK** button when finished.



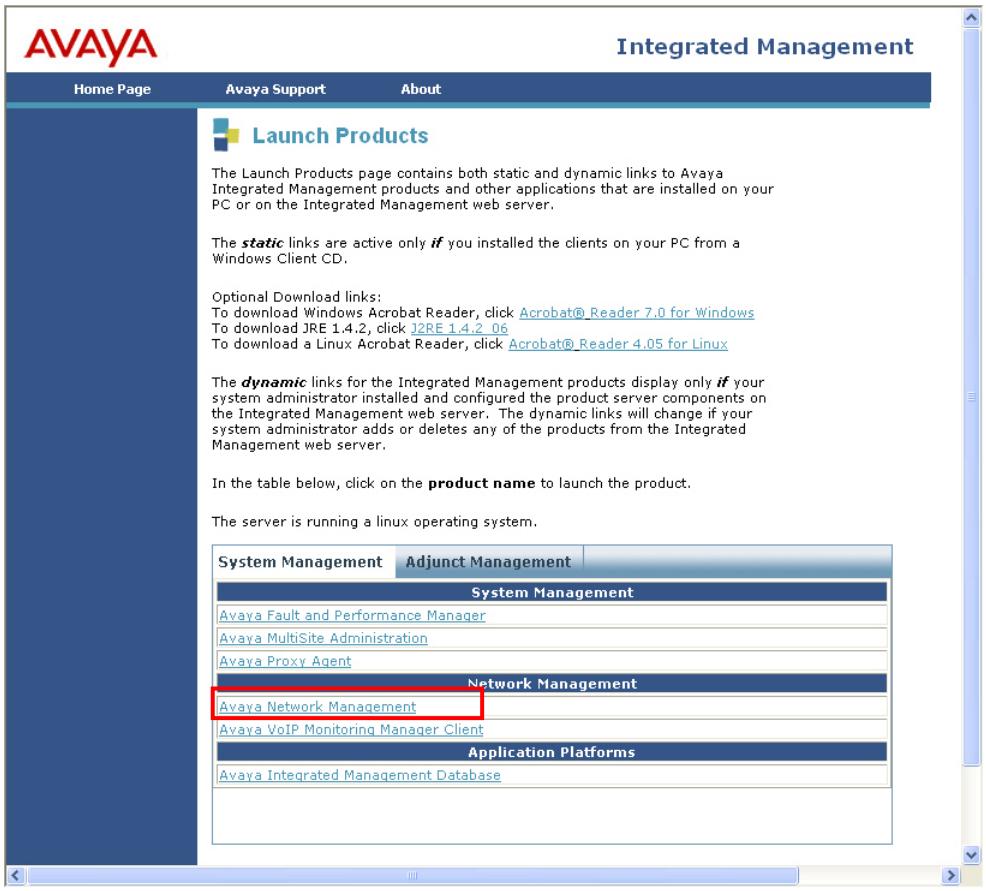
4. Configure Avaya Chain Store Management for Avaya IP Office

These Application Notes describe the configuration steps required to provision centralized management of Avaya IP Office using the designated CSM applications. Administrative procedures for the designated CSM applications are mentioned in the subsequent sections.

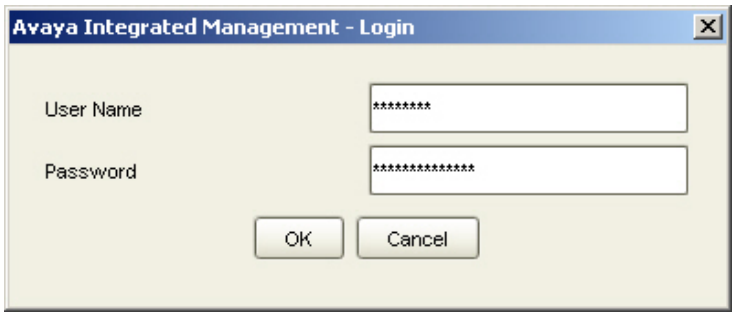
4.1. Configure Avaya Network Management Console

Listed below are the steps used to provision the Avaya Network Management Console with configuration parameters for network discovery of Avaya IP Office at the Branch locations illustrated in **Figure 1**.

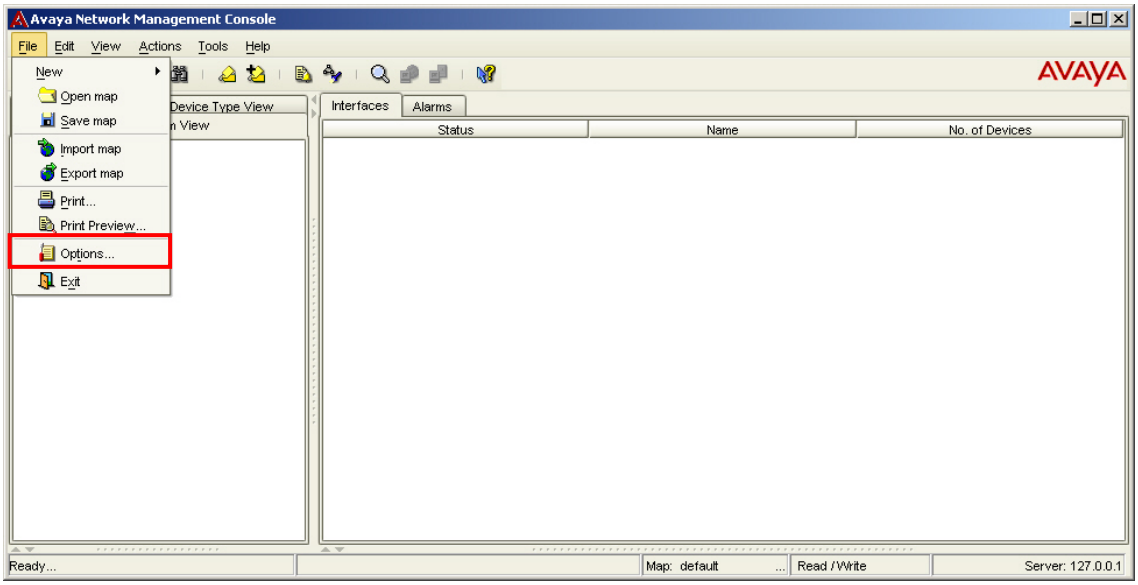
1. To access the Integrated Management Launch Products page, enter http://<a.b.c.d> at a web browser where a.b.c.d is the IP address of the server hosting the Avaya Integrated Management Network Management suite. Click on the link for **Avaya Network Management** under **Network Management** to open a new window for the NMC application.



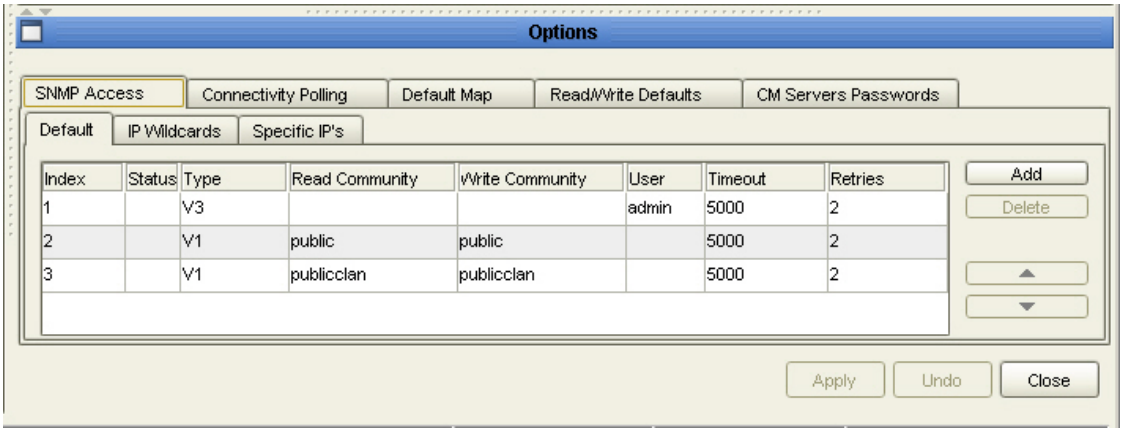
2. Enter valid login credentials at the authentication prompt. Click the **OK** button to display the opening page of the NMC application.



