Avaya one-X® Mobile Integration, Administration, and Maintenance Guide

Release 5.2
January 2010
0.5

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 support information, please see the complete document, *Avaya Support Notices for Software Documentation*, document number 03-600758.

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

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Copyright

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

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

Chapter 1: Introduction 7
Audience 7
What You Need to Know. 7
Conventions 7
Acronyms 8
Avaya one-X Mobile Documentation 8
Other Product Documentation 9

Chapter 2: Overview 11
Avaya one-X Mobile Overview 11
What's New in this Release 11
Supported Equipment 12
Before You Begin 13
Required Tasks for New Installations 14

Chapter 3: Integration with Avaya equipment 17
Integration task flow 17
Configure integration with Communication Manager 18
Validate licensed features 18
Configuring Communication Manager for SIP 18
Add a node 19
Add a signaling group 19
Add a trunk group 19
Configure Off-PBX EC500 settings 20
Integration with Modular Messaging 21
Voicemail profile with MSS integration. 21
Configure Modular Messaging with Exchange 22
Integration with Modular Messaging using MS Exchange 2000 or 2003 22
Create a domain user using MS Exchange 2000 or 2003 22
Validate Exchange administrative user permissions 23
Add the domain user as an administrative user 24
Integration with Modular Messaging using MS Exchange 2007 24
Create a new domain user. 24
Validate Exchange administrative user permissions 24
Add the domain user as an administrative user 25
Assign full access rights to mailboxes. 25
Configure the EdgeMapiMgr service 26
Stop the Universal Search Command Line (USCL) service host 27
Start the Universal Command Line (USCL) service host and redeploy application. 28

Chapter 4: Avaya one-X Mobile Administrative Interface 31
Obtain the Avaya one-X Mobile License 31
Avaya one-X Mobile Administration 32
Configure the Avaya one-X Mobile Server 33
Configure the Server Settings 34
Configure Split Server Settings 34

Chapter 5: Avaya Setup 37
Create a Provisioning Profile 37
Create a Communication Manager Profile 40
Create a Voicemail Profile 43
Voicemail profile with Exchange Integration 44
Voicemail profile with MSS integration 45
Create a Corporate Directory Profile 46
Create a Class of Service 48
Administer Users 52
Import Users 53
Manage Unlicensed Users 53
License Selected Users 54
Manage Licensed Users 54
Change Class of Service 55
Reprovision Selected Users 55
Unlicense Selected Users 55
Delete Selected Users 56
View User Details 56
Lost or Stolen Mobile Phone 56
No Longer an Employee 56
Unlock one-X Mobile Account 57
Configure Dial Plans and Conversion Rules 57
Add Non-LDAP Extension/Numbers to E.164 number Rules 59
Add New Conversion Dial Plan 60
Add a New Dial Plan 61
User entered number to PBX dialable number for Callbacks Dial Plan 61
User entered number to mobile (EC500) format Dial Plans 61

Chapter 6: Serviceability 65
View Control Center 65
View Trace Components 65
View Component Info 65

Chapter 7: Licenses 67
View License Information 67
Chapter 8: Direct Call PBX Numbers 69
Appendix A: Log Cleaning Utility 71
Schedule the Tomcat Log Cleaning Utility 71
Appendix B: Dial Plan Configuration Scenarios 73
Extension Conversion 73
Scenario: Administrator provisions a user 73
Requirements and assumptions 74
Final destination number computation (callback) 74
Examples for Final destination number conversions (callback) 77
Global configurations 77
Mobile numbers and quick entries conversions for callback 85
Examples for mobile numbers and quick entries conversions 87
Examples for user entered to mobile dial plan rules conversions 88
Mobile numbers and quick entries conversions on incoming call 89
Example for applying the Tango (Incoming Call Routing) prefix 91
GSM Prefixes (Tango Prefix for incoming calls and LCR Prefix for callback) . . 91
Caller ID related transformations 92
Appendix C: Acceptance Testing 93
Appendix D: Enhanced scalability by Tomcat tuning 95
. . . . . .
Reduce the logging 95
. . . . . .
Optimize Java 95
Optimize the Tomcat server 96

Chapter 1: Introduction

The *Avaya one-X® Mobile Integration, Administration, and Maintenance Guide* provides the procedures required to integrate the Avaya one-X Mobile Server with existing equipment in a corporate IP voice network as well as provision the Avaya one-X Mobile Server itself.

Audience

This guide is written for network and IT administrators who are responsible for administering, configuring, and maintaining the Avaya one-X Mobile Server. Administrator permissions are required to accomplish the tasks in this guide.

What You Need to Know

To successfully integrate the Avaya one-X Mobile server into your network, you need to know:

- the details of your IP network
- how to configure Avaya Aura® Communication Manager 5.2.1
- how to configure the Avaya Modular Messaging, Messaging applications, and messaging platform.
- how to configure the enterprise directory infrastructure

Conventions

The following conventions are found in this guide:

Convention	Description
Bold font	Keywords and names of text fields
Italic font	Values that the administrator must enter into text fields

Convention	Description
`Courier` Font	Text that must be entered into a terminal session
Menu Font	Menu Items

Note:
The last page at the end of all the chapters is intentionally left blank as per our documentation template.

Acronyms

The following acronyms might be found in this guide:

Acronym	Meaning
CM	Communication Manager
COS	Class of Service
EC500	Extension to Cellular
IMAP	Internet Message Access Protocol
LDAP	Lightweight Directory Access Protocol
MAPI	Messaging Application Programming Interface
MSS	Message Storage Server
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer

Avaya one-X Mobile Documentation

Avaya documents are available on the Avaya support Web site at http://www.avaya.com/support.The documents listed below are part of the Avaya one-X Mobile documentation set.

- Avaya one-X Mobile Site Survey/Pre-Installation Checklist (for Communication Manager 5.2.1 Environment)

- Avaya one-X Mobile Installation Guide
- Avaya one-X Mobile Installation and Upgrade Checklists
- Avaya one-X Mobile Integration, Administration, and Maintenance Guide
- Avaya one-X Mobile User Guide for J2ME
- Avaya one-X Mobile User Guide for RIM Blackberry
- Avaya one-X Mobile User Guide for Palm Treo
- Avaya one-X Mobile User Guide for iPhone
- Avaya one-X Mobile User Guide for Windows Mobile
- Avaya one-X Mobile Web User Guide

Other Product Documentation

The documents listed below may help in completing the tasks in this book:

Communication Manager 5.2.1 documentation

You should also refer to the manuals for other vendor’s equipment that may be installed in your network.

Chapter 2: Overview

This chapter provides a brief description of Avaya one-X Mobile, highlights new features, lists supported equipment, and describes tasks that must be completed before you begin using this guide. A list of all integration and configuration tasks is also provided that must be completed for a new installation of Avaya one-X Mobile.

Avaya one-X Mobile Overview

Avaya one-X Mobile is software and hardware that offers enterprise voice, messaging, voicemail, and corporate directory integration on mobile devices (cell phones and PDAs). Avaya one-X Mobile allows the corporate voice network to be seamlessly extended to employees' mobile phones. The one-X Mobile features include:

- Managing call routing of corporate PBX extensions directly to other locations, such as a mobile phone
- Routing incoming calls based on the identity of an individual caller by using special routing rules (for example, allow a manager to reach an employee's mobile phone, while all other calls are redirected to the voicemail)
- Accessing and receiving corporate voicemail
- Viewing and managing personal phone book and corporate directory
- Accessing the one-X Mobile features by using the one-X Mobile Web interface or application on the mobile handsets.

What's New in this Release

Avaya one-X Mobile Release 5.2 introduces the following new features:

- Improved reliability with two party callback
- Support for the following systems:
  - Communication Manager 5.2.1 only (no support for prior versions)
  - Modular Messaging 5.0 and later
- Support for iPhone Native, Windows Mobile, J2ME, Palm, and Blackberry mobile clients

- Support for Avaya Common Server
- Enhanced support for Microsoft Office Communicator (MOC) 2007 and Office Communications Server (OCS)
- Support for Secure Access Link (SAL): SAL provides complete control over all remote access to your networks and also provides channel-neutral support in addition to control, auditable logging, and strong identification and authentication of any users who access their networks. SAL also provides clear, auditable logging of any access attempt, either by a technician or an automated tool

Note:
one-X Mobile works with the SIP phones that are connected to SIP Enablement Service (SES).

Important:
one-X Mobile R 5.2 does not require an integration with Avaya AES (as was necessary in one-X Mobile 1.X). In one-X Mobile R 5.2, a SIP trunk is established between Communication Manager 5.2.1 and the one-X Mobile internal server. The SIP trunk replaces the AES JTAPI interface.

Supported Equipment

The following table lists the supported equipment that might be in your network.

Function	Avaya Equipment	Other Vendor's Equipment
Call Management	Communication Manager	
Voicemail	Modular Messaging	MS Exchange Server
IP Phones	Supported Avaya IP Phones (Avaya 9600, 1600, and 4600 series IP phones are supported.) For more information, see the release notes available at http://www.avaya.com/support.	

Function	Avaya Equipment	Other Vendor's Equipment
Phones	Supported Avaya H.323 and SIP phones. The 8400 series phones are not supported. DCP with 6400 series phones is supported.	
Corporate Directory		Microsoft Active Directory (2003, 2007 and 2008) SunOne Netscape_iPlanet
MS Exchange		MS Exchange 2000, 2003, and 2007
LDAP Server		LDAP v3 directories

Before You Begin

Before you begin performing the integration and administration tasks provided in this guide:

1. The following equipment and software must be installed on your network:
   - Communication Manager (version 5.2.1 or later)

   You should also have all the relevant documentation for this equipment on hand for reference.
2. Installation of the following equipment and software is optional:
   - Modular Messaging version (5.0 or later)
   - one-X Speech software
     For more information, see the Avaya one-X Speech Release 5.0 Installation Guide.
3. Review the worksheets in the *Avaya one-X Mobile Site Survey/Pre-Installation Checklist* and complete as much information as possible:

Note:
You will complete some information on the worksheets as you perform the tasks in this guide.

4. Complete the installation of the Avaya one-X Mobile Server software. For more information, see the *Avaya one-X Mobile Installation Guide*.

Required Tasks for New Installations

Perform the following integration and configuration tasks for the new installations of Avaya one-X Mobile. For tasks listed that do not have a corresponding procedure in this guide, refer to the administration and maintenance documents for Communication Manager 5.2.1, and Modular Messaging.

Task	Procedure
Communication Manager	
Configure Communication Manager for SIP	
Modular Messaging	
If using Modular Messaging with Message Storage Server (MSS):	
Add one-X Mobile server as a trusted server on the MSS	See Integration with Modular Messaging on page 21.
Verify that LDAP/SMTP/IMAPI4 ports are enabled (in MSS).	See Voicemail profile with MSS integration on page 21.
Set Restrict Client Access to NO in Class of Service for Avaya one-X Mobile users (in MSS).	
If using Modular Messaging with Microsoft Exchange:	
Perform the following integration steps depending on the version of MS Exchange that you are using.	
Set transfer or outcall to Full for the voicemail domain on the MAS	
Perform the integration with Modular Messaging using MS Exchange 2000 or 2003	See Integration with Modular Messaging using MS Exchange 2000 or 2003 on page 22.
	1 of 2

Task	Procedure
Perform the integration with Modular Messaging using MS Exchange 2007	See Integration with Modular Messaging using MS Exchange 2007 on page 24
Avaya one-X Mobile	
Log into the Avaya one-X Mobile server using the administrator login.	
Create SMTP login and password for voicemail notification.	See Configure the Server Settings on page 34.
Check that the Log Cleaning Utility has been configured. For more information, see Log Cleaning Utility on page 71.	
Install one-X Mobile licenses.	See Obtain the Avaya one-X Mobile License on page 31.
Create Dial Plans and Conversion Rules as required by your configuration.	See Add a New Dial Plan on page 61.
Create a Communication Manager Profile	See Create a Communication Manager Profile on page 40
Create a Provisioning Profile.	See Create a Provisioning Profile on page 37.
Create a Voicemail Profile.	See Create a Voicemail Profile on page 43.
Create a Corporate Directory Profile.	See Create a Corporate Directory Profile on page 46.
Create a Class of Service Profile.	See Create a Class of Service on page 48.
Configure Direct Call PBX Numbers	See Direct Call PBX Numbers on page 69
Import users.	See Import Users on page 53.
License users.	See License Selected Users on page 54.
	2 of 2

Chapter 3: Integration with Avaya equipment

This chapter provides procedures to integrate Communication Manager and Modular Messaging with the Avaya one-X Mobile Server. This chapter provides instructions to show basic functionality on new installs; these are instructions for a production system.

Note:
Ensure that you back up the one-X Mobile server data by using the standard Microsoft Windows server backup procedures before making any updates to the one-X Mobile server. To open the **Backup or Restore** wizard, click **Start> Programs> Accessories > System Tools > Backup**.

For more information about the one-X Mobile server security settings and the required ports, see the one-X Mobile 5.2 Security White Paper on the Avaya support Web site at http://www.avaya.com/support.

Integration task flow

To integrate Avaya one-X Mobile in a network containing Avaya equipment, perform these tasks in the following order:

1. Configure integration with Communication Manager on page 18.
   a. Validate the Licensed Features
   b. Configure SIP trunk on Communication Manager

   Note:
   To configure SIP trunk on Communication Manager, see SIP Support in Avaya Communication Manager Running on Avaya S8xxx Servers.
2. Integration with Modular Messaging on page 21.
   a. Configure Modular Messaging 5.0 with MSS
   b. Configure Modular Messaging 5.0 with Exchange

Configure integration with Communication Manager

Avaya one-X Mobile uses Communication Manager to:

- Route inbound calls to match the call handling settings selected by the user in Avaya one-X Mobile.
- Place calls on behalf of a user who is away from the office.
- Monitor inbound and outbound call activity by the user so it can be displayed in the one-X Mobile client call log.