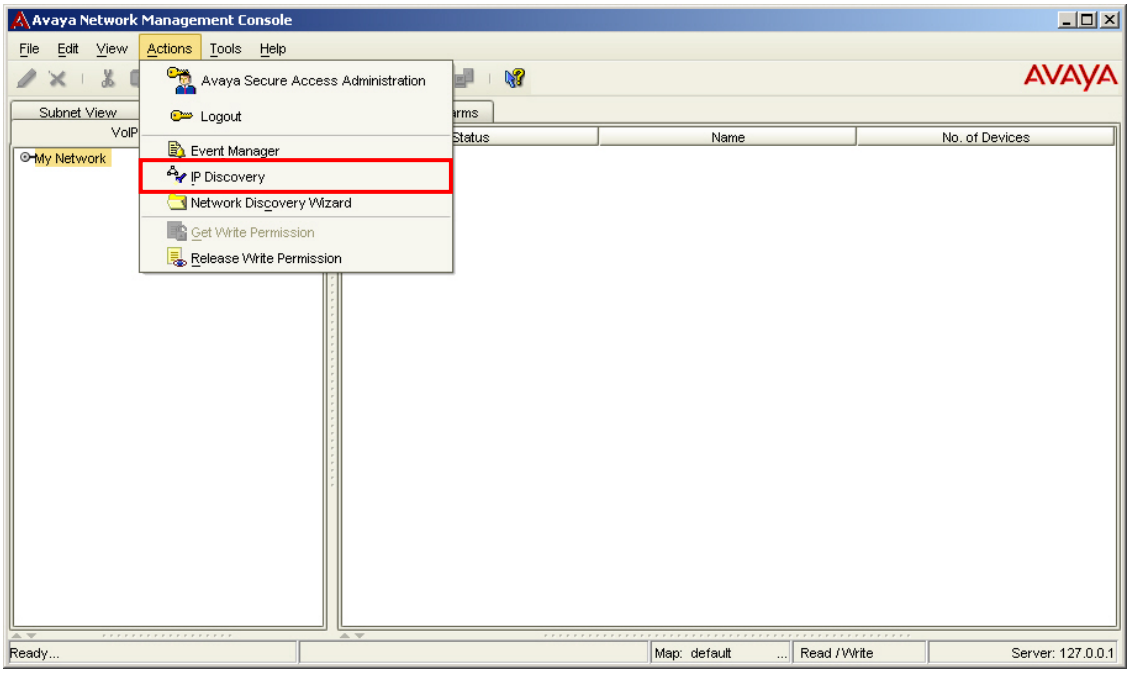
3. From the opening page of the NMC application, select the **File** option from the top menu and scroll to the **Options...** selection to open the Options window.



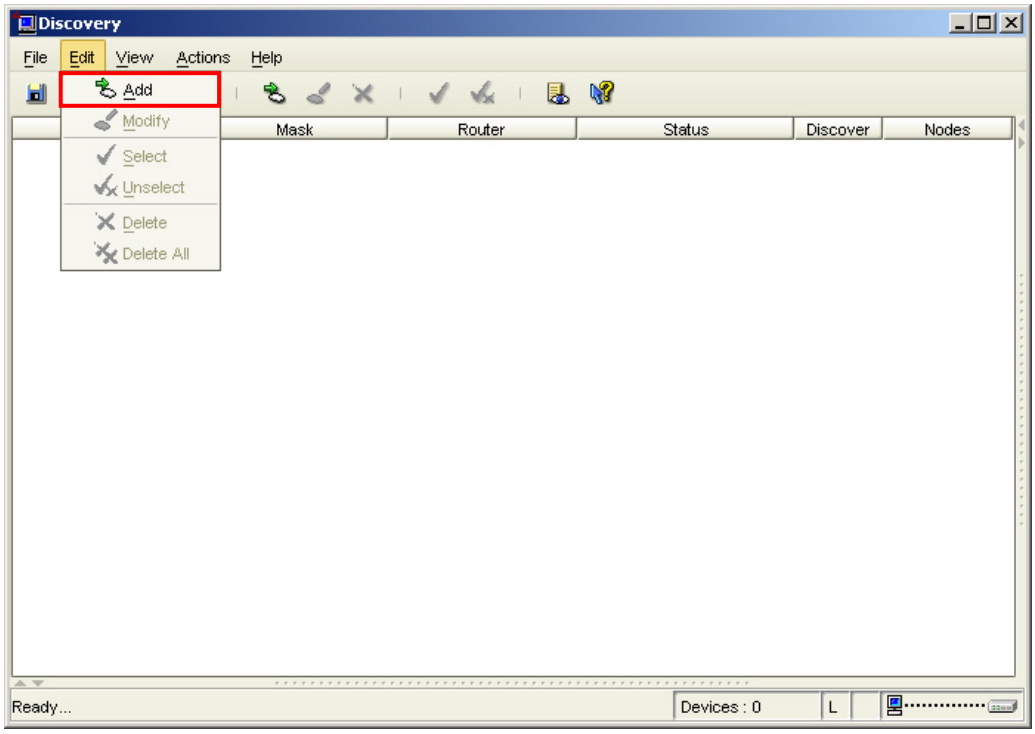
4. At the Options window, click the **SNMP Access** tab followed by the **Default** sub-tab to display the default SNMP parameters used for network discovery. Retain the initial default parameters used for network discovery or modify the parameters (community string, timeout values, etc.) to implement specific SNMP requirements used by managed devices. The community string configured under the **Read Community** column must match the community string defined in Step 4 of Section 3. Click the **Apply** button when finished.



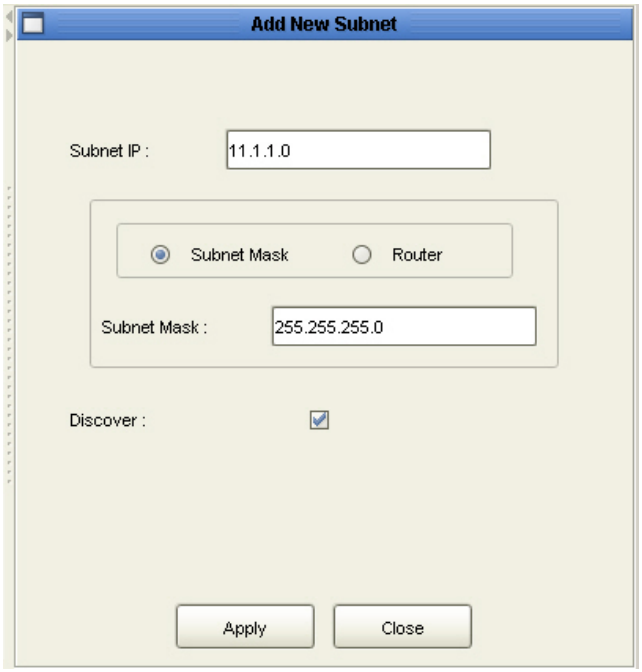
5. From the NMC application, select the **Actions** option from the top menu and scroll to the **IP Discovery** selection to open the Discovery window.



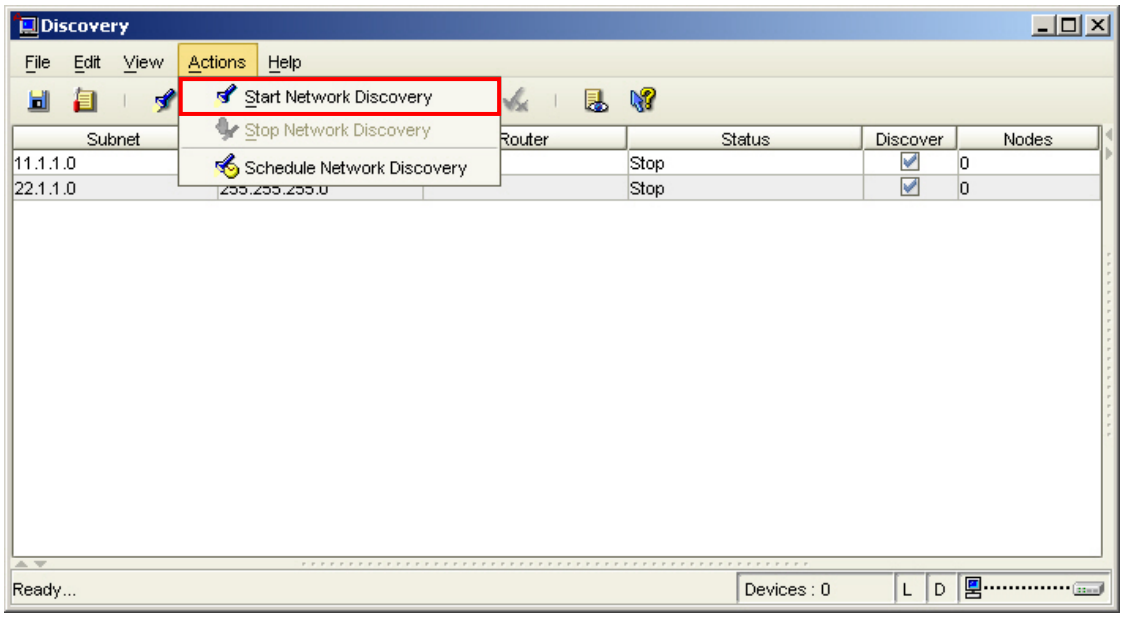
6. In the Discovery window, select the **Edit** option from the top menu and scroll to the **Add** selection. This will open the Add New Subnet window to add network prefixes hosting managed devices for discovery.



7. In the Add New Subnet window, enter the network prefix hosting an Avaya IP Office system in the **Subnet IP** field. Select the **Subnet Mask** radio button and enter the corresponding subnet mask in the **Subnet Mask** field for the network prefix entered. Mark the checkbox for **Discover** to enable discovery for the network prefix entered, then click the **Apply** button when finished. Repeat this step for each network prefix hosting managed devices that is designated for discovery by the NMC application.