You must configure certain Communication Manager features and capabilities in order to properly integrate with the Avaya one-X Mobile server. You can perform these configurations by using System Access Terminal (SAT) commands entered through a SAT session or the Avaya Site Administration (ASA) utility.

Validate licensed features

It is important to validate the licensed features on Communication Manager before attempting to configure.

To validate licensed features:

At the System Administration Terminal, enter the **`display system-parameters customer-options`** command.

You can verify whether you have the required Communication Manager licenses by using this command.

Validate that the following licensed features and capacities exist:

- Maximum Administered SIP Trunks
- Platform Maximum Ports
- Enhanced EC500 = y
- Maximum Off-PBX Telephones - EC500
- Maximum Off-PBX Telephones - PBFMC

Contact your Avaya Partner if you do not have the proper features licensed.

Configuring Communication Manager for SIP

The Session Initiation Protocol (SIP) is used to initiate a session between one-X Mobile and Communication Manager.

Log into the Communication Manager through Avaya Site Administration (ASA) tool and configure the following:

Add a node

To add the server as a node in the Communication Manager:

1. In Communication Manager, use the **`change node-names ip`** command to add a new node.
2. In the **Name** field, enter a name for the one-X Mobile node. For example, onexmhq.
3. In the **IP Address** field, enter the IP address of the one-X Mobile server.

Note:
In a Split Server configuration this should be the IP of the internal server.

Add a signaling group

To add a signalling group:

1. In Avaya Site Administration, use the **`add signaling-group next`** command to add a signalling group or PROCR to a CLAN.

Note:
You must not use "next" or "n" in the Communication Manager "Add" commands at a customer site. You must use the specific object number provided by the customer, a value which is consistent with the customer's organization of lines, stations, and trunks.

2. In the **Group Type** field, enter SIP.
3. In the **Transport** field, enter TCP.
4. In the **Near-end Node Name** field, enter the node name of the Communication Manager CLAN.
5. In **Far-end Node Name** field, enter name of the node that you had created using the **Add a node** procedure.
6. In the **Far-end Domain Name** field, enter a name for the far-end domain.
This field is optional.

Note:
If you use "next" or "n" in the command, the system generates and displays a signaling group number in the top left corner in Avaya Site Administration. Note down this signaling group number for further configuration.

Add a trunk group

To add a new trunk group:

1. In Avaya Site Administration, use the **`add trunk-group next`** command to add a new trunk group.
2. In the **Group Type** field, enter *SIP*.
3. In the **Group Name** field, enter a name for the group.
4. In the **TAC** field, enter a valid and unused Trunk Access Code (TAC) that is not assigned to any other trunk group and the the **TAC** must be of **Call Type** "DAC".

   Note:
   In the Communication Manager, to determine a valid and unused Trunk Access Code (TAC), run the **`Display dialplan analysis`** command and in the result of this command, ensure that the **Call Type** is "DAC".
5. In the **Service Type** field, enter *tie*.
6. In the **Signaling Group** field, enter the group number that was generated using the **Add a signaling group** procedure.
7. In the **Number of members** field, enter a number so that there is one member per 10 one-X Mobile subscribers.

Configure Off-PBX EC500 settings

For all the one-X Mobile users, ensure that the EC500 application is not administered in the off-pbx-telephone-station-mapping form, as this feature is redundant and can be incompatible with the one-X application that one-X Mobile leverages. Remove the EC500 entry if the user already has an EC500 application assignment.

Note:
If you remove the user's EC500 entry in the off-pbx-telephone-station-mapping form of Communication Manager, then the EC500 activate or deactivate button is disabled on the user's desk phone, but the system displays the button on the phone display. You should remove that button from the station administration for these users.

Note:
Disable Mobility on the user’s one-X Portal system or group profile configuration for those one-X Mobile users who choose to enable one-X Portal. Disabling Mobility prevents the user from setting the **Also ring** phone number functionality in one-X Portal. In one-X Portal, **Also ring** functionality is equivalent to EC500.

Integration with Modular Messaging

Modular Messaging is the voicemail platform used by Communication Manager and Avaya one-X Mobile to manage a user's voicemail.

Voicemail profile with MSS integration

To configure Modular Messaging with Message Storage Server (MSS), you must configure the trusted server in the Modular Messaging Administration.

Perform the following steps to configure the trusted server:

1. Log onto the MSS administration Web page.
2. Click **Trusted Server**.
3. Click **Add a New Trusted Server**.
4. In the **Trusted Server Name** field, enter a user name for the account that one-X Mobile will use to manage voicemail on the MSS.
5. In the **Password** and **Confirm Password** fields, enter a password for the account that one-X Mobile will use to manage voicemail on the MSS.

   Note:
   This user name and password is needed in the Avaya one-X Mobile Server configuration. Add them to the *Avaya one-X Mobile Site Survey/Pre-Installation Checklist* (section 2.1) for future reference.
6. In the **Machine Name/IP Address** field, enter the IP address of the Avaya one-X Mobile server.
7. In the **Service Name** field, enter *edge*.
8. In the **LDAP Access Allowed** drop-down list, select **yes**.
9. In the **LDAP Connection Security** drop-down list, select **No encryption required**.
10. In the **IMAP4 Super User Access Allowed** drop-down list, select **yes**.
11. In the **IMAP4 Super User Connection Security** drop-down list, select **Must use SSL or encrypted SASL**.
12. Click **Save**.

Configure Modular Messaging with Exchange

Integration with Modular Messaging using MS Exchange 2000 or 2003

When you create a voicemail profile in the Avaya one-X Mobile administrative interface, you must complete the Exchange Administrative User section. The Exchange Administrative User section includes the configuration of the location and authentication credentials of the exchange server. Authentication credentials of the Exchange administrative user must be entered so that the Avaya one-X Mobile Server can access voicemail for any user.

To create a user with the permissions required to be the Exchange Administrative User, see Create a domain user using MS Exchange 2000 or 2003 on page 22. Ideally, this user should be a member of the Domain Administrators group. Additionally, the user must have permissions to Log on as a Service locally on the Avaya one-X Mobile Server.

Create a domain user using MS Exchange 2000 or 2003

Access to Exchange is required by the Avaya one-X Mobile Server to provide the Avaya one-X Mobile Visual Voicemail functionality. The Domain User is used by Avaya one-X Mobile Server to access voice messages from user mail boxes for this purpose.

To create a domain user:

1. In the **Active Directory Users and Computer**, create a domain user account in the domain where the Microsoft Exchange server resides. The user created here is used as the EdgeMapiMgr service account on the one-X Mobile server.

   Note:
   If multiple Exchange Servers are being used, perform the following tasks on each Exchange Server used by the Avaya one-X Mobile Application Suite.

2. In the **Exchange System Manager**, assign the permissions to Domain User:
   a. Navigate down to the **Mailbox Store** of the Exchange Server.
   b. Right-click on it and select **Properties**.
   c. Select the **Security** tab.
   d. Click **Add** to add the Domain User.
   e. Assign the following permissions to it:
      - Read
      - Execute
      - Delete
      - Read permission
      - Change permission

- List contents
- Read properties
- Write properties
- List object
- Open mail send queue
- Receive As
- Send As

Once these permissions have been applied to the Domain User, stop and restart the Microsoft Exchange System Attendant Service, Microsoft Exchange MTA Stacks service, and Microsoft Exchange Information Store service. Alternatively, wait for the update period to pass (usually around 24 hours). The permissions assigned to the domain user are read into the Microsoft Exchange Applications.

Validate Exchange administrative user permissions

Validate that the designated Exchange Administrative User has sufficient permissions to manage the end user mailbox. Perform this procedure to validate the Exchange Administrative User permissions for the Avaya MM system.

Perform the following steps:

1. Go to the Domain Controller for the specified domain whose member is the Administrative user.
2. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
   The system displays the Management Console.
3. Click **View > Advanced Features**.
4. Expand the tree control for the specified domain of the Administrative user.
5. Click **Users**.
6. Locate the user in the right-hand pane.
7. Right-click on the designated user and click **Properties**.
8. Locate the group to which the user belongs.
9. In the **Permissions** frame, select all the listed permissions as **allow** except for **Full Control**. Do not select any option (**allow** nor **deny**) for **Full Control**.
10. Click **Apply** if changes were required.
11. Click **OK** to exit the property page.
12. Exit out of the Management Console.

Add the domain user as an administrative user

The domain user must be associated with the Edge MAPI Manager service that runs as part of the one-X Mobile application. It is also recommended that the service be set up to start automatically upon system reboot.

To add the user as an administrative user:

1. Go to **Start > Control Panel > Administrative Tools > Services**.
2. Locate the EdgeMapiMgr service.
3. Right-click the service and select **Permissions**.
4. Select the **Log On** tab.
5. Select **This Account**.
6. Specify the domain user you defined in the **Create a Domain User** section.
7. Enter and confirm the domain password for the user.
8. Click the **General** tab.
9. Set **Startup type** to Automatic.
10. Click **OK**.

Integration with Modular Messaging using MS Exchange 2007

Create a new domain user

The user created here is used as the EdgeMapiMgr service account on the one-X Mobile server.

1. Log into the LDAP server using an account that has all administrative rights.
2. Create a new domain user account in the same domain as the Microsoft Exchange Server 2007.

Validate Exchange administrative user permissions

Validate that the designated Exchange Administrative User has sufficient permissions to manage the end user mailbox. Perform this procedure to validate the Exchange Administrative User permissions for the Avaya MM system.

Perform the following steps:

1. Go to the Domain Controller for the specified domain whose member is the Administrative user.
2. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
   The system displays the Management Console.

3. Click **View > Advanced Features**.
4. Expand the tree control for the specified domain of the Administrative user.
5. Click **Users**.
6. Locate the user in the right-hand pane.
7. Right-click on the designated user and click **Properties**.
8. Locate the group to which the user belongs.
9. In the **Permissions** frame, select all the listed permissions as **allow** except for **Full Control**. Do not select any option (**allow** nor **deny**) for **Full Control**.
10. Click **Apply** if changes were required.
11. Click **OK** to exit the property page.
12. Exit out of the Management Console.

Add the domain user as an administrative user

The domain user must be associated with the Edge MAPI Manager service that runs as part of the one-X Mobile application. It is also recommended that the service be set up to start automatically upon system reboot.

To add the user as an administrative user:

1. Go to **Start > Control Panel > Administrative Tools > Services**.
2. Locate the EdgeMapiMgr service.
3. Right-click the service and select **Permissions**.
4. Select the **Log On** tab.
5. Select **This Account**.
6. Specify the domain user you defined in the **Create a Domain User** section.
7. Enter and confirm the domain password for the user.
8. Click the **General** tab.
9. Set **Startup type** to Automatic.
10. Click **OK**.

Assign full access rights to mailboxes

The domain user account created is given full access to the mailboxes on MS Exchange Server 2007 that are to be managed by one-X Mobile. This domain user account is not required to have an Exchange Mailbox associated with it.

1. Click **Start > All Programs > Microsoft Exchange Server**.
2. Click **Exchange Management Shell**.

3. Log into the MS Exchange Server 2007 by using an account that has all administrative rights.
4. Ensure that Exchange 2007 Server SP1 is installed.
5. Ensure that SP1 rollup update 7 or later is installed.
6. Ensure that IMAP4 is enabled and its service is running. If it is not running, enable IMAP4 and start the service by performing the following commands on the MS Exchange Management Shell:

   ```
   Set-Service msExchangeImap4 -StartupType Automatic
   ```

   ```
   Start-Service -Service msExchangeImap4
   ```

7. To set plain-text logon for the IMAP4 server, run the following command in the Exchange Management Shell:

   ```
   Set-IMAPSettings -LoginType PlainTextLogin
   ```

   ```
   Restart-Service -Service msExchangeImap4
   ```

8. To grant full access rights for all mail boxes on the MS Exchange Server 2007 server, run the following commands in the Exchange Management Shell.

   ```
   Get-mailbox –Server <Exchange Server 2007 Name> |
   Add-MailboxPermission –User <Domain User Account> -AccessRights
   FullAccess
   ```

   Note:
   Full Access is required to listen to, save, and delete voicemails using one-X Mobile clients. For configuring permissions, refer to the following link for more details: http://technet.microsoft.com/en-us/library/aa997244.aspx.

9. Ensure that Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 are installed on the Exchange Server 2007. You can download the software from the Microsoft download center: http://www.microsoft.com/downloads/details.aspx?FamilyID=E17E7F31-079A-43A9-BFF2-0A110307611E&displaylang=en

Configure the EdgeMapiMgr service

Use the domain user that you created in section Create a new domain user on page 24 to log onto the EdgeMapiMgr service.

1. Log into the one-X Mobile internal server as an administrator.
2. Upgrade to the General Availability (GA) version of one-X Mobile server, if necessary.