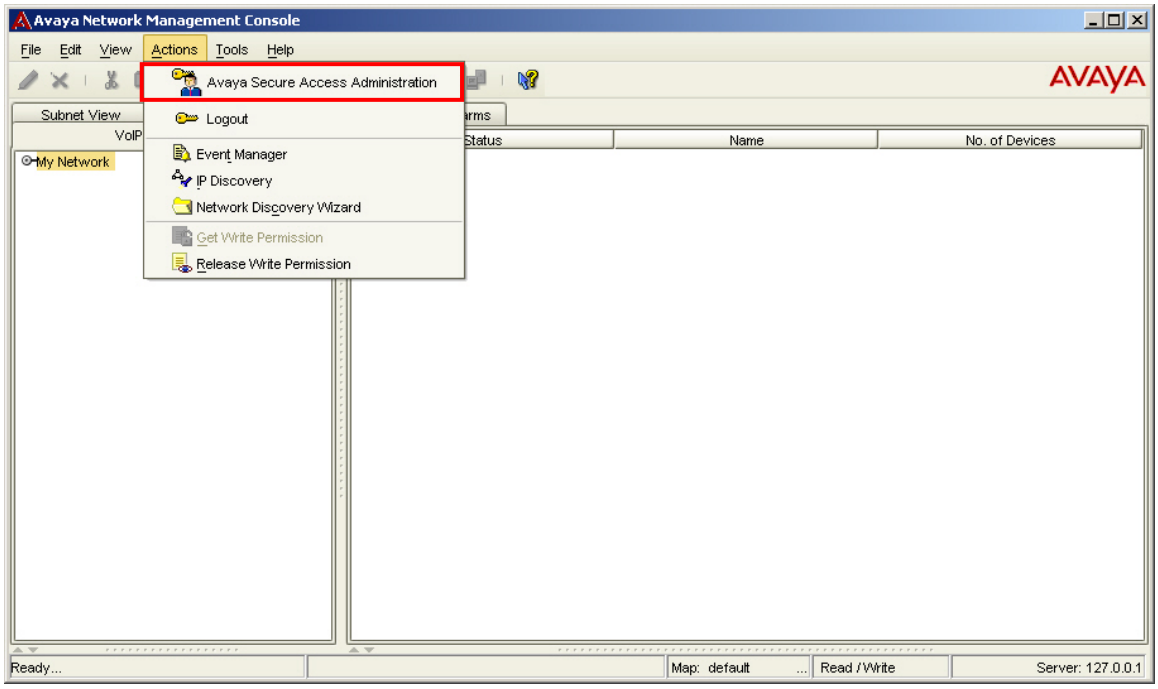
8. In the Discovery window, select the **Actions** option from the top menu and scroll to the **Start Network Discovery** selection. This selection will initiate the network discovery for detecting Avaya IP Office systems hosted in network prefixes defined in the previous step. The managed devices found during network discovery are updated in an internal database for the NMC and is referenced by other applications for administration.



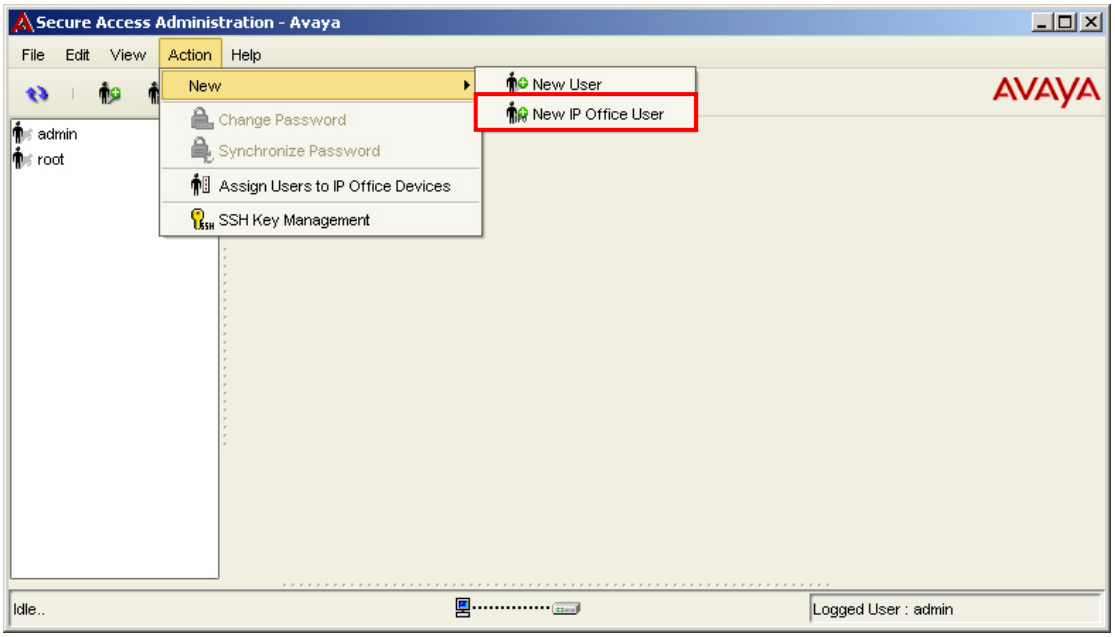
4.2. Configure Avaya Secure Access Administration

The following are the steps used to provision administrator privileges for authorized users with Avaya Secure Access Administration. For authorized users, administering SAA permits system configuration of Avaya IP Office systems at the Branch locations illustrated in **Figure 1**.

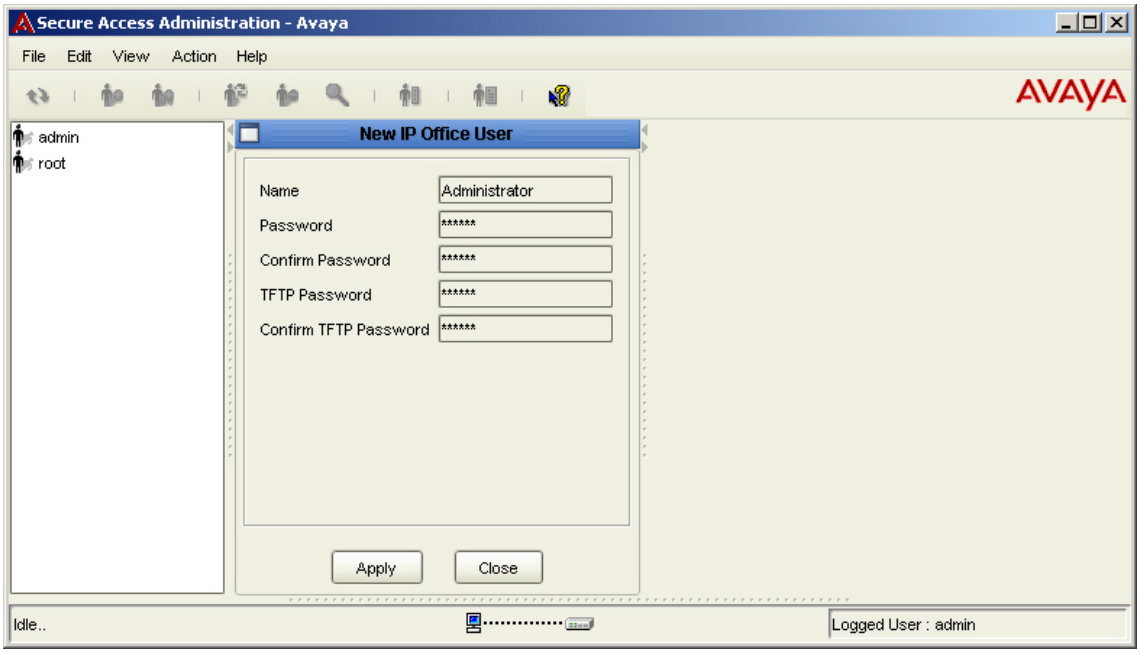
1. From the NMC application, select the **Actions** option from the top menu and scroll to the **Avaya Secure Access Administration** selection to open the SAA application.



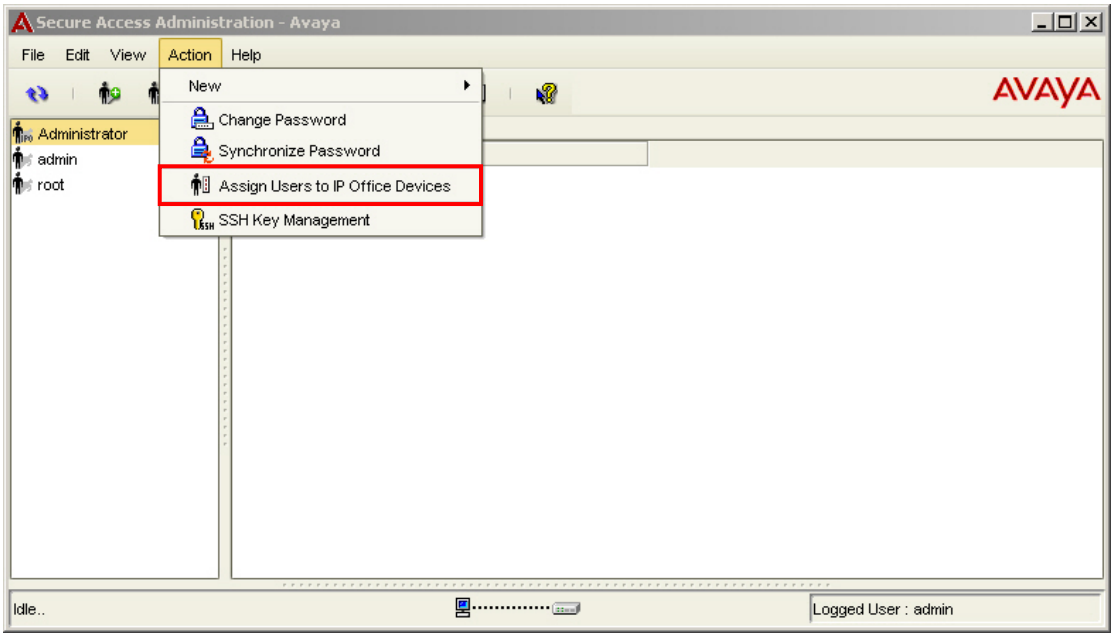
2. At the SAA application, navigate to the **Action > New** option from the top menu and scroll to the **New IP Office User** selection. The New IP Office User window will open in the SAA application to administer an authorized user for accessing Avaya IP Office.



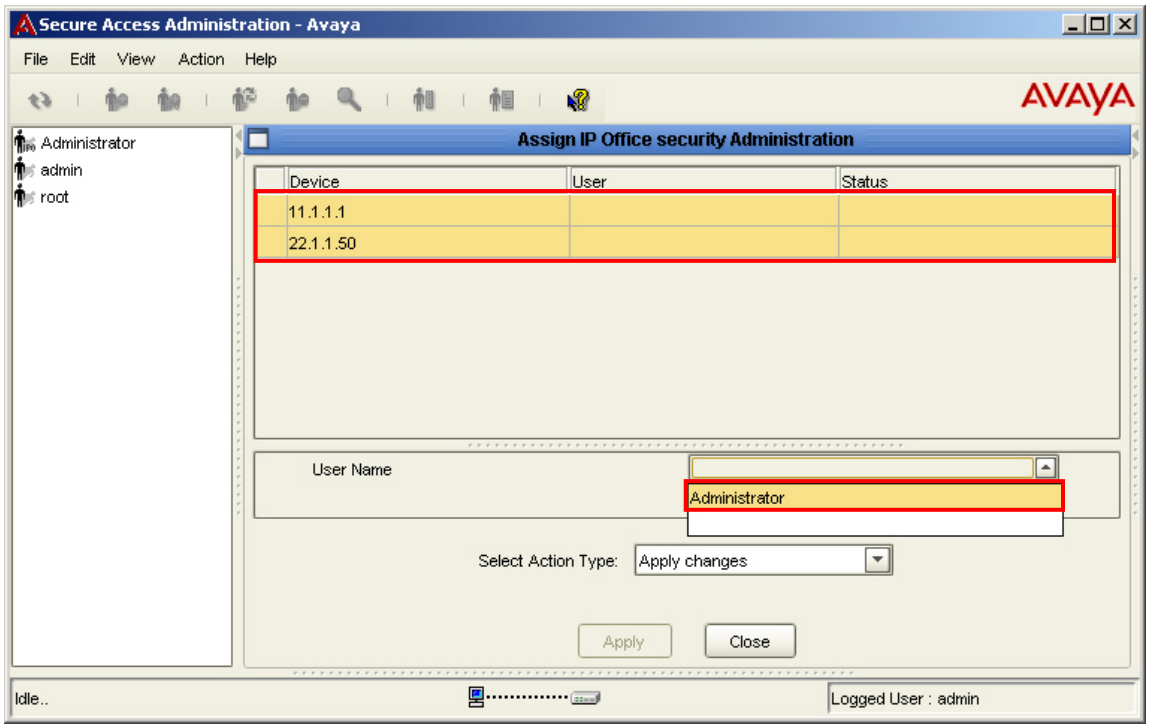
3. In the New IP Office User window, enter the name and password, in the respective fields, that will be used for accessing Avaya IP Office systems at the Branch 1 and Branch 2 locations. Enter the password, in the respective fields, used by Avaya IP Office for authenticating requests during TFTP downloads. Click the **Apply** button when finished to display the created user in the left pane of the SAA application.



4. Select the **Action** option from the top menu and scroll to the **Assign Users to IP Office Devices** selection. The Assign IP Office security Administration pane will open to assign access into Avaya IP Office systems for authorized users.

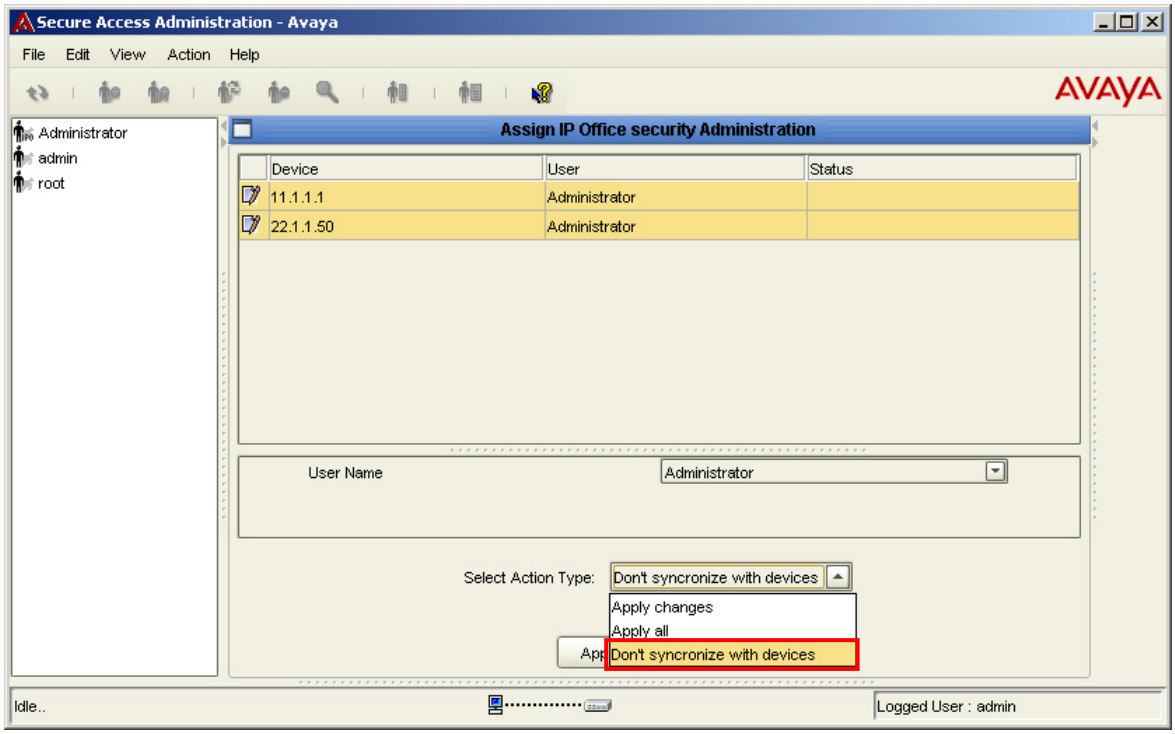


5. At the Assign IP Office security Administration pane, highlight the Avaya IP Office systems discovered in Step 8 of Section 4.1 to assign an authorized user. Select the user configured in Step 3 from the **User Name** drop-down list to populate the fields under **User** column for the highlighted Avaya IP Office systems.



6. At the Assign IP Office security Administration pane, select an option from the **Select Action Type** drop-down list. Click the **Apply** button when finished.

Note: *The SAA application does not support software version 3.2 for Avaya IP Office. The workaround for security administration in earlier versions of Avaya IP Office is to select the* ***Don't synchronize with devices*** *option from the* ***Select Action Type*** *drop-down list.*