3. Ensure that Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 is installed on the one-X Mobile server. You can download the software from the Microsoft download center:
   http://www.microsoft.com/downloads/details.aspx?FamilyID=E17E7F31-079A-43A9-BFF2-0A110307611E&displaylang=en
4. Click **Start > Run**.
5. In the Run text box, enter **`secpol.msc`** and click **OK**.
6. In the **Local Security Settings** window, click **Local Policies -> User Rights Assignments** and find the **Log on as a service** policy in the right pane.
7. Open the properties page for this policy and verify that the domain user created in section Create a domain user using MS Exchange 2000 or 2003 on page 22 is listed under the Local Security Setting tab. If it is not listed, add the account and save the changes.
8. Open the one-X Mobile Administrative interface and create a new Voicemail Profile with Profile Type, **Modular Messaging with Exchange Integration**, and specify the domain user.
9. Right-click on **My Computer** and select **Manage**.
10. In the **Computer Management** window, select **Services and Applications > Services**.
11. In right pane, right-click on **EdgeMapiMgr** and select **Properties**.
    The system displays the properties page for the EdgeMapiMgr service.
12. Set the service startup type to **Automatic**.
13. In the **LogOn** tab, enter the domain user details created in section Create a domain user using MS Exchange 2000 or 2003 on page 22 and password.
14. Select **This account** and click **OK**.
15. Right-click on **EdgeMapiMgr** and select **Restart**.
16. Verify that the **Edge NotificationServer** service is started and the startup type is set to **Automatic**.

Stop the Universal Search Command Line (USCL) service host

You might need to stop the Universal Search Command Line (USCL) service host in some instances such as when you need to clear the sipcchandler logs, or when you need to update Microsoft SQL Server Desktop Engine (MSDE) to SQL 2000 Server SP4 and when you need to apply any updates.

1. Go to **Start > Programs > Ubiquity > Ubiquity Element Manager > Ubiquity Element Manager**.
2. In the management tree, select the **Service Host Collection** node for the appropriate cluster.

3. Click the **Applications** tab.
4. In the Deployed Applications list, select the application you want to undeploy.
5. Click **Undeploy**.
   A message is displayed stating that the application may be in use by current sessions.
6. Select the **Delete application configuration** check box, if you want to delete the application configuration.
7. Click **Yes**.
   Ensure that the required application is removed from the Deployed Applications list
8. Click **Apply** and **OK**.
9. Select **Channel 1** under the **Service Host Collection** node.
10. Right-click and select **Destroy Channel**.
    When the channel is destroyed, then you can find the **Service Host** under the **Pooled Service Hosts** node.
11. Right-click on the **Service Host**, and select **Stop**.

Note:
You cannot restart the Service Host through the Ubiquity Element Manager (UEM), you can restart the Service Host through the Windows Services.

Start the Universal Command Line (USCL) service host and redeploy application

To redeploy an application:

1. Click **Start > Run**.
2. In the **Run** text box, enter **`services.msc`** and click **OK**.
3. In the **Services** window, click **USCL ServiceHost**.
4. Click **Start the service**.
5. On the Ubiquity Element Manager (UEM), to create the channel, right-click on the **Service Host Collection** node, and select **Create Channel**.
6. Go to **Start > Programs > Ubiquity > Ubiquity Element Manager > Ubiquity Element Manager**.
7. In the management tree, select the **Service Host Collection** node for the appropriate cluster.
8. Click the **Applications** tab.
9. Click **Configure**.
10. Select the application in the **Application Repository** list and move the application to the **Deployed Applications** list.

11. Click **Apply**.
    - If the system displays a configuration window, enter the requested details, proceeding through the configuration windows until the configuration is complete and click **Apply**. The system displays a message stating that the configuration has been successfully applied to the cluster. Click **OK** and go to the next step.
    - If the system does not display a configuration window, go to the next step.

    Ensure that the required application is listed under Deployed Applications list
12. Click **Apply** and **OK**.

Chapter 4: Avaya one-X Mobile Administrative Interface

This chapter provides information to get started using the Avaya one-X Mobile administrative interface. It provides information about the Avaya one-X Mobile license and configuring the Avaya one-X Mobile server.

Obtain the Avaya one-X Mobile License

To access the Avaya one-X Mobile Server administrative user interface, first install the Avaya one-X Mobile Server. For instructions on how to install the software, see the *Avaya one-X Mobile Installation Guide*.

Before you begin working with the Avaya one-X Mobile administrative interface, you must install the Avaya one-X Mobile license.

Follow these steps to obtain and install the Avaya one-X Mobile license:

1. To obtain the correct MAC address, go to a command line and type **`ipconfig /all`**. (If the information scrolls off the screen, type **`ipconfig /all | more`**.)
2. Find the network adapter for which you want to know the MAC address.
3. Locate the number next to the Physical Address.

Note:
To find the Server Host ID (MAC address or Physical Address), you can also refer to the WebLM Server Properties page.

This is the MAC address. The MAC address is displayed in the form **`00-02-2D-11-55-4D`**. Following is an example from the command prompt of the ipconfig /all output:

```
Ethernet adapter Wired:
        Connection-specific DNS Suffix  . : roundfile.com
       Description . . . . . . . . . . . : ORiNOCO PC Card (5 Volt)
        Physical Address .. . . . . . . . : 00-02-2D-11-55-4D
```

4. Use your established Product Licensing and Delivery System (PLDS) Web procedures for obtaining licenses for Avaya servers.
   a. Use the MAC address you obtained in step 3.

b. Go to the PLDS Web site at http://plds.avaya.com and download the license file to a location that can be accessed later on by services personnel.

5. Copy the license file to the one-X Mobile server.
6. Log into the Avaya one-X Mobile server and launch the Web browser.
7. Go to the address https://127.0.0.1:8443/WebLM/LicenseServer.
8. From the WebLM screen, select **License Administration** and then enter the WebLM default administrative password.

Note:
The default login ID for WebLM is admin and password is weblmadmin.

9. After your initial login to WebLM, the system prompts you to change the password. When you do, WebLM logs you out and expects you to log back in with your new password.
10. Select **Install license**.
11. Select **Browse** and navigate to the location where you saved the license file in step 4.
12. Select **Install**.

    The proxy server will renew acquired licenses every 5 minutes. Initially, however, it has not acquired any licenses (since none were installed) so the proxy server will attempt to acquire licenses every 60 seconds. After it has acquired all licenses, it will renew them every 5 minutes.
13. Proceed with the Avaya one-X Mobile Server administrative interface.

Avaya one-X Mobile Administration

The Avaya one-X Mobile Server administration user interface is available by typing a URL of this form into your browser's address bar: http://<server IP or name>/Admin.

You need the Microsoft Windows credentials to log into the Avaya one-X Mobile Server Administrative Web site. This includes credentials for the local host of the Avaya one-X Mobile Server or for the Avaya one-X Mobile Server domain.

The status screen is displayed by default when navigating to the Avaya one-X Mobile Server administrative interface.

On the Status page, in the Mobile Release Synchronization group box, click **Synchronize mobile software release versions**. This will synchronize the one-X Mobile database with the most current software release versions for mobile devices. You must do this before users can log into the Avaya one-X Mobile Web site.

If the user requires a proxy server to access app.avaya.com outside the enterprise firewall, you must add configuration for that proxy server in the one-X Mobile server file, C:\edge\gemini\enduserweb\web.config. That configuration should look like this:

```
<!-- proxy -->
<system.net>
 <defaultProxy>
 <proxy usesystemdefault="false" proxyaddress="http://
your.proxy.here:8000" bypassonlocal="true" />
</defaultProxy>
</system.net>
```

After adding this proxy configuration, you must click the **Synchronize mobile software release versions** link on the **Status** tab of the one-X Mobile Administration interface in order to force a resynchronize with app.avaya.com.

You can complete administrative tasks by updating the configurations on the tabs on this screen. If the Avaya one-X Mobile Server is being configured for the first time, click the **Server Setup** tab.

Note:
Synchronization will run in the background and might take some time to complete.

Configure the Avaya one-X Mobile Server

The Server Setup section of the Avaya one-X Mobile administrative interface is used to configure administrative information for the following servers:

- SMTP server
- one-X Mobile External server (if the External Server is deployed)
- one-X Mobile Internal server

The **Server Setup** page provides two tabs:

- **Settings**—enables configuration of the SMTP Setting and Language Setting
  The Avaya one-X Mobile Server uses the SMTP server to send notifications of new voicemail to the users.
- **Split Server Configuration**—enables configuration of internal and external servers when multiple servers are used
  The Split Server Configuration settings can be configured only if a split server setup was chosen at the time of installation.

Configure the Server Settings

To configure the Avaya one-X Mobile Server Settings:

1. Click **Server Setup > Settings**.
2. In the **one-X Mobile Server IP Address** field, enter the IP address of the internal one-X Mobile server.
3. From the **User Interface Language** drop-down list, select the appropriate language.
4. In the **SMTP Username** field, enter the username that will be used to login to the SMTP server.
5. In the **SMTP Password** field, enter the SMTP password.
   The system displays the asterisks in the field for security purposes.
6. In the **SMTP Server** field, enter the IP address or hostname of the SMTP server.
   For example, enter 192.168.20.6. Enter the SMTP Username and Password only if the server requires authentication.
7. In the **SMTP Port** field, enter the number of the SMTP port.
   The default port number for SMTP is typically 25.
8. In the **Sender's email** field, enter the sender's e-mail address.
   Use a descriptive name such as notifier@example.com. The end user will see this e-mail address as the sender of links for one-X Mobile device software updates and notifications of new voicemails.
9. In the **Administrator's email** field, enter the Avaya one-X Mobile Server administrator's e-mail address. This is the e-mail address of the administrator that will be setting up and managing the system.

   When certain events occur, the Avaya one-X Mobile Server can send an e-mail to notify the IT administrator. An example of this is when an account is locked out due to exceeding the allowed number of login retries.
10. Click **Save Changes**.

Configure Split Server Settings

The Split Server Configuration settings can be configured only if a split server setup was chosen at the time of installation.

To configure the split server settings:

1. Select **Server Setup > Split Server Configuration**.

   The Split Server Configuration page identifies the IP address of the internal server as it exists on the external servers. It also identifies the IP addresses of all servers allowed access to the internal server.

Note:
The **localhost** field is pre-populated with the loopback IP address 127.0.0.1.

2. Modify the fields as appropriate, and then click **Save Changes**.
3. To add a server that will be allowed access to the internal server, click **Add Trusted Server**.

Note:
Ensure that you add one-X Mobile internal and external servers as trusted servers.

4. In the **Server Name** field, enter a name for this server.
5. In the **Server IP Address** field, enter the server IP address as appropriate.
6. From the **Server Type** drop-down list, select the type of server.
7. Click **Save**.

For more information on the split server configuration, see the *Avaya one-X Mobile Installation Guide*. The Avaya one-X Mobile Server must know the IP addresses of external servers for security purposes. This prevents connections from non-approved servers.

Chapter 5: Avaya Setup

The Avaya Setup section of the Avaya one-X Mobile administrative interface allows you to set up the Avaya one-X Mobile Server for systems that use Communication Manager.

Perform the Avaya Setup tasks in the following order:

1. Setup Profiles:
    a. Create a Provisioning Profile
    b. Create a Phone Number to Extension Conversion Rule
    c. Create a Communication Manager Profile
    d. Create a Voicemail Profile
    e. Create a Corporate Directory Profile
    f. Create a Class of Service
2. Administer Users:
    a. Import Users
    b. Manage Unlicensed Users
    c. Manage Licensed Users
3. Configure Dial Plans and Conversion Rules

Create a Provisioning Profile

The Provisioning Profile must be completed before any further steps are taken. The Provisioning Profile task imports the users from the Active Directory and is used for two purposes:

- To indicate the source of user accounts that will be imported into the Avaya one-X Mobile database. For example, Active Directory.
- To indicate the source for user account authentication. For example, Active Directory.

Avaya one-X Mobile is capable of using LDAP v3 directories for the Provisioning Profile.

To create a new Provisioning Profile:

1. Select **Avaya Setup > Setup Profiles > Provisioning Profile**.
2. Click **New Provisioning Profile**.

3. In the **Profile Name** field, choose a unique profile name which will identify this profile.

   Note:
   This is the name that is used when specifying a Corporate Directory Profile for a Class of Service.

4. In the **Description** field, enter a description for the profile.
5. From the **LDAP Search Type** drop-down list, select the appropriate search type.

   This field defines the type of LDAP search based on the LDAP platform. Specific search routines are provided for Active Directory, SunOne, and Netscape_iPlanet. In addition, a generic search routine is provided that is platform independent. Choosing an appropriate platform results in better search performance.

   - Microsoft Active Directory 2000 and 2003 – offers support for paged searches
   - SunOne – offers support for Virtual Views
   - NetScape_iPlanet – offers support for Virtual Views
   - Generic – retrieves data from any other LDAP v3 compliant Directory Server if the user's LDAP server is not one of the above three supported platforms

   Note:
   The generic search operation can be highly resource consuming, depending upon the result set size. Also, for the same reason, the LDAP server may not always return complete results.

   Note:
   Support for Secure LDAP Connections (Optional): The one-X Mobile Provisioning and Corporate Profiles contain the LDAP connection and search configuration parameters. To setup a secure connection, the LDAP Hostname value needs to be prefixed with "ldaps://" and the port needs to be an LDAP secure port.
   If certificates are required, install the certificates and restart the one-X Mobile services such as the Apache Tomcat service by using the controls on the one-X Mobile administration interface's **Serviceability** tab. LDAP SSL Certificate import information is only displayed after you save the Provisioning Profile. If secure LDAP port is used, the port is typically 636.

   For details on installing and deleting LDAP certificates, see the *Avaya one-X Mobile Installation Guide*.

6. In the **LDAP User DN** field, enter the LDAP user DN (For example, cn=one-Xldap, ou=users, dc=example, dc=com). This is the user that will be used to search the directory for Avaya one-X Mobile users.
7. In the **LDAP Hostname** field, enter the IP address or FQDN of the MSS server.
8. In the **LDAP Port Number** field, enter the LDAP port number. For example, for the secure LDAP, the LDAP port number is 636. The default value is 389 or 636 for secure LDAP.
9. In the **LDAP Password** field, enter the password for this user.
   The system displays asterisks in the field for security purposes.