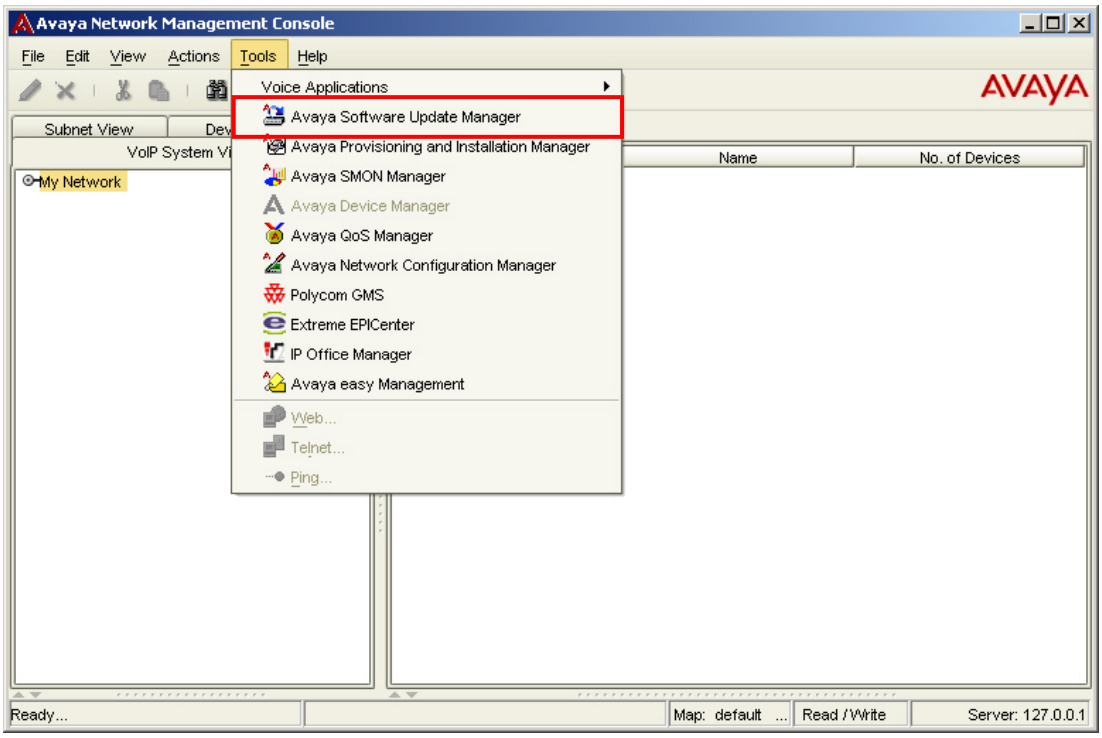


4.3. Configure Software Update Manager

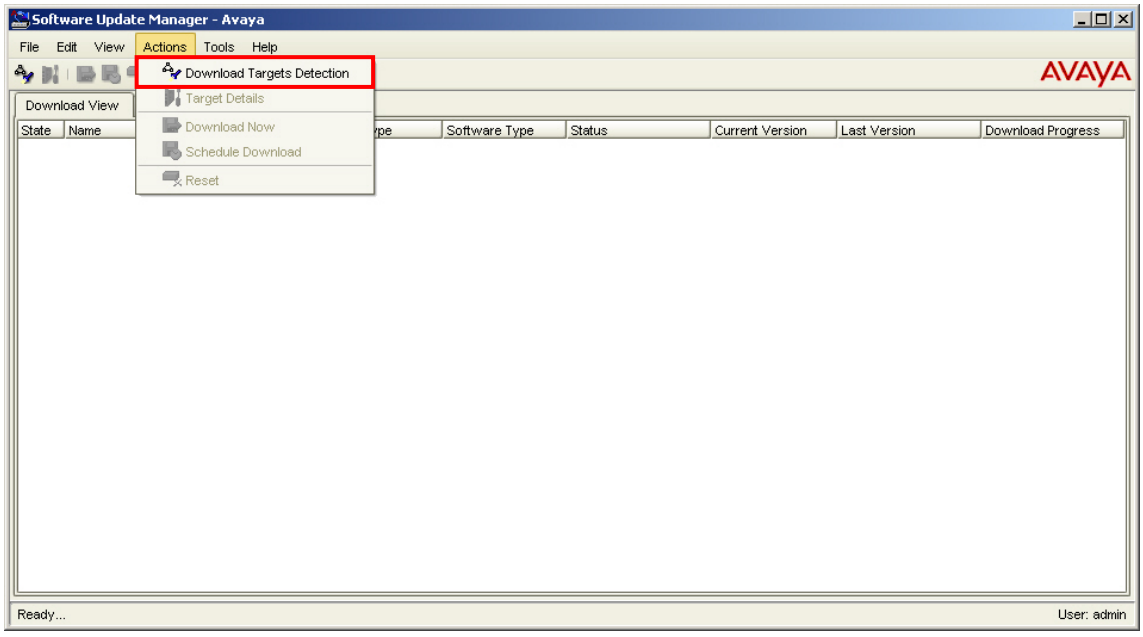
The following are the steps to configure the SUM application for software upgrades of Avaya IP Office at the Branch locations in **Figure 1**. The server hosting the Avaya Integrated Management suite, including SUM, will require Internet access for analysis of Avaya IP Office systems and for obtaining the latest software releases from the Avaya Support web site.

Note: *Before Avaya IP Office can be accessible for analysis and software upgrades by the SUM application, it must be discovered as a managed device in the NMC application.*

1. From the NMC application, select the **Tools** option from the top menu and scroll to the **Avaya Software Update Manager** selection to open the SUM application.

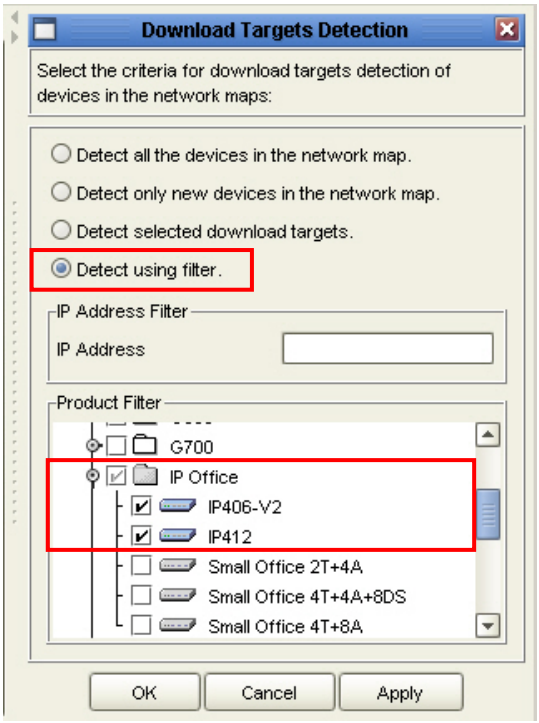


2. From the opening page of the SUM application, select the **Actions** option from the top menu and scroll to the **Download Targets Detection** selection. The Download Targets Detection window will open to select search criteria during network discovery of managed devices.

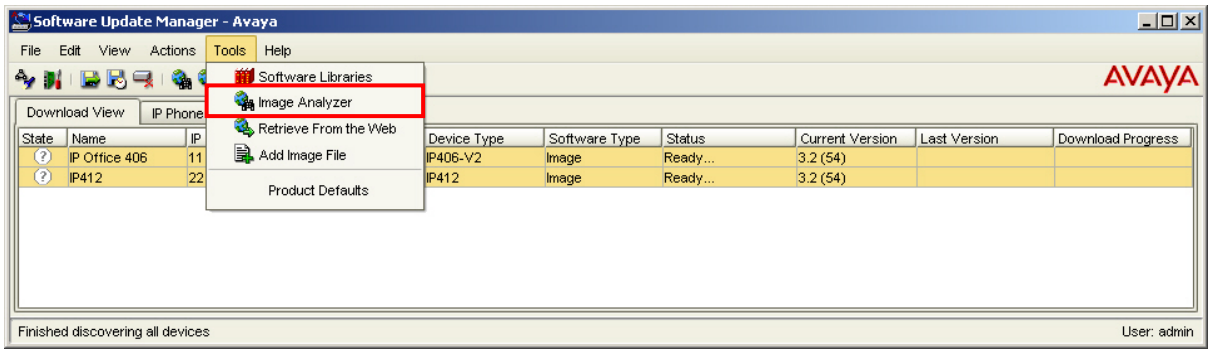


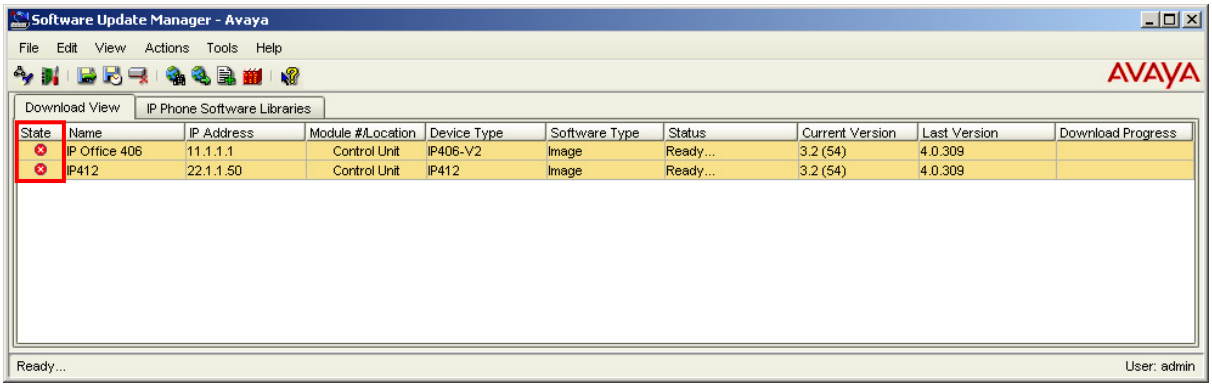
3. In the Download Targets Detection window, select the **Detect using filter** option to perform a network discovery based on Avaya product type. Alternatively, the **Detect all the devices in the network map** option can be selected to display all managed devices found during the initial network discovery performed by the NMC application. The search criteria given for Download Targets Detection is used to parse the managed devices found during the initial network discovery performed by the NMC application.

Under **Product Filter**, scroll the list of Avaya devices for the **IP Office** product family. Expand the **IP Office** product family and mark the corresponding checkbox for each Avaya IP Office product type hosted at the Branch locations in **Figure 1**. Click the **OK** button when finished to discover the selected Avaya IP Office systems under management by the NMC application.

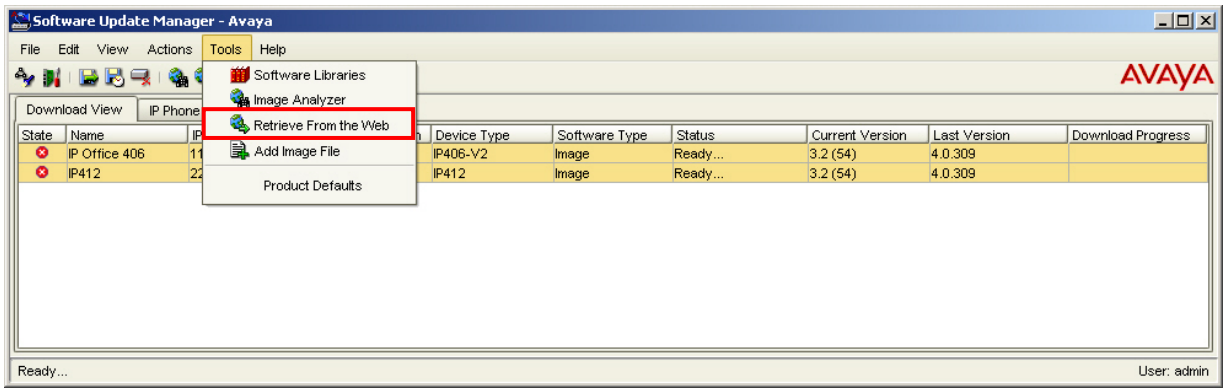


4. After performing the Download Targets Detection operation, select the **Tools** option from the top menu and scroll to the **Image Analyzer** selection. The Image Analyzer will compare the current software version found during the Download Targets Detection with the latest software version available at the Avaya Support web site. Verify the status icon is displayed under the **State** column. The status icon identifies the current software version as upgradeable and a newer version is available for download from the Avaya Support web site.