10. In the **LDAP Base DN** field, enter the search base DN (For example, ou=users, dc=example, dc=com.)

    Depending on the Directory setup, it may be necessary to fill out the advanced settings for LDAP attributes. The **LDAP Attributes** section allows for parameterization of the required fields as different directory implementations may use different attribute names to store the information required by the Avaya one-X Mobile Server.

    When Avaya one-X Mobile is first installed, the default names in the LDAP Attributes fields are the commonly-used Microsoft Active Directory attribute names. You may need to change these LDAP attribute names to make them consistent with the customer's LDAP implementation.

11. To change the LDAP attribute settings, click **Show Advanced Settings**.

12. In the **Extension** field, enter the attribute name used to hold the extension. If the extension does not exist in the directory, it may be derived as part of the import process.

    Note:
    This field is used to determine the extension if the **Determine Extension from** field is set to **From LDAP extension attribute** in the Advanced Settings of the Class of Service. See step 31 in Create a Class of Service on page 48 for more information.

13. In the **Phone Number** field, enter the attribute name for phone number.

    Note:
    This field is used to determine the extension if the **Determine Extension from** field is set to **Phone number using phone number conversion to extension** in the Advanced Settings of the Class of Service. See step 31 in Create a Class of Service on page 48 for more information.

14. In the **Handle or UserID** field, enter the attribute name for the user ID.

15. In the **First Name** field, enter the attribute name for the user's first name.

16. In the **Last Name** field, enter the attribute name for the user's last name.

17. In the **Email** field, enter the attribute name for the user's e-mail address.

18. In the **Department** field, enter the attribute name for the user's department.

19. In the **Directory Fetch Size** field, enter the appropriate number.

    Note:
    The LDAP administrator may have limited the return value size of requests by setting an LDAP page size limit. If this has been done, you must set the Directory Fetch Size to be equal to or less than the LDAP page size limit. Otherwise, requests to the LDAP server may time out.

20. From the **Search Referrals** drop-down list, select the appropriate setting. The options are:

    - **None** – select **None** if your User DN contains your LDAP Base DN, or if your User DN is at a higher level in the hierarchy than the LDAP Base DN.

- **Follow** – select **Follow** if your LDAP User DN is deeper than the LDAP Base DN in the DN hierarchy, or if your User DN is in a completely different tree. The LDAP server must allow for this type of search.
- **Ignore** – this option is not recommended.
- **Throw** – this option is not recommended.

Note:
From the **Search Referrals** drop-down list, you must select **None, Follow, Ignore, or Throw**. If you select **Follow** from the **Search Referrals** drop-down list, one-X Mobile retrieves the data from the referral URL. The commonly used values are **None** (no referrals) and **Follow** (follow referrals). **Ignore** and **Throw** options should be selected only in installations in which the system administrator has thorough knowledge of the domain forest. If used improperly, selecting Ignore or Throw may result in the failure of searches for particular objects in the domain. For more information on this topic see the following: http://java.sun.com/products/jndi/tutorial/ldap/models/exceptions.html, http://technet.microsoft.com/en-us/library/cc978014.aspx.

21. Click **Save**.
    The Provisioning Profile settings are saved.

Note:
If an entry was not configured correctly, the system displays an error message. Red text indicates the sections that contain errors.

On the **Provisioning Profile Edit** page, when you click **Save** or **Import Cert**, the system imports the LDAP SSL Certificate. The certificate is retrieved from the LDAP Hostname entry on the port specified by the LDAP Port Number entry.

On the **Provisioning Profile New** page, when you click **Save**, the system imports the LDAP SSL certificate.

Note:
You must create a dial plan, to be able to Create a Communication Manager Profile on page 40. To create a dial plan, see Add a New Dial Plan on page 61.

Create a Communication Manager Profile

The Communication Manager Profile is used to configure the one-X Mobile interface with Communication Manager.

To create a Communication Manager Profile:

1. Select **Avaya Setup > Setup Profiles > CM Profile**.
2. Click **New CM Profile**.
3. In the **CM Profile Name** field, enter a profile name.

4. In the **Description** field, enter a description for the profile.
5. In the **SIP Port** field, enter the port number.
   5060 port is the default port.
6. From the **SIP Protocol** drop-down list, select the SIP protocol.

   Note:
   The TLS (Secure) option is not supported. You must select TCP (non secure) SIP protocol.
7. From the **Phone number Conversion to Extension Rules** drop-down list, select the Phone number Conversion to Extension rule.
8. In the **one-X Speech Access Number** field, enter the extension used to access your one-X Speech server, if you have Avaya one-X® Speech installed.

   Note:
   If one-X Speech is available, you can place callbacks to it from the one-X Mobile client by clicking **Speech Access**.
9. In the **Callback routing prefix** field, enter the prefix digit string.
   This enables the Communication Manager to route the mobile leg of callbacks through a Global System for Mobile (GSM) gateway.

   Note:
   This strategy modifies the mobile leg of a callback, transforming it from a fixed-to-mobile (CM-to-cell phone) call to a less expensive mobile-to-mobile (GSM gateway-to-cell phone) call. The Communication Manager prepends the prefix digits to the phone number for all callback calls that it dials to the cell phone. The prefix digits force the selection of a route by using a trunk to the GSM gateway rather than a standard PSTN trunk. As part of the administration for this arrangement, in the Communication Manager, you must create the appropriate route to the GSM gateway and associate that route with the prefix digit string. For more information, contact your Communication Manager System Administrator.

   Note:
   The combined length of the International Direct Dialing (IDD) prefix and the Callback Routing prefix must be less than or equal to four.
10. Select the **Force callback via mobile device** check box to enable the client handset's callback preference setting to **Call via Mobile**. This option is applicable only when callback is initiated from the mobile device. It allows you to make callbacks through only the mobile carrier and does not allow callbacks through the PBX. When this checkbox is selected, the client handset's callback preference setting, **Call via PBX**, is disabled.

Note:

When users search the corporate directory for a contact, the contact's telephone number can be displayed and used either in E.164 format or as an extension. The E.164 format is preferred.

The first administered Class of Service controls the phone number display format for all one-X Mobile users, regardless of their assigned Class of Service. You can find the first Class of Service immediately after the **Default** entry on the **Class of Service** tab (**Avaya Setup -> Setup Profiles -> Class of Service**).

To configure the E.164 display format for contact numbers, you must first determine the name of the attribute that the LDAP server uses to store each contact's E.164 phone number. When you have determined the LDAP attribute name, perform the following steps:

- Configure the **Corporate Directory Profile** so that the **Extension** field contains the LDAP attribute name identified above, (**Show Advanced Settings** link, **LDAP Attributes** section).
- **Edit the first Class of Service entry**: Click **Show Advanced Settings** and navigate to the **LDAP Attribute Source Profiles** section.
- From the **Determine Extension from** drop-down list, select **LDAP Extension Attribute**.
- From the **Phone Number Source** drop-down list, select **Corporate Directory Profile**.
- Click **Save** to save the configuration.

11. In the **Incoming call routing prefix** field, enter the dial string prefix that will enable the Communication Manager to route the user's incoming calls to the Mobile Send Calls destination through a GSM gateway (lower cost) rather than through a PSTN trunk (higher cost).

Note:

The prefix is applied only to the off-net number Send Calls destination. Other Send Calls destinations (desk phone, quick entry, and others) are routed in the standard manner in the Communication Manager.

12. In the **CLAN or PROCR IP address** field, enter the IP address for the CLAN or PROCR (Communication Manager server Processor Ethernet interface), which serves as the Communication Manager end of the one-X Mobile-to- Communication Manager SIP trunk.
13. Click **Save**.

Note:

Configuring multiple Communication Manager Profiles with the same CLAN or PROCR IP Address interferes with call control and causes call failure. Do not create multiple Communication Manager Profiles with the same CLAN or PROCR IP Address.

Create a Voicemail Profile

There are two types of Voicemail Profiles:

- **Modular Messaging with Exchange Integration**—the settings displayed under this type of Voicemail Profile are LDAP Settings and Exchange Administrative User Setting

  Note:
  You must create a domain user account and provide specific administrative access to the mailboxes that are managed by one-X Mobile on the MS Exchange Server. This domain user account should not have an associated Exchange Mailbox. If you are using MS Exchange 2000 or 2003, see Integration with Modular Messaging using MS Exchange 2000 or 2003 on page 22. If you are using MS Exchange 2007, see Integration with Modular Messaging using MS Exchange 2007 on page 24.

- **Modular Messaging with MSS (Default for Avaya)**—the settings displayed under this type of Voicemail Profile are MSS Administrative User Setting, MSS LDAP Settings, and Voicemail Mailbox Setting

  Note:
  The server specified in the MSS Administrative User Setting section must be set up in the Trusted Servers section on the MSS Admin page. See Integration with Modular Messaging on page 21 for more information.

To create a new Voicemail Profile:

1. Select **Avaya Setup > Setup Profiles > Voicemail Profile**.
2. Click **New Voicemail Profile**.
3. In the **Profile Name** field, choose a unique profile name which will identify this profile.

   Note:
   This is the name that is used when specifying a Corporate Directory Profile for a Class of Service.
4. From the **Profile Type** drop-down list, select the profile type.
5. In the **Voicemail Platform Hostname** field, enter the hostname of the voicemail platform.
6. In the **IMAP Port** field, enter the IMAP port. In the previous field, if you selected **Modular Messaging with MSS**, the IMAP Port should be a secure port. The IMAP Secure port is typically 993. For the Modular Messaging with Exchange Integration profile type, the IMAP port is often 143.
7. From the **Voicemail Audio Format** drop-down list, select the format that matches the audio encoding set for the voicemail domain on the Modular Messaging System.
8. Depending on the Profile Type you selected in step 4, do one of the following:
   - If you selected Modular Messaging with Exchange Integration, see Voicemail profile with Exchange Integration on page 44

- If you selected Modular Messaging with MSS, see Voicemail profile with MSS integration on page 45

Note:
To delete the MSS SSL certificate, click **Delete Cert**. To import the MSS SSL certificate, click **Import Cert**. The system displays these buttons only when you edit a voicemail profile.

On the Voicemail Profile edit page, when you click **Save** or **Import Cert**, the system imports the MSS SSL Certificate. The certificate is retrieved from the Voicemail Platform Hostname entry on the port that is designated from the IMAP Port entry.

Voicemail profile with Exchange Integration

If you select a **Profile Type of Modular Messaging with Exchange Integration** in the New Voicemail Profile, the system displays the LDAP Settings and Exchange Administrative User Setting sections.

The **LDAP Settings** section enables the configuration of the location and authentication credentials of the Active Directory associated with the Microsoft Exchange Server. The Avaya one-X Mobile Server must be a member of a domain that is trusted by the Microsoft Exchange Servers where Modular Messaging deposits voicemail. Access to Active Directory is required by the Avaya one-X Mobile Server for the following tasks:

- To accurately map received voice messages with the person that left the message
- To retrieve configuration information such as the hostname of the Microsoft Exchange Server for a particular user
- To retrieve the Microsoft Exchange Alias of a particular user

The **Exchange Administrative User Setting** section enables the configuration of the location and authentication credentials of the Exchange Server. Access to the Exchange Server is required by the Avaya one-X Mobile Server to provide Visual Voicemail functionality. You must enter authentication credentials of the Exchange Administrator User so that the Avaya one-X Mobile Server can access voicemail for any user.

To Voicemail profile with Exchange Integration:

1. In the **Active Directory IP Address** field, enter the Active Directory IP address or hostname.
2. In the **Active Directory Port Number** field, enter the Active Directory LDAP port number. In Active Directory deployments, port 389 is the default LDAP port.
3. In the **Administrator User DN** field, enter the Active Directory administrator user DN (for example, cn=one-Xldap, cn=users, dc=example, dc=com).
4. In the **Administrator Password** field, enter the Active Directory administrator password. The system displays an asterisk for security purposes when the password is entered.

5. In the **User Base DN** field, enter the Active Directory user base DN (for example, cn=users, dc=example, dc=com). This should be the base DN where all users of Modular Messaging are stored.
6. In the **Exchange Username** field, enter the username for the Exchange Administrative User you wish to use for Visual Voicemail to access end user messages. Note that the domain name must be included here for Visual Voicemail to work correctly (for example, mydomain\administrator).

   Note:
   You must create a domain user account and provide specific administrative access to the mailboxes that are managed by one-X Mobile on the MS Exchange Server. This domain user account should not have an associated Exchange Mailbox. If you are using MS Exchange 2000 or 2003, see Integration with Modular Messaging using MS Exchange 2000 or 2003 on page 22. If you are using MS Exchange 2007, see Integration with Modular Messaging using MS Exchange 2007 on page 24.
7. In the **Exchange Password** field, enter the Exchange Administrative User password. The system displays asterisks for security purposes when the password is entered.
8. Click **Save** to save the Voicemail Profile settings.

   Note:
   If an entry was not configured correctly, the system displays an error message. Red text indicates the sections that contain errors.

Voicemail profile with MSS integration

If you selected **Modular Messaging with MSS** in the **Profile Type** field in the New Voicemail Profile, the system displays the MSS Administrative User Setting, MSS LDAP Settings, and Voicemail Mailbox Settings sections.

To configure voicemail profile with MSS integration:

1. In the **Trusted Server Name** field, enter the same Trusted Server Name that was created in the Trusted Servers section on the MSS Admin page. For more information, see Integration with Modular Messaging on page 21.
2. In the **Trusted Server Password** field, enter the same Trusted Server Password that was created in the Trusted Servers section on the MSS Admin page. For more information, see Integration with Modular Messaging on page 21.
3. In the **LDAP User DN** field, enter the LDAP user DN in the format “cn=<trusted_server_name>,dc=Avaya”. For example, “cn=onexmobile,dc=Avaya".
4. In the **LDAP Hostname** field, enter the LDAP hostname, that is, the IP Address or FQDN of the MSS server.
5. In the **LDAP Port Number** field, enter the LDAP port number. For example, the LDAP port number for MSS is 389 and for the secure LDAP, the LDAP port number is 636.

6. In the **LDAP Password** field, enter the LDAP password.
7. In the **LDAP Base DN** field, enter the search base DN (always in MSS, the setting is ou=People, dc=Avaya**)**.
8. From the **Voicemail Mailbox ID Source** drop-down list, select the source for the voicemail mailbox ID.
9. Click **Save** to save the Voicemail Profile settings.
   The MSS SSL Certificate is retrieved from the MSS when you click Save for the first time.

Note:
If an entry was not configured correctly, the system displays an error message. Red text indicates the sections that contain errors.

Create a Corporate Directory Profile

In order to provide the Avaya one-X Mobile client Corporate Directory Lookup feature, the Avaya one-X Mobile Server must integrate with a directory source such as Active Directory or SunOne. This integration is known as a Corporate Directory Profile and may later be applied to a Class of Service which can be applied to a user group.

Note:
one-X Mobile builds a single Corporate Directory view based on the enterprise directory sources specified in the profiles.

To create a Corporate Directory Profile:

1. Select **Avaya Setup > Setup Profiles > Corporate Directory Profile**.
2. Click **New Corporate Directory Profile**.
3. In the **Profile Name** field, choose a unique profile name which will identify this profile.

   Note:
   This is the name that is used when specifying a Corporate Directory Profile for a Class of Service.
4. In the **Description** field, enter a description of this profile.
5. From the **LDAP Search Type** drop-down list, select the LDAP search type. This field defines the type of LDAP search based on the LDAP platform. A specific search routine is provided for Active Directory, SunOne, and Netscape_iPlanet. In addition, a generic search routine is provided that is platform independent. Choosing the appropriate platform will provide better search performance.
6. In the **LDAP User DN** field, enter the LDAP user DN (for example, cn=one-Xldap, ou=users, dc=example, dc=com).
   The login used to administer one-X Mobile is typically the user selected for this entry.
7. In the **LDAP Hostname** field, enter the IP address or FQDN of the MSS server.

8. In the **LDAP Port Number** field, enter the LDAP port number. The default value is 389 or 636 for secure LDAP.
9. In the **LDAP Password** field, enter the LDAP password for the user specified in the **LDAP User DN** field.
10. In the **Corporate Directory Search Base DN** field, enter the corporate directory search base DN (for example, ou=users, dc=example, dc=com).
11. Click **Show Advanced Settings** to view the LDAP Attributes section.
12. In the **User LDAP Filter** field, enter the user LDAP filter. This field provides for an LDAP search filter specification used to build the Corporate Directory. For example, you will enter *objectclass=user* in this field to restrict retrievals from the LDAP server to user entries.
13. In the **Extension** field, enter the attribute name used to hold the extension.

Note:
If the user's extension attribute is not populated in the directory, it may be derived as part of the import process.

14. In the **Phone Number** field, enter the attribute name for phone number.
15. In the **Handle or UserID** field, enter the attribute name for the user ID. This attribute name is identical to the one entered in the **LDAP Attributes** section of the **Provisioning Profile** tab.
16. In the **First Name** field, enter the attribute name for the user's first name.
17. In the **Last Name** field, enter the attribute name for the user's last name.
18. In the **Email** field, enter the attribute name for the user's e-mail address.
19. In the **Department** field, enter the attribute name for the user's department identifier.
20. In the **Directory Fetch Size** field, enter the appropriate number.

Note:
The LDAP administrator may have limited the return value size of requests by setting an LDAP page size limit. If this has been done, you must set the Directory Fetch Size to be equal to or less than the LDAP page size limit. Otherwise, requests to the LDAP server may time out.

21. From the **Search Referrals** drop-down list, select the appropriate setting. The options are:
    - **None** – select **None** if your User DN contains your LDAP Base DN, or if your User DN is at a higher level in the hierarchy than the LDAP Base DN
    - **Follow** – select **Follow** if your LDAP User DN is deeper than the LDAP Base DN in the DN hierarchy, or if your User DN is in a completely different tree. The LDAP server must allow for this type of search
    - **Ignore** – this option is not recommended
    - **Throw** – this option is not recommended
22. Click **Save** to save the Corporate Directory Profile settings.

Note:

If an entry was not configured correctly, the system displays an error message. Red text indicates the sections that contain errors. Ignore and Throw options should be selected only in installations in which the system administrator has thorough knowledge of the domain forest. If used improperly, selecting **Ignore** or **Throw** may result in the failure of searches for particular objects in the domain. For more information on this topic see the following: http://java.sun.com/products/jndi/tutorial/ldap/models/exceptions.html, http://technet.microsoft.com/en-us/library/cc978014.aspx.

Create a Class of Service

After completing the profiles, a Class of Service is required. Class of Service is a representation of ways in which an Avaya one-X Mobile user will interact with the system. Class of Service settings include profiles (as described earlier in this chapter) as well as non-aggregated settings.

Note:

A valid Provisioning Profile is required to create a Class of Service. The system displays an error message if there is an attempt to create a Class of Service using an invalid Provisioning Profile.

To create a new Class of Service:

1. Select **Avaya Setup > Setup Profiles > Class of Service**.
2. Click **New Class of Service**.
3. In the **Class of Service Name** field, enter a unique name for this class of service.
4. In the **Description** field, enter a description of this Class of Service.
5. From the **Provisioning Profile** drop-down list, select the appropriate profile.
6. From the **Voicemail Profile** drop-down list, select the appropriate profile.

Note:

Select **No Voicemail Profile** to configure this Class of Service so that users will not have voicemail on their mobile client. The mobile client will provide Call Control only and will not be integrated with a voicemail platform.

7. From the **Corporate Directory Profile** drop-down list, select the appropriate profile.
8. From the **CM Profile** drop-down list, select the appropriate profile.
9. Select the **Allow voicemail to be stored on the mobile device** check box if you want to enable voicemail download to the Avaya one-X Mobile Web client or Avaya one-X Mobile client.

Note:

Select the **Allow voicemail to be stored on the mobile device** check box if you want to enable voicemail download to the Avaya one-X Mobile Web client or Avaya one-X Mobile Client. You can download or save voicemail on the Avaya one-X Mobile Client, or download, or save voicemail from the Avaya one-X Mobile Web client. Alternatively, call the corporate voicemail to listen to the voicemails from the Avaya one-X Mobile Web client or Avaya one-X Mobile client. If **Allow voicemail to be stored on the mobile device** check box is not selected, the user can still view the caller's name or number but must call the corporate voicemail number directly to listen to voicemail from the Avaya one-X Mobile Web client or mobile device.

10. Select the **Allow voicemail to be forwarded via email** check box if you want to enable the forward via e-mail feature available on Avaya one-X Mobile Web client.

Note:

Clear the **Allow voicemail to be forwarded via email** check box if you want to disable the forward via e-mail feature available on Avaya one-X Mobile Web client.

11. Select the **Require login each time one-X Mobile is launched on mobile device** check box, if required.
12. Set the **Maximum number of attempts before user is locked out** (default is 7).
13. Set the **Time period for which a user is locked out in minutes** (default is 90).
14. Set the **Maximum number of phones to Send Calls to**.

Note:

The minimum and maximum number of phones to send calls to is 2 and 5 respectively.

15. Set the **PSTN Prefix**.
    PSTN Prefix is the number that you need to dial to reach an external phone line.
16. Select the **Require DTMF during Callback via PBX** check box if you require that the mobile user indicate readiness to participate in a callback by pressing a key to generate a DTMF tone back to the Communication Manager. If you select this check box, then callbacks initiated by the mobile handset will only complete if Communication Manager receives the confirmation DTMF tone.
17. Select the **Require DTMF during incoming calls** check box if you require that the mobile user indicate readiness to participate in an incoming call by pressing a key to generate a DTMF tone back to the CM. If you select this check box, then incoming calls to the mobile handset will only complete if Communication Manager receives the confirmation DTMF tone.
18. Select the **Translate e-164 numbers to extensions** check box if you want one-X Mobile to determine whether or not a callback destination is an on-PBX number that has been entered in e.164 format. The one-X Mobile software uses dial plans to do the conversion.

19. Select the **Transform Send calls destination numbers using user entered to PBX dialable number rules** check box if you want one-X Mobile to use its dial plans to ensure that user-entered digit strings are converted to dialable numbers before they are sent to the PBX.

    Note:

    The **User entered number to mobile (EC500) format** dial plan is always applied to the mobile and quick entry numbers. In the **Class of Service** tab, when you select the **Transform Send calls destination numbers using user entered to PBX dialable number rules** check box, the **User entered number to PBX dialable number for Callbacks** dial plan is applied (from the **Dial Plans and Conversion Rules** tab) and then the **User entered number to mobile (EC500) format** dial plan is applied on the mobile and quick entry numbers.

20. Select the **Apply National Direct Dialing Prefix to send calls destination numbers** check box if **User entered number to PBX dialable number for Callbacks** needs a National Direct Dialing prefix.

21. Select the **Require client software upgrades** check box if you want to enable the mobile client software upgrade notifications.
    When you select the **Require client software upgrades** check box, the mobile client software upgrade notifications are sent to the users as per the number of days entered in the **Number of days to warn users before making updates mandatory** field.

22. In the **Number of days to warn users before making updates mandatory**, enter the number of days after which you want the mobile client software upgrade notifications to be sent to the users.
    In the **Number of days to warn users before making updates mandatory** field if you enter 7, then after seven days upgrading your mobile client software becomes mandatory. When upgrades for mobile devices are checked by the one-X Mobile server, the users in this Class of Service who have their user account configured receive notifications to upgrade.

23. From the **User Interface Language** drop-down list, select the appropriate language.

24. Click **Show Advanced Settings** to view the LDAP Attribute Source Profiles.

    In the **LDAP Attribute Source Profiles** section, there is an opportunity to fine tune the Avaya one-X Mobile Server to use different directory sources for different data fields collected from directories. In some enterprise deployments, one directory may contain some information such as first name, last name; while another may contain information such as the phone number.

    The Avaya one-X Mobile Server can map from one directory to another; where the sources are the Corporate Directory Profile and the Provisioning Profile. The Provisioning Profile will always be used for authentication and the Corporate Directory Profile may be used for name resolution. In all cases, the **Handle or UserID** must be the key between the two directory sources. That is, if mapping is done, the UserID in one directory must match that of the other directory.

    Use the drop-down lists to tell the Avaya one-X Mobile Server from what directory to source the different attributes. Once the directory source is set for each attribute and Class of Service (COS) is saved, then the same attribute mappings are set for all defined class of services. This ensures a consistent one-X Mobile directory configuration across the enterprise.

25. From the **Handle or UserID** drop-down list, select the appropriate profile.
26. From the **Phone Number** drop-down list, select the appropriate profile.
27. From the **First Name** drop-down list, select the appropriate profile.
28. From the **Last Name** drop-down list, select the appropriate profile.
29. From the **Email** drop-down list, select the appropriate profile.
30. From the **Department** drop-down list, select the appropriate profile.
31. From the **Determine Extension from** drop-down list, select the appropriate source.

Note:

For the **Determine Extension from** drop-down list, extensions for users can be determined either directly from the LDAP attribute or from the phone number by using the dial plan.

Note:

When users search the corporate directory for a contact, the contact's telephone number can be displayed and used either in E.164 format or as an extension. The E.164 format is preferred.

The first administered Class of Service controls the phone number display format for all one-X Mobile users, regardless of their assigned Class of Service. You can find the first Class of Service immediately after the **Default** entry on the **Class of Service** tab (**Avaya Setup -> Setup Profiles -> Class of Service**).

To configure the E.164 display format for contact numbers, you must first determine the name of the attribute that the LDAP server uses to store each contact's E.164 phone number.

When you have determined the LDAP attribute name, perform the following steps:

- **Edit the Corporate Directory Profile**: In the **Provisioning Profile** tab, click **Show Advanced Settings** and under the **LDAP Attributes** section add the LDAP attribute name in the **Extension** field as identified above in the note.
- **Edit the first Class of Service entry**: Click **Show Advanced Settings** and navigate to the **LDAP Attribute Source Profiles** section.
- From the **Determine Extension from** drop-down list, select **LDAP Extension Attribute**.
- From the **Phone Number Source** drop-down list, select **Corporate Directory Profile**.
- Click **Save** to save the configuration.

32. From the **LDAP Extension Source** drop-down list, select the appropriate profile.
33. Click **Save**.

Administer Users

This section describes how to provision users for whom the Avaya one-X Mobile Server services will be available. This section describes how to:

- Import Users
- Manage Unlicensed Users
- Manage Licensed Users

Import Users

To import users:

1. Select **Avaya Setup > Users > Import Users**.
2. From the **Class of Service** drop-down list, select the appropriate Class of Service.
3. In the **Filter** field, enter the filter. Valid filters are similar to those entered directly in LDAP:
   - To import a single user, use **sAMAccountName=<LDAPusername>**. For example, to import a single user enter **sAMAccountName=edge8**.

   Note:
   Use the wildcard characters cautiously because these can import a large number of users.

   - To import several users, **use wildcards cn=edge*, objectclass=user**. For example, to import several users, enter **cn=edge***, **cn=one-Xldap**, **mail=*mydom.com**.

   Note:
   The screen does not refresh itself during a user import.
4. Click **Import Users**.
   The system displays a message letting you know that it is importing users in a background process.

   Note:
   Navigate to the "Unlicensed User Management" tab to confirm that the users were correctly imported.