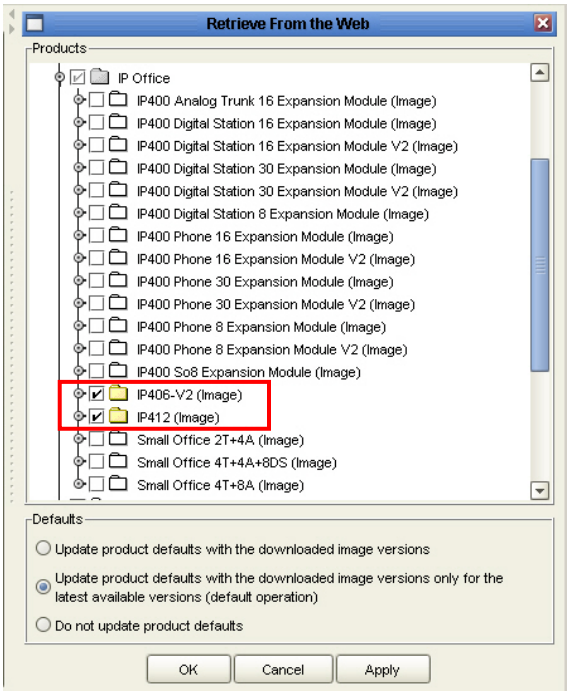


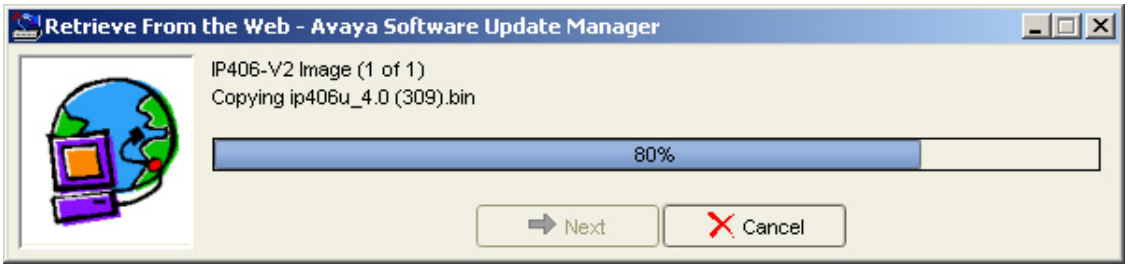


5. From the SUM application, highlight the Avaya IP Office systems discovered during the Download Targets Detection in Step 3. Select the **Tools** option from the top menu and scroll to the **Retrieve From the Web** selection to open a window displaying an Avaya product list with software available from the Avaya Support web site.

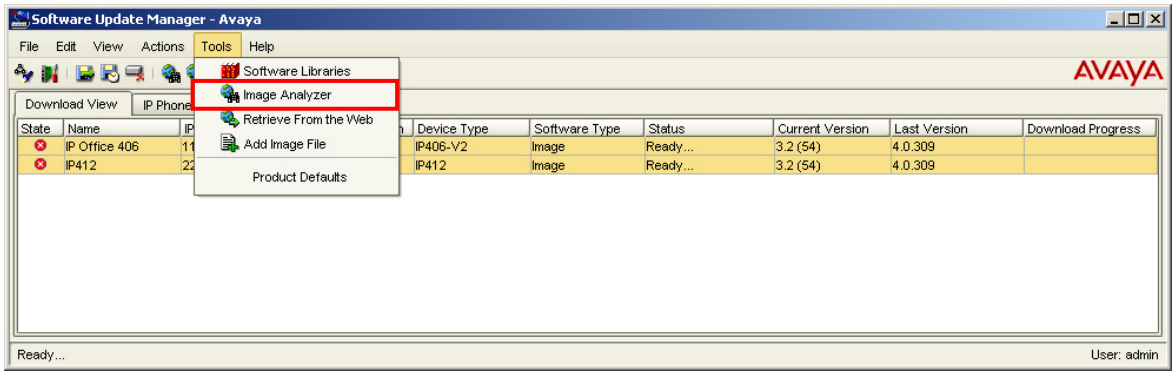


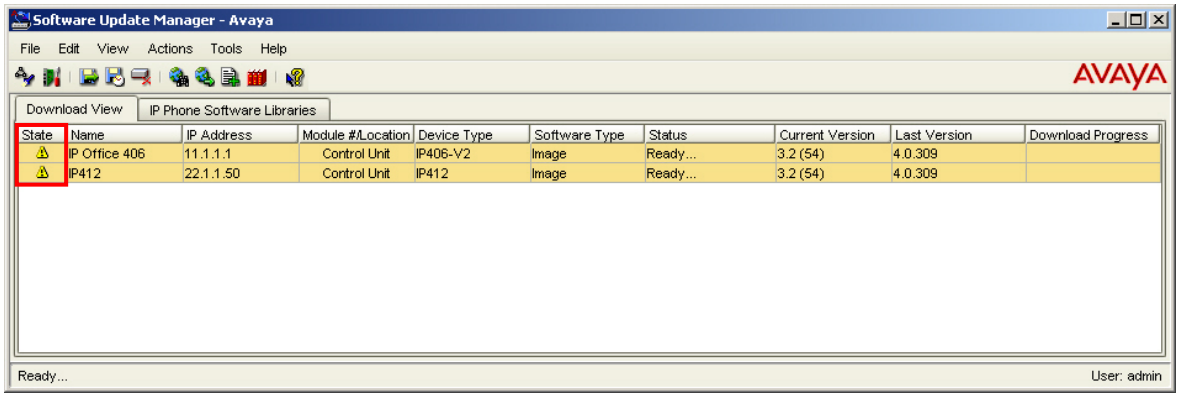
6. In the Retrieve From the Web window under **Products**, scroll the list of Avaya devices for the IP Office product family. Expand the **IP Office** product family and mark the corresponding checkbox of the software images for the respective Avaya IP Office product type. Leave the remaining parameters at the default settings and click the **OK** button when finished. This will open a dialog window displaying the software images being downloaded for the selected Avaya IP Office systems from the Avaya Support web site.



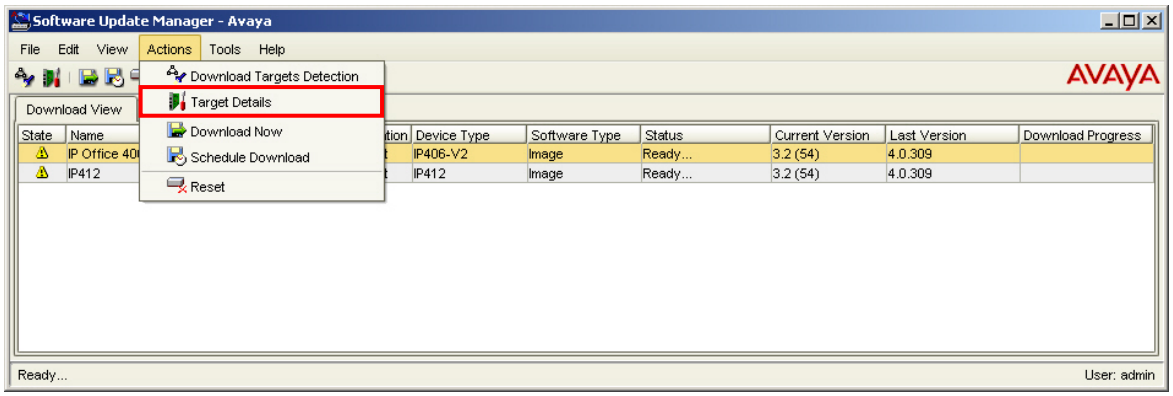


7. After downloading files for Avaya IP Office from the Retrieve From the Web operation, select the **Tools** option from the top menu and scroll to the **Image Analyzer** selection. The Image Analyzer will compare the current software version with the latest software version available at the Avaya Support web site. Verify the ⚠ status icon is displayed under the **State** column. The ⚠ status icon identifies the current software version as upgradeable with the newer version, downloaded in the previous step, which is available locally.