Manage Unlicensed Users

To view all imported user accounts that are not yet licensed:

1. Select **Avaya Setup > Users > Unlicensed User Management**.
2. To search for specific users, enter text in the **Search** field.
3. Click **Show All** to display a list of all users after performing a search.
4. From the **Show** drop-down list, select the appropriate page to change the page displayed.
5. From the **Sort by** drop-down list, select the appropriate item to change the way the information is sorted on the page.

License Selected Users

To license a user:

1. On the Unlicensed User Management screen, click the check box next to the name of the user that you want to license.
2. Click **License Selected Users**.

   This will license the user in the Avaya one-X Mobile Server database and decrement the number of licenses available for assignment.

   Licensing users can take some time depending on the size of the user base. When users are licensed, the Avaya one-X Mobile Server works in the background to retrieve required provisioning information for the user. When complete, you will be able to locate the new users in the **Licensed User Management** tab.

Manage Licensed Users

To view all imported user accounts that are licensed:

1. Select **Avaya Setup > Users > Licensed User Management**.
2. To search for a user, in the **Search** field enter the first few characters of last name, first name, and extension. For example, in the **extension** field, if you enter 33, the system will return the search results with the telephone extensions starting with 33.
3. From the **Show** drop-down list, select the appropriate page to change the page displayed.
4. From the **Sort by** drop-down list, select the appropriate item to change the way the information is sorted on the page.

To manage licensed users, the following features are available:

- Change Class of Service
- Reprovision Selected Users

- Unlicense Selected Users
- Delete Selected Users

Change Class of Service

To change the Class of Service for a user or group of users:

1. On the **Licensed User Management** screen, click the check box next to each user for whom you want to change the Class of Service.
2. Click **Change Class of Service**.
3. From the **Class of Service** drop-down list, select the new class of service.
4. Click **Yes**.

Reprovision Selected Users

To reprovision users or a group of users:

1. On the **Licensed User Management** screen, click the check box next to each user or user group that you want to reprovision.
2. Click **Reprovision Selected Users**.
3. Click **Yes**.

   The Avaya one-X Mobile Server retrieves the new user information and updates the Avaya one-X Mobile Server database.

Unlicense Selected Users

Unlicensed users are not able to log in to their Avaya one-X Mobile account from either the Avaya one-X Mobile Web site or their mobile device.

To unlicense a user:

1. On the **Licensed User Management** screen, select the check box next to the user you want to unlicense.
2. Click **Unlicense Selected Users**.

   This will increment the number of licenses available for assignment.

   Important:
   When you revoke the license from the user, the Avaya one-X Mobile Server does not manage the calls for that user.

Delete Selected Users

Deleting a user will delete all the call logs and any other data associated with that user in the Avaya one-X Mobile database. The user will not be able to login to their Avaya one-X Mobile account from either the Avaya one-X Mobile Web site or their mobile device.

To delete a user:

1. On the **Licensed User Management** screen, click the check box next to the users you want to delete.
2. Click **Delete Selected Users**.

   This will decrement the number of used licenses and remove the user from the Avaya one-X Mobile Server database. It will **not** remove the user from the LDAP directory.

View User Details

Click on **Details** next to any user on the **Licensed User Management** or **Unlicensed User Management** screens to display more information about that user.

From the User Details screen you can:

- Reprovision a user
- Delete a user
- Take action on a user's account if the user has lost their mobile phone
- Take action on a user's account if the user is no longer an employee
- Unlock a locked user account

Lost or Stolen Mobile Phone

If a user's mobile phone has been lost or stolen, click on **Lost or Stolen Mobile** on the User Details screen. This screen will provide instructions for further steps you should take. This may include resetting the user's password and loss of local data on their mobile phone.

No Longer an Employee

If a user is no longer an employee, click on **No Longer an Employee** on the User Details screen. This screen will provide further instructions depending on whether the user account needs to be retained or completely removed from the Avaya one-X Mobile Database.

Unlock one-X Mobile Account

A user account may get locked out by the Avaya one-X Mobile Server if the user enters an incorrect login too many times. This will prevent a user from logging into the Avaya one-X Mobile application on both their mobile phone and the Avaya one-X Mobile Web site. A user account that is locked will automatically be unlocked after the lockout time (as set in the Class of Service for the user) has expired.

If a user account needs to be unlocked before the lockout time expires, click on **Unlock one-X Mobile Account** on the User Details screen. This will unlock the user account, and access to the Avaya one-X Mobile Web site and the Avaya one-X Mobile application on the user's mobile phone will be allowed.

Note:
This does not unlock a user's voicemail mailbox.

Configure Dial Plans and Conversion Rules

The Dial Plans and Conversion Rules section shows how the dial plans and conversion rules are configured. The Dial Plans and Conversion Rules section allows the administrator to setup conversion rules and dialing rules. For Avaya Setup, this is based on the Class of Service. For international support, the phone numbers in LDAP must have a format that includes the country code.

Note:
One important difference in functionality between one-X Mobile 1.1 and one-X Mobile 5.2 is that one-X Mobile 5.2 only handles off-PBX destinations for simulring and as the service link or first leg of a callback. In one-X Mobile 1.1, it was possible to use the quick entry destinations to set on-PBX extension numbers as simulring destinations. The mobile destination did not have this capability as it used EC500 routing to allow for Easy Mobile switcher, extend call features, and other mobility features. In one-X Mobile 5.2, all destinations (including quick entry) leverage the EC500 capabilities. A key restriction around this is that any valid destination must be routed out from a trunk off the PBX.

To configure Dial Plans and Conversion Rules:

1. Select **Avaya Setup > Dial Plans and Conversion Rules**.
2. In the **Country Code** box, enter the country code of the country where the office phone system (PBX) is located. The length of the Country Code must be less than or equal to three.

Note:
The only configuration currently supported is one where all PBXs have the same country code.

3. In the **IDD** box, enter the International Direct Dialing (IDD) prefix of the office phone system (PBX) where the extension is managed. The combined length of the International Direct Dialing (IDD) prefix and the Callback Routing prefix must be less than or equal to four. The administrator is not allowed to save the PBX Settings if the **IDD** field is blank.

   Note:
   This value must be provided to the managed users in order for them to dial an international number using the appropriate IDD.

4. In the **National Direct Dialing Prefix** box, enter the appropriate NDD prefix. The length of NDD must be greater than zero and less than equal to fifteen.

   The NDD prefix is the access code used to make a call within a particular country from one city to another. When calling from one city to another in the same vicinity, an NDD prefix may not be necessary. The NDD prefix is followed by the city/area code for the place you are calling. Phone numbers are often written in the format **+44-(0)1224-XXXX-XXXX**. This represents the numbers used for both international and national long-distance calls. In this example, **+44** is the country code and **(0)** indicates the NDD. When dialing from outside the country, the NDD *will not* be used after dialing the country code; when dialing from within that country, the NDD will be used, but the country code will not.

5. In the **National Number Length** box, enter the appropriate National Number Length.

   For any country, the National Number Length is the total number of digits you dial to make up a complete phone number. For example, in the USA, to dial the number **408-XXX-XXXX**, the National Number Length will be 10.

   Note:
   In the EMEA region, the dial plan numbering varies and it is not fixed to ten digits. For variable national number length, enter the appropriate comma separated values in the **National Number Length** field.

6. Select the **Strip Caller ID Prefix** check box to remove the prefix of the caller ID.

   Note:
   In some environments, the caller ID is prefixed with an extra prefix.

7. Click **Save** to save the PBX settings.

   The PBX settings section on the Dial Plans and Conversion Rules page allows the admin to setup country specific items such as the country code, international dialing code, and national number length. This is configured on a per system basis. This release of one-X Mobile supports multiple PBX's within the same country, but not multiple countries from the same one-X Mobile installation.

   There are several types of number transformations that one-X Mobile requires. This includes: extension conversion, conversion from a user entered number to a dialable string (from a deskset), conversion from User entered number to PBX dialable number for Callbacks to user entered number to mobile (EC500) format, and conversions for external numbers.

   In the Dial Plans and Conversion Rules section, you can configure the transformations for **User entered number to PBX dialable number for Callbacks** and **User entered number to mobile (EC500) format**. Create a new dial plan to define a new dial plan rule.

   The rules are applied to the following:

- Dialable strings entered by users in the **Connect to** field for callbacks
- Mobile (EC500) format needed for the callback call to the off-net number, for Send Calls destinations, and for quick entry numbers

8. To configure additional rules, click **Edit** next to the appropriate CLAN IP.
9. Edit the information as appropriate.
10. Click **Save Changes**.

Add Non-LDAP Extension/Numbers to E.164 number Rules

The Non-LDAP Extension/Numbers to E.164 number rules convert extension numbers of users that are not imported from Active Directory to E164 format numbers so that these extension numbers can be displayed properly in the Call Log. When incoming call numbers are extension ranges or phone numbers in the PBX and that are not in LDAP user records, these rules modify the extension ranges or phone numbers to E.164 format.

To add a new external number rule for the external telephone numbers:

1. Select **Avaya Setup > Dial Plans and Conversion Rules**.
2. Click **Add New Rule**.
   The system displays the **New Rule** screen.
3. In the **Matching Pattern** box, enter the prefix or matching pattern to be identified, as follows:
   - Enter *ALL* if you want to match any numeric pattern.

- Enter the specific pattern if you want to match on that pattern. For example, if you want to set up a rule for dialing phone numbers beginning with 510, you will enter *510* in this box.

4. In the **Number Length** box, enter the length of the number for which the rule applies. For example, if you want the rule to apply only to numbers that begin with 510 and are 10 digits in length, you will enter *10* in this box.
5. In the **Strip Digits** field, enter the number of digits to delete from the beginning of the number.
   For example, enter *0* (zero).
6. In the **Add Prefix** field, enter the prefix that will be attached to the dialled number. For example, a new dial plan rule is configured as:

- Matching Pattern = 77
- Number Length = 5
- Strip digits = 0
- Add Prefix = 4085

In this example, no digits are stripped from the 5-digit extensions beginning with “77” and the extensions will be prefixed with the digits “4085.”

7. Click **Save**.

Add New Conversion Dial Plan

You can add the Phone number Conversion to Extension Rules to use these plans for converting caller ID of an incoming call to an extension. The conversion can happen if the caller is on the same switch but the caller is not identified in the enterprise directory and one-X Mobile is not able to resolve the number. You can also use the conversion dial plan to convert numbers from the LDAP to build the corporate directory.

To add a new conversion dial plan for the conversion of phone numbers to extensions while importing users:

1. Select **Avaya Setup > Dial Plans and Conversion Rules**.
2. Click **Add New Conversion Dial Plan**.
3. In the **Dial Plan Name** field, enter a name for the dial plan on the New Extension Conversion Plan page.

Note:
Pattern Matching is selected by default. You can either select Pattern Matching or Regular Expression.

4. Select **Pattern Matching** if you want to enter a pattern matching for conversion of extensions.

a. In the **Minimum Length** field, enter the minimum length for the extension number.
b. In the **Maximum Length** field, enter the maximum length for the extension number.
c. In the **Starts With** field, enter the number with which the extension number must start.
d. In the **Delete Length** field, enter the count of numbers that need to be deleted.
e. In the **Prepend** field, enter the number to be prepended.

5. Select **Regular Expression** if you want to enter a regular expression for conversion of extensions.
   a. In the **Expression** field, enter the expression for conversion of extensions.
   b. In the **Replace With** field, enter the number that you want to replace the expression.
6. Click **Save**.

Note:
If you want to test the extension conversion plan, enter the number to convert to extension in the **Number to Convert** field and click **Test Conversion**. You cannot use extensions as destinations.

Add a New Dial Plan

You can configure dial plans for **User entered number to PBX dialable number for Callbacks** and for **User entered number to mobile (EC500) format** conversions.

These are Send Calls destination numbers (typically your off-net number) and the off-PBX number that you are trying to call.

User entered number to PBX dialable number for Callbacks Dial Plan

When the user places a callback, the User entered number to PBX dialable number for Callbacks section is used. During a callback there are two calls placed. The first call is placed to the off-net number and the second call is placed to the destination requested by the user. This dial plan section handles the transformation needed for the second call. The number should be transformed as if it were being dialed from a deskset. one-X Mobile automatically places the PSTN prefix in this number when it detects that it is an off-PBX number that is being dialed.

User entered number to mobile (EC500) format Dial Plans

The user entered number to mobile (EC500) format dial plan deals with transformations on the first call of callback. The first call is placed to the user's off-net number. It also handles transformations needed for the Send Calls settings. These are the destinations the user enters to have one-X Mobile and Communication Manager ring those numbers on an incoming call.

To add a new Dial Plan:

1. Select **Avaya Setup > Dial Plans and Conversion Rules**.
2. Click **Add New Dial Plan**.
3. From the **CLAN or PROCR IP Address** drop-down list, select the appropriate CLAN or PROCR IP Address.

   Note:
   User entered number to PBX dialable number for callbacks is selected by default. You can either select **User entered number to PBX dialable number for callbacks** or **User entered number to mobile (EC500) format**.

4. Select **User entered number to PBX dialable number for callbacks** if you want to convert a phone number to PBX dialable number for callbacks.
   a. In the **Number Length** box, enter the length of the number for which the rule applies. For example, if you want the rule to apply only to numbers that begin with 510 and are 10 digits in length, you will enter *10* in this box.
   b. In the **Matching Pattern** box, enter the prefix or matching pattern.
      - Enter *ALL* if you want to match to any numeric pattern.
      - Enter the specific pattern if you want to match on that pattern. For example, if you want to set up a rule for dialing phone numbers beginning with 510, you will enter *510* in this box.
   c. In the **Strip Digits** box, enter the number of digits to delete from the beginning of the number.
   d. In the **Add Prefix** box, enter the prefix to add to the number.
   e. Click **Save**.
      The new dial plan for the **User entered number to PBX dialable number for callbacks** option is saved.