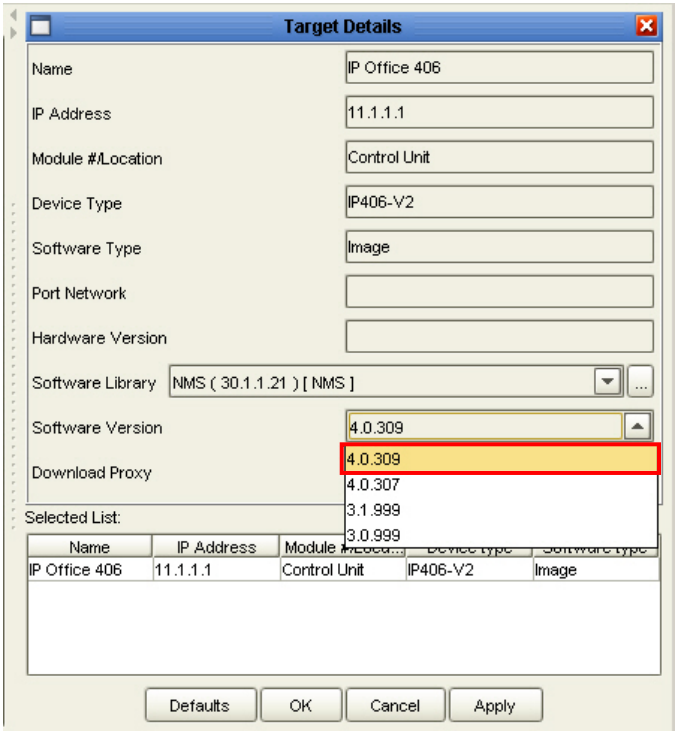




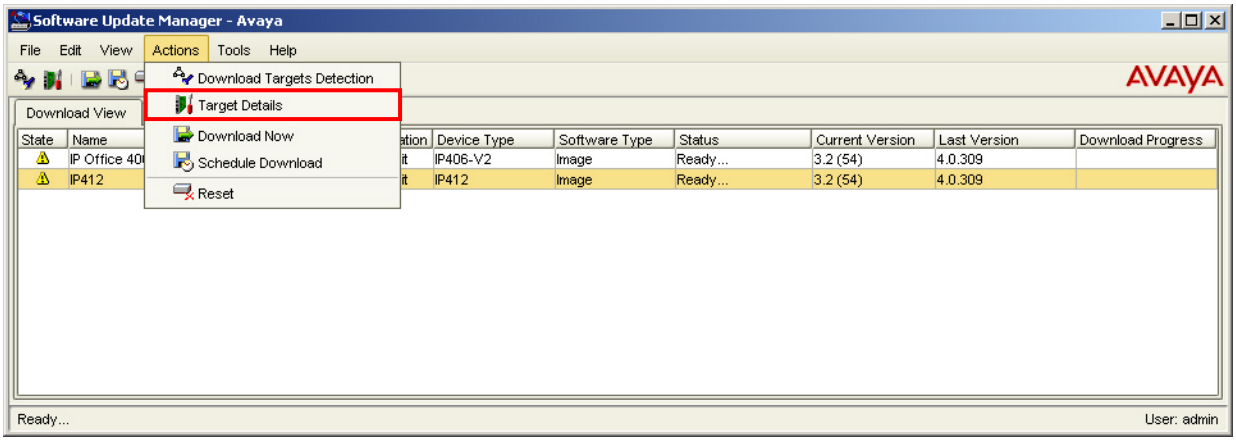
8. From the SUM application, highlight the Avaya IP Office 406v2 discovered during the Download Targets Detection in Step 3. Select the **Actions** option from the top menu and scroll to the **Target Details** selection. The Target Details window will open to provide configuration parameters for upgrading the Avaya IP Office 406v2 hosted at the Branch 1 location in **Figure 1**.



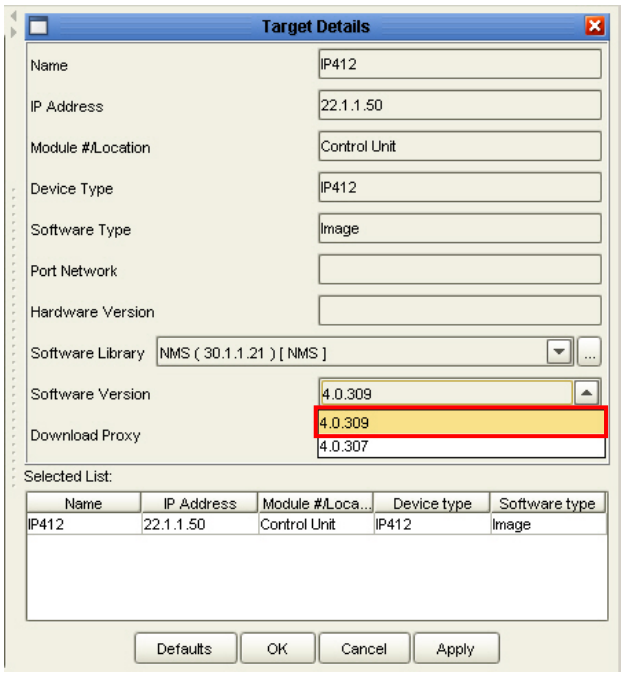
9. In the Target Details window, select the latest software release from the **Software Version** drop-down list to perform an upgrade using the software binaries downloaded in Step 6. Leave the remaining parameters at the default settings and click the **OK** button when finished.



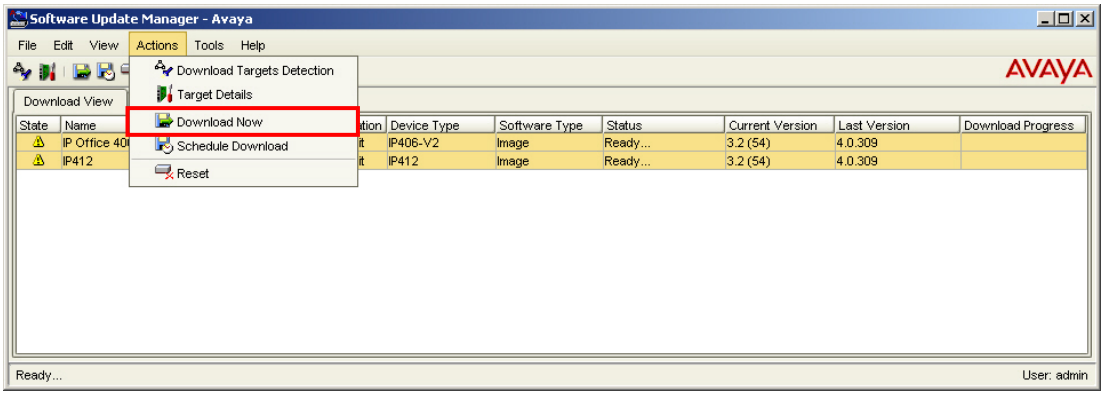
10. Repeat Step 8 for the Avaya IP Office 412 discovered during the Download Targets Detection in Step 3. The Target Details window will open to provide configuration parameters for upgrading the Avaya IP Office 412 hosted at the Branch 2 location in **Figure 1**.

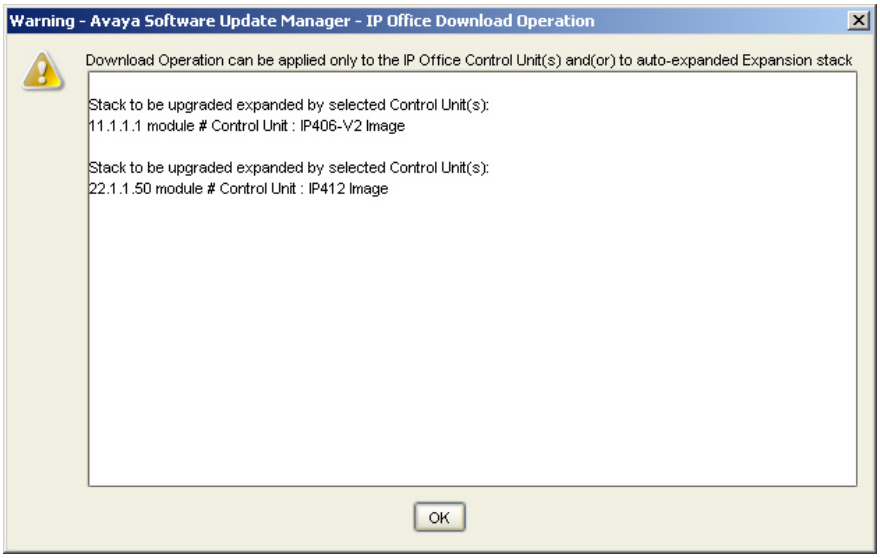


11. Repeat Step 9 for the Avaya IP Office 412 to perform an upgrade using the software binaries downloaded in Step 6. Leave the remaining parameters at the default setting and click the **OK** button when finished.



12. Highlight both the Avaya IP Office 406v2 and the Avaya IP Office 412 after configuring the target details for each system. Select the **Actions** option from the top menu and scroll to the **Download Now** selection. This will initiate the upgrade procedure with the software binaries selected for the corresponding Avaya IP Office systems in Steps 9 and 11. At the Warning window, click the **OK** button to confirm upgrade procedure for the designated Avaya IP Office systems.





5. Verification

These Application Notes verified the functionality for centralized management with CSM applications using the procedures listed in the subsequent sections below. Each section describes the verification steps used to determine system status of the application as well as the operational status of the managed devices. Perform the following steps after the upgrade procedure of the Avaya IP Office systems:

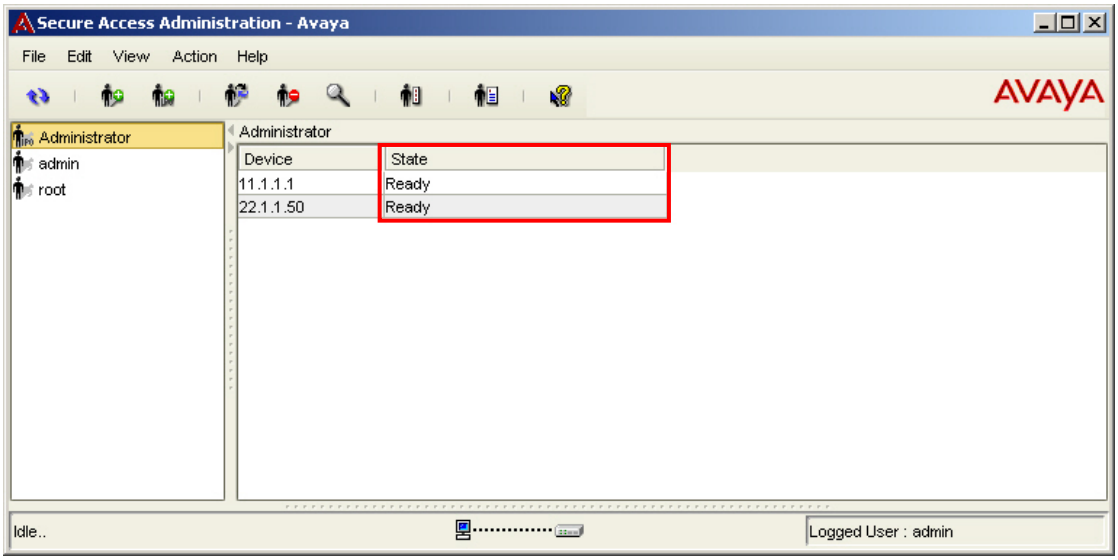
1. Verify the Avaya IP Office systems at each Branch location have operational status after the upgrade and re-established network connectivity with the Main location

2. Place a call between the Avaya 5610SW IP Telephone and the Avaya 5420 Digital Telephone at the Branch 1 location. Verify two-way audio and voice quality is acceptable. Repeat this step for the Branch 2 location.

3. Place a call between telephones at the Branch 1 and Branch 2 locations. Verify two-way audio and voice quality is acceptable between the two locations.

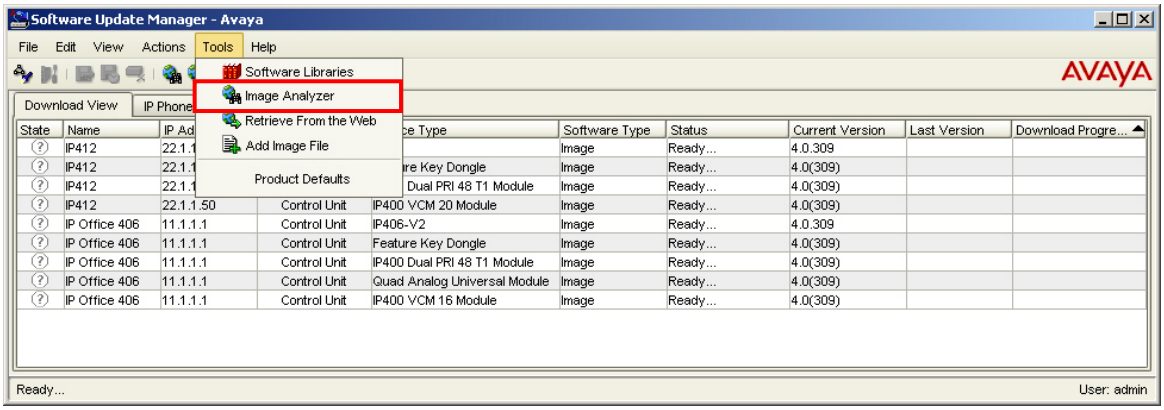
5.1. Avaya Secure Access Administration Verification

1. At the SAA application, click the user created in Section 4.2 to display the security assignment for accessing managed devices. Verify the user has a **Ready** status for the Avaya IP Office 406v2 and Avaya IP Office 412 at the corresponding Branch locations in **Figure 1**.

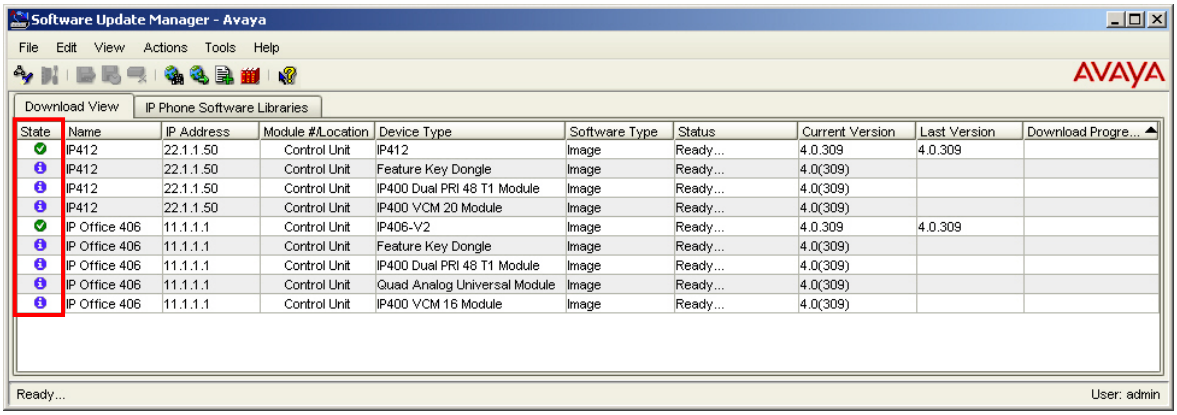


5.2. Avaya Software Update Manager Verification

1. After the upgrade operation performed in Step 12 is completed, select the **Tools** option from the top menu and scroll to the **Image Analyzer** selection. The Image Analyzer will compare the upgraded software version for the Avaya IP Office systems with the latest software version available at the Avaya Support web site.



2. After the Image Analyzer operation is completed, verify the ✔ status icon under the **State** column identifies the upgraded software version for both Avaya IP Office systems as identical to the software version available on the Avaya Support web site. Also, verify the ℹ status icon under the **State** column identifies the supplemental hardware features discovered for the latest software version. The ℹ status icon appears after an upgrade to 4.x software for Avaya IP Office and provides additional information that is not present in 3.x software.



3. Log into the local server hosting Avaya Integrated Management Network Management suite using the proper login credentials, and open the **Backup/Logs** folder in the installation directory for CSM. Examine the latest **UpdateManagerLog.csv** file displayed in the directory folder and view the status of the software upgrade performed in Step 12 for the Avaya IP Office systems. Verify the upgrade status for the Avaya IP Office 406v2 that is demonstrated in the highlighted ASCII text below.

```
Normal  ,11:03 Wednesday 21 Feb 2007,11.1.1.1,Upgrade completed
Normal  ,11:03 Wednesday 21 Feb 2007,11.1.1.1 (Control Unit),Discovered IP Office IP400
VCM 16 Module Image Version 4.0(309)
Normal  ,11:03 Wednesday 21 Feb 2007,11.1.1.1 (Control Unit),Discovered IP Office Quad
Analog Universal Module Image Version 4.0(309)
Normal  ,11:03 Wednesday 21 Feb 2007,11.1.1.1 (Control Unit),Discovered IP Office IP400
Dual PRI 48 T1 Module Image Version 4.0(309)
Normal  ,11:03 Wednesday 21 Feb 2007,11.1.1.1 (Control Unit),Discovered IP Office
Feature Key Dongle Image Version 4.0(309)
Normal  ,11:03 Wednesday 21 Feb 2007,11.1.1.1 (Control Unit),Discovered IP Office IP406-
V2 Image Version 4.0(309)
Normal  ,11:03 Wednesday 21 Feb 2007,11.1.1.1 Control Unit,[IP 11.1.1.1, ModuleID
Control Unit, Classification IP Office,IP406-V2,Image, VersionInfo (4.0.309,image
version), ApplicationName UpdateMaster],(4.0.309,image version),[{Running
Version,4.0.309}, {icon,0}]
```

4. Repeat the previous step for the Avaya IP Office 412 to view the status of the software upgrade. Verify the upgrade status for the Avaya IP Office 412 that is demonstrated in the highlighted ASCII text below.

```
Normal  ,11:02 Wednesday 21 Feb 2007,22.1.1.50,Upgrade completed
Normal  ,11:02 Wednesday 21 Feb 2007,22.1.1.50 (Control Unit),Discovered IP Office IP400
VCM 20 Module Image Version 4.0(309)
Normal  ,11:02 Wednesday 21 Feb 2007,22.1.1.50 (Control Unit),Discovered IP Office IP400
Dual PRI 48 T1 Module Image Version 4.0(309)
Normal  ,11:02 Wednesday 21 Feb 2007,22.1.1.50 (Control Unit),Discovered IP Office
Feature Key Dongle Image Version 4.0(309)
Normal  ,11:02 Wednesday 21 Feb 2007,22.1.1.50 (Control Unit),Discovered IP Office IP412
Image Version 4.0(309)
Normal  ,11:02 Wednesday 21 Feb 2007,22.1.1.50 Control Unit,[IP 22.1.1.50, ModuleID
Control Unit, Classification IP Office,IP412,Image, VersionInfo (4.0.309,image version),
ApplicationName UpdateMaster],(4.0.309,image version),[{Running Version,4.0.309},
{icon,0}]
```

6. Conclusion

These Application Notes illustrate the procedures required for configuring the Avaya Integrated Management Network Management suite to centrally manage software upgrades for Avaya IP Office 406v2 and Avaya IP Office 412 in a distributed network environment. System options were successfully provisioned in Avaya IP Office for network discovery, and the Avaya Network Management Console established SNMP connectivity with managed devices during the discovery. Avaya Secure Access Administration was successfully configured to enforce security assignment of authorized users administering Avaya IP Office systems. Avaya Software Update Manager successfully upgraded software from 3.2 to 4.0 for both the Avaya IP Office 406v2 and the Avaya IP Office 412 depicted at the Branch locations in **Figure 1**. These Application Notes provide administrators the necessary steps for implementing the Avaya Integrated Management Network Management suite in a multi-location network environment to support the Avaya Chain Store Management solution.

7. References

The following references below can be found at http://support.avaya.com:

- Avaya Integrated Management 3.3 Network Management Console User Guide, Issue 1, February 2007.
- Avaya Integrated Management 3.3 Secure Access Administration, Issue 1.0, February 2007.
- Avaya Integrated Management 3.3 Software Update Manager User Guide, Issue 1, February 2007.
- Avaya IP Office 4.0 Installation Manual, Issue 15e, January 2007.
- Avaya IP Office 3.2 Manager, Issue 18g, June 2006.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com