   Note:
   If you want to add another dial plan for the **User entered number to mobile (EC500) format** option, click **Add New Dial Plan**.

5. Select **User entered number to mobile (EC500) format** if you want to convert a phone number to mobile format.
   a. In the **Min Length** field, enter the minimum length for the User entered number to mobile (EC500) format rule.
   b. In the **Max Length** field, enter the maximum length for the User entered number to mobile (EC500) format rule.
   c. In the **Matching Pattern** box, enter the prefix or matching pattern.
      - Enter *ALL* if you want to match to any numeric pattern.

- Enter the specific pattern if you want to match on that pattern. For example, if you want to set up a rule for dialing phone numbers beginning with 510, you will enter *510* in this box.

d. In the **Strip Digits** box, enter the number of digits to delete from the beginning of the number.

e. In the **Add Prefix** box, enter the prefix to add to the number.

6. Click **Save**.
   The new dial plan for the **User entered number to mobile (EC500) format** option is saved.

There are two types of Dial Plans:

- User entered number to PBX dialable number for Callbacks
- User entered number to mobile (EC500) format

Important:
If you are prefixing for GSM gateways, the prefix will be part of the **IDD** field. Ensure that the IDD + GSM gateway prefix does not exceed four digits.

Important:
The ARS code is not used in the **user entered number to mobile (EC500) format** numbers. If ARS code is used, then it will cause a problem. The ARS is the number (“9” is typically used in many installations) that is used to access an external phone line. The Communication Manager includes the ARS code.

Important:
The **User entered number to mobile (EC500) format** dial plan is always applied to the mobile and quick entry numbers. In the **Class of Service** tab, when you select the **Transform Send calls destination numbers using user entered to PBX dialable number rules** check box, the **User entered number to PBX dialable number for Callbacks** dial plan is applied (from the **Dial Plans and Conversion Rules** tab) and then the **User entered number to mobile (EC500) format** dial plan is applied on the mobile and quick entry numbers.

Chapter 6: Serviceability

The Serviceability section of the Avaya one-X Mobile administrative interface allows monitoring and management of services, and provides information about Avaya one-X Mobile Server components and allows fine tuning of these components.

View Control Center

To view the Control Center, select **Serviceability > Control Center**.

Control Center allows you to stop, start, and monitor services controlled by the Avaya one-X Mobile Server. All components show whether they are installed or not.

View Trace Components

To view Trace Components, select **Serviceability > Trace Components**.

Trace Components allow you to manipulate the data stored in logs. The default setting for each field on this page is **debug**. Trace will provide the most granular level of detail, but is not currently implemented by any of the components.

View Component Info

To view Component Info, select **Serviceability > Component Info**.

Component Info provides information about various components such as version numbers and last known status.

Some of the server components are:

- one X Mobile Servlet - Used for call routing
- Avaya Call Control Service - Used for call processing. Replaces the old edge ccHandler service
- Apache Tomcat - Used for importing of users, Web requests, and licensing

- Message checker - Used for retrieving messages from and to the MS Exchange message store
- Notification Manager - Used for sending the new voicemail notifications

Note:
The list of Serviceability components are shown in the Control Center tab.

Chapter 7: Licenses

The Licenses section of the Avaya one-X Mobile administrative interface displays the most current information about licenses being used, licenses available, and licenses acquired.

View License Information

To view License Information:

1. Select **Licenses > License Information**.
2. In the **WebLM Hostname URL** field, enter the hostname of the WebLM server to get accurate information about licenses.

There are three Application Modes in which WebLM will operate:

- **Grace** — allows users to be licensed for a trial period of 30 days
  The number of grace days remaining will be displayed on the License Information page if the server is in Grace mode.
- **Normal** — indicates that WebLM is functioning normally
- **Restricted** — indicates the Grace period has expired and users cannot log in to their accounts

Chapter 8: Direct Call PBX Numbers

The Direct Call PBX Numbers section of the Avaya one-X Mobile administrative interface allows special numbers or a set of numbers to use the Avaya one-X Mobile callback and simulring features. These special numbers are not managed by Avaya one-X Mobile but they need to be processed as internal numbers. To configure this, use Direct Call PBX Numbers tab. An example of the Direct Call PBX number is a voicemail pilot. A voicemail pilot might not exist in the enterprise directory, but there might be a need to dial the voicemail pilot number as an internal number when making a callback to it. A dial-out prefix or dial plan is not applied to the Direct Call PBX numbers.

You can configure mapping rules in the Direct Call PBX Numbers tab to represent any extension numbers on the PBX that are not in the corporate directory. When these extensions are called by using the one-X Mobile callback or simulring feature, one-X Mobile will process these numbers as on-PBX extensions and will not insert a dial out prefix.

Note:

one-X Mobile cannot be used to simulring internal extensions. For example, you cannot use your co-worker's desk number as your simulring destination and Quick Entry number for callback.

To configure mapping rules for PBX numbers:

1. Select **Direct Call PBX Numbers**.
   The system displays the Direct Call PBX Numbers screen.
2. Click **New Direct Call PBX Number**.
3. From the **CLAN or PROCR IP Address** drop-down list, select the appropriate host name.
4. In the **Leading String** field, enter the extension number (or wild cards) that represents the set of extensions.
5. In the **Digit Count** field, enter the number of digits in the extension or set of extensions.
6. Click **Save**.

Appendix A: Log Cleaning Utility

This appendix provides the procedure to configure the Tomcat log cleaning utility so that it automatically runs on a specified schedule. This task is performed on the Windows server running the Avaya one-X Mobile Server software.

Note:
Ensure that SqlServerAgent.exe is running on the machine. This process handles the backup and cleanup of the database to ensure that the database does not reach the full capacity.

Note:
You can have between 10 files to 100 files (100 MB of logs) for the one-X Mobile components.

Schedule the Tomcat Log Cleaning Utility

To schedule the Tomcat log cleaning utility:

1. Select **Start > Control Panel > Schedule Tasks**.
2. Click **Add Scheduled Task**.
3. Click **Next**.
4. Browse to the folder <Edge installation folder>\Utilities, for example, C:\Edge\Utilities.
5. Open the file **tnlogDeleter.exe**.
6. Select **Daily**.
7. Click **Next**.
8. In the **Start time:** box, set the time to **12:30**, and then click **Next**.
9. Enter the **user name** and **password**.
10. Enter the **password** again to confirm, and then click **Next**.
11. Click **Finish** to close the Scheduled Task Wizard.

    The task will be performed at 12:30 AM, every day.

Appendix B: Dial Plan Configuration Scenarios

This appendix provides several dial plan configuration scenarios.

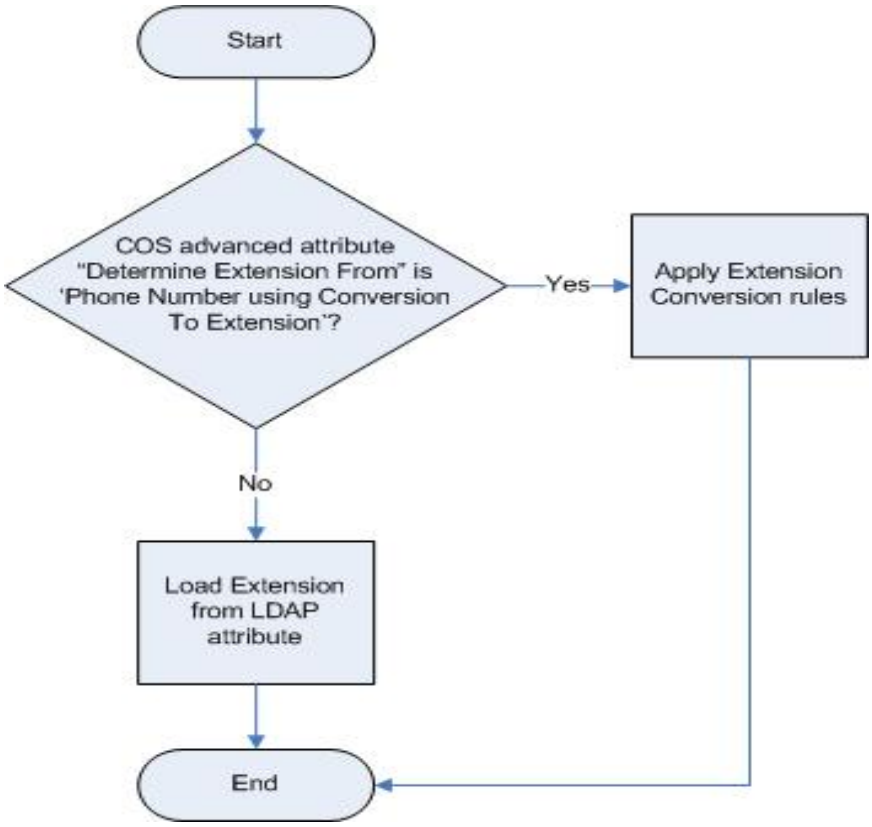
Important:
The values given in the various scenarios in this section are purely for demonstration purposes. Find out your site-specific requirements before you finalize the dial plan for your one-X Mobile implementation.

Extension Conversion

Scenario: Administrator provisions a user

The user is provisioned using a one-X Mobile Class of Service (COS). The COS profile configuration contains a link to a Communication Manager Profile. As part of the user provisioning activity, a user receives an extension on the associated Communication Manager. The user extension is loaded directly from the LDAP user configuration or can be computed using the user phone number as the input from the LDAP and the Extension Conversion dial plan associated with the Communication Manager.

one-X Mobile retrieves the user telephone number from the LDAP based on the COS and the LDAP profile configurations. If COS Advanced attribute “Determine Extension From” (see Admin UI COS configuration) is set to “Phone Number using Conversion to Extension” the dial plan rules associated with the Communication Manager are applied to the telephone number for converting it to an extension.



Requirements and assumptions

- Extensions must be unique across the whole enterprise.
- LDAP telephone numbers including the country code must follow the E.164 format.
- The Extension Conversion dial plan rule pattern does not contain the + character even if the number in the LDAP starts with a + because one-X Mobile strips the + before applying the dial plan.

Final destination number computation (callback)

one-X Mobile managed user initiates a Callback. The Callback Connect number is converted in order to be dialed out by the Communication Manager. All configurations involved in this scenario are related to the Communication Manager on which the user has the extension.

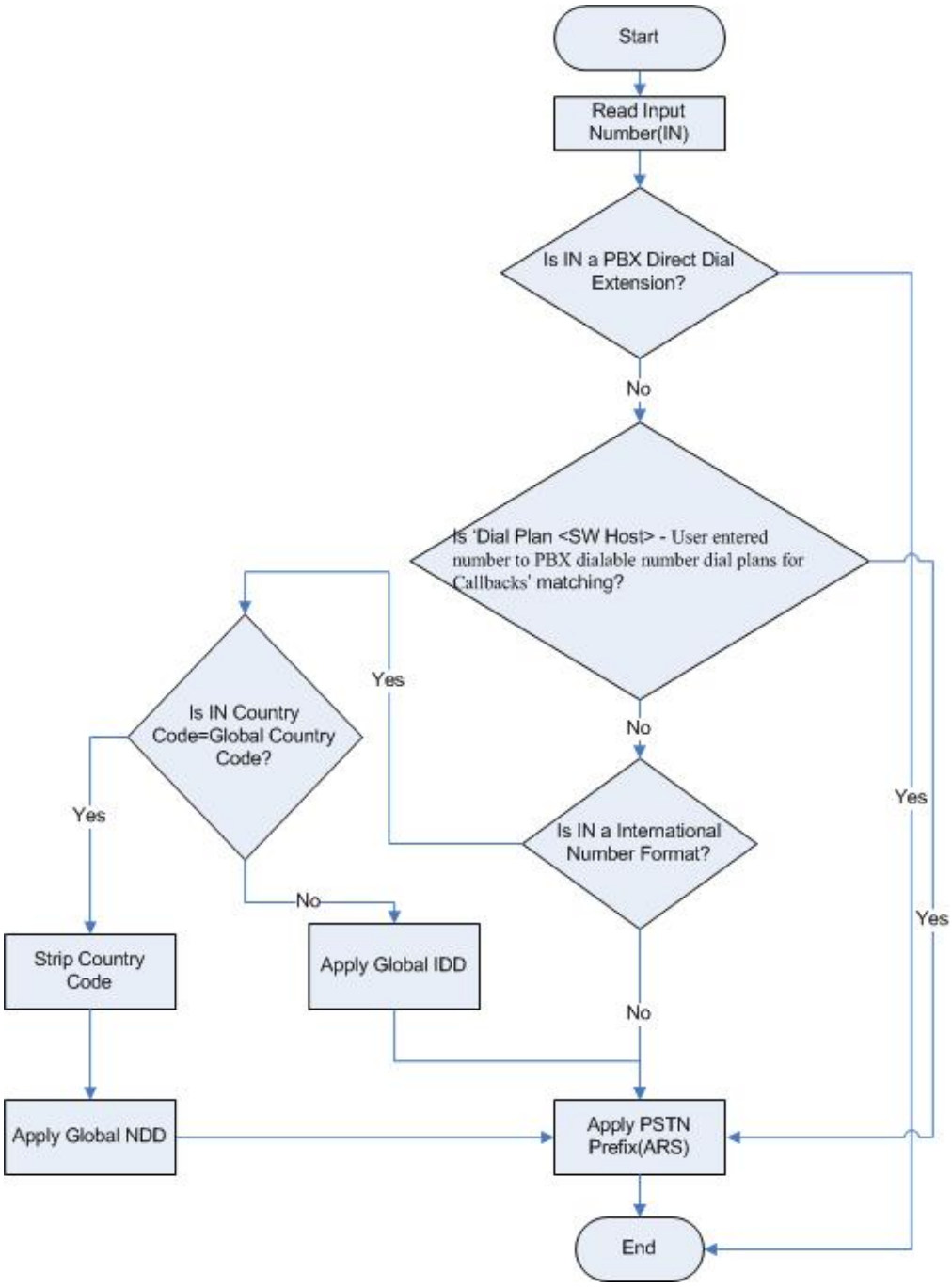
This is the sequence of dial plan rules that are applied for this case.

- The user entered number is checked to match a PBX Direct Dial Extension definition. A number is considered to be a PBX number if there is a matching Direct Call PBX rule or if there is a managed user with an extension on the same switch. In this case, the ARS prefix is not applied, no other transformation is applied. The result is returned to the calling service.
- In the case of “User entered number to PBX dialable number dial plan for Callbacks” the rule applies and the result is returned to the calling service.
- In case when the number has an international format and the country code is the same as the PBX Settings Country Code (see Admin, Dial Plan And Conversions Rules tab), the country code is replaced with the “PBX Settings National Direct Dialing Prefix”.
- In case the number has an international format and the country code is different from the PBX Settings Country Code, the PBX Settings IDD is applied.
- COS Dial Plan Settings “PSTN Prefix” (ARS) is applied.

Dial plan rules of a certain type are applied in the sequence as they have been defined. If no dial plan rule matches for a specific switch, a rule is searched in the default dial plan.

PSTN prefix (ARS) value is set in the COS associated with the managed user. If no ARS is required, this field can be blank.

Pattern matching does not contain the + character because one-X Mobile strips the + character before applying the dial plan rule even when the rule is intended for an international number transformation.


Start
Read Input Number(IN)
Is IN a PBX Direct Dial Extension?
No
Is 'Dial Plan <SW Host> - User entered number to PBX dialable number dial plans for Callbacks' matching?
Yes
No
Is IN Country Code=Global Country Code?
Yes
Is IN a International Number Format?
Yes
Yes
No
Strip Country Code
Apply Global IDD
No
Apply Global NDD
Apply PSTN Prefix(ARS)
End

Examples for Final destination number conversions (callback)

User entered phone number to PBX dialable number conversion rules are defined with examples in Table 1.

Note:
Ensure that you select the **User entered number to PBX dialable number for callbacks** option within the Dial Plan settings for your CLAN/Procr for callbacks for all the dial plan rules in table 1.

Global configurations

In these examples, the following global configurations are applied:

- Country Code = 1
- IDD = 011
- National Direct Dialing Prefix = 1
- National Number Length = 10

Note:
SW Host is the CLAN or PROCR IP address that you can find on the Dial Plan and Conversion Rules tab on the Admin UI.

Table 1: User entered phone number to PBX dialable number conversion rules

Examples	Input	Dial Plan Rules	Output
Example 1	User entered number = 408 5555555	User entered number to PBX dialable number dial plans for callback: Matching Pattern = ALL Number Length = 10 Strip digits = 0 Add Prefix = 1 User COS PSTN Prefix = 9	The converted PBX dialable number = 914085555555.
Example 2	User entered number = 408 5555555	User entered number to PBX dialable number dial plans for callback: Switch and Default dial plans have no rules. User COS PSTN Prefix = 9	No rule is found. PSTN prefix is applied. The converted PBX dialable number = 94085555555
Example 3	User entered number = +44 1234567890	User entered number to PBX dialable number dial plans for callback: Matching Pattern = ALL Number Length = 10 Strip digits = 0 Add Prefix = 1 User COS PSTN Prefix = 9	The user entered number has an international format. The Country Code of the user entered number and the Country Code configured in the **PBX Settings** section are different. For more information, see Global configurations on page 77. No dial plan rule is matched. The IDD is applied. PSTN prefix is also applied. The converted PBX dialable number = 901144123456789

Examples	Input	Dial Plan Rules	Output
Example 4	User entered number = +44 1234567890	User entered number to PBX dialable number dial plans for callback: Matching Pattern = ALL Number Length = 10 Strip digits = 0 Add Prefix = 1 Matching Pattern = 44 Number Length = 12 Strip digits = 2 Add Prefix = 01144 User COS PSTN Prefix = 9	The PSTN prefix is applied. Dial plan rule is applied. Please note, pattern matching should not contain the + character because one-X Mobile strips the + character before applying the dial plan rule. The converted PBX dialable number = 9011441234567890
Example 5	User entered number = 4877	User entered number to PBX dialable number dial plans for callback: Number Length = 10 Matching Pattern = ALL Strip digits = 0 Add Prefix = 1 PSTN Prefix = 9 Direct Call PBX Numbers: CLAN or PROCR IP address = 111.111.103.3 PBX Number/Numbers = 48xx	No other rule applies. This number pattern matches the a "Direct Call PBX Numbers" rule defined. The converted PBX dialable number = 4877
Example 6: Local Call	User entered number = 555 5555	User entered number to PBX dialable number dial plans for callback: Matching Pattern = ALL Number Length = 7 Strip digits = 0 Add Prefix = User COS PSTN Prefix = 9	The converted PBX dialable number = 9 555 5555.

Examples	Input	Dial Plan Rules	Output
Example 7: 10 digit local call	User entered number = 303 555 5555	User entered number to PBX dialable number dial plans for callback: Matching Pattern = 303 Number Length = 10 Strip digits = 0 Add Prefix = User COS PSTN Prefix = 9	The converted PBX dialable number = 9 408 555 5555.
Example 8: 11 digit long distance call	User entered number = 1 408 555 5555	User entered number to PBX dialable number dial plans for callback: Matching Pattern = 1 Number Length = 11 Strip digits = 0 Add Prefix = User COS PSTN Prefix = 9	The converted PBX dialable number = 9 1 408 555 5555.
Example 9: International Call, dialed as if from a land-line in home country	User entered number = 011 65 6666 6666	User entered number to PBX dialable number dial plans for callback: Matching Pattern = 011 Number Length = 13 (repeat for ranges 14-18) Strip digits = 0 Add Prefix = User COS PSTN Prefix = 9	The converted PBX dialable number = 9 011 65 6666 6666.
Example 10: International Call, 10 digit E.164 destination	User entered number = +65 6666 6666	User entered number to PBX dialable number dial plans for callback: Matching Pattern = ALL Number Length = 10 (repeat for ranges 11-15) Strip digits = 0 Add Prefix = 011 User COS PSTN Prefix = 9	The converted PBX dialable number = 9 011 65 6666 6666.

Examples	Input	Dial Plan Rules	Output
Example 11 : Call-back to local number	User entered number = 555 5555	The user entered number to a EC500 dialable number: Matching Pattern = ALL Number Length = 7 Strip digits = 0 Add Prefix =	The one-X off-PBX-telephone station mapping is converted to: 555 5555.
Example 12: Call-back to a local number, 10 digit format	User entered number = 303 555 5555	The user entered number to a PBX dialable number: Matching Pattern = 303 Number Length = 10 Strip digits = 0 Add Prefix =	The one-X off-PBX-telephone station mapping is converted: 303 555 5555.
Example 13: Call-back a local number, 11 digit long distance or E.164 format	User entered number = 1 408 555 5555	The user entered number to a PBX dialable number: Matching Pattern = 1 Number Length = 11 Strip digits = 0 Add Prefix =	The one-X off-PBX-telephone station mapping is converted: 1 408 555 5555.
Example 14: Call-back to an international number, entered as if dialing from a land line in home country	User entered number = 011 65 6666 6666	The user entered number to a PBX dialable number: Matching Pattern = 011 Number Length = 13 (repeat for ranges 14-18) Strip digits = 3 Add Prefix = 011--	The one-X off-PBX-telephone station mapping is converted: 65 6666 6666.
Example 15: Call-back to an international number, E.164 format	User entered number = +65 6666 6666	The user entered number to a PBX dialable number: Matching Pattern = ALL Number Length = 10 (repeat for lengths 10-15) Strip digits = 0 Add Prefix = 011--	The one-X off-PBX-telephone station mapping is converted: 65 6666 6666.

Examples	Input	Dial Plan Rules	Output
Example 16: Local Call	User entered number = 4444 4444	The user entered number to a PBX dialable number: Matching Pattern = ALL Number Length = 8 Strip digits = 0 Add Prefix = User COS PSTN Prefix = 0	The converted PBX dialable number = 0 4444 4444.
Example 17: Call to a local phone - 10 digit dialing	User entered number = 02 4444 4444	The user entered number to a PBX dialable number: Matching Pattern = 02 Number Length = 10 Strip digits = 2 Add Prefix = User COS PSTN Prefix = 0	The converted PBX dialable number = 0 4444 4444.
Example 18: Call to a mobile phone - E.164 dialing	User entered number = 61 2 4444 4444	The user entered number to a PBX dialable number: Matching Pattern = 612 Number Length = 11 Strip digits = 3 Add Prefix = User COS PSTN Prefix = 0	The converted PBX dialable number = 0 4444 4444.
Example 19: Call to a mobile phone - 10 digit dialing	User entered number = 04 3333 3333	The user entered number to a PBX dialable number: Matching Pattern = 0 Number Length = 10 Strip digits = 0 Add Prefix = User COS PSTN Prefix = 0	The converted PBX dialable number = 0 04 3333 3333
Example 20: Call to a mobile phone - E.164 dialing digit dialing	User entered number = +61 4 3333 3333	The user entered number to a PBX dialable number: Matching Pattern = 614 Number Length = 11 Strip digits = 2 Add Prefix = 0 User COS PSTN Prefix = 0	The converted PBX dialable number = 0 04 3333 3333

Examples	Input	Dial Plan Rules	Output
Example 21: call to a long distance number - 10 digit dialing	User entered number = 03 2222 2222	The user entered number to a PBX dialable number: Matching Pattern = 0 Number Length = 10 Strip digits = 0 Add Prefix = User COS PSTN Prefix = 0	The converted PBX dialable number = 0 03 2222 2222
Example 22: call to a Long Distance Number - E.164 dialing digit dialing	User entered number = +61 3 2222 2222	The user entered number to a PBX dialable number: Matching Pattern = 61 Number Length = 11 Strip digits = 2 Add Prefix = 0 User COS PSTN Prefix = 0	The converted PBX dialable number = 0 03 2222 2222
Example 23: International Call, dialed as if from a land line	User entered number = 0011 65 6666 6666	The user entered number to a PBX dialable number: Matching Pattern = 0011 Number Length = 14 (repeat for ranges 15-19) Strip digits = 0 Add Prefix = PSTN Prefix = 0	The converted PBX dialable number = 0 0011 65 6666 6666.
Example 24: International Call, 10 digit E.164 destination	User entered number = +65 6666 6666	The user entered number to a PBX dialable number: Matching Pattern = ALL Number Length = 10 (repeat for lengths 11-15) Strip digits = 0 Add Prefix = 0011 PSTN Prefix = 0	The converted PBX dialable number = 0 0011 65 6666 6666.
Example 25: Local Call-back number	Users call-back number = 4444 4444	The user entered number to a EC500 dialable number: Matching Pattern = ALL Number Length = 8 Strip digits = 0 Add Prefix =	The converted PBX dialable number = 4444 4444.

Examples	Input	Dial Plan Rules	Output
Example 26: Call-back to a local phone - 10 digit format	Users call-back number = 02 4444 4444	The user entered number to a PBX dialable number: Matching Pattern = 02 Number Length = 10 Strip digits = 2 Add Prefix =	The converted PBX dialable number = 4444 4444.
Example 27: Call-back to a mobile phone - E.164 format	Users call-back number = 61 2 4444 4444	The user entered number to a PBX dialable number: Matching Pattern = 612 Number Length = 11 Strip digits = 3 Add Prefix =	The converted PBX dialable number = 4444 4444.
Example 28: Call-back to a mobile phone - 10 digit format	Users call-back number = 04 3333 3333	The user entered number to a PBX dialable number: Matching Pattern = 0 Number Length = 10 Strip digits = 0 Add Prefix =	The converted PBX dialable number = 04 3333 3333.
Example 29: Call-back to a mobile phone - E.164 format	Users call-back number = +61 4 3333 3333	The user entered number to a PBX dialable number: Matching Pattern = 612 Number Length = 11 Strip digits = 2 Add Prefix = 0	The converted PBX dialable number = 04 3333 3333.
Example 30: Call-back to a long distance number - 10 format	Users call-back number = 03 2222 2222	The user entered number to a PBX dialable number: Matching Pattern = 0 Number Length = 10 Strip digits = 0 Add Prefix =	The converted PBX dialable number = 04 2222 2222.
Example 31: Call-back to a Long Distance Number - E.164 format	Users call-back number = +61 3 2222 2222	The user entered number to a PBX dialable number: Matching Pattern = 61 Number Length = 11 Strip digits = 2 Add Prefix = 0	The converted PBX dialable number = 03 2222 2222.

Examples	Input	Dial Plan Rules	Output
Example 32: Call-back to an international number, as if dialed from a land line in home country	Users call-back number = 0011 65 6666 6666.	The user entered number to a PBX dialable number: Matching Pattern = 0011 Number Length = 14 (repeat for lengths 15-19) Strip digits = 4 Add Prefix = 0011--	The converted PBX dialable number = 65 6666 6666.
Example 33: Call-back to an international number, E.164 format	Users call-back number = +65 6666 6666.	The user entered number to a PBX dialable number: Matching Pattern = ALL Number Length = 10 (repeat for lengths 11-15) Strip digits = 0 Add Prefix = 0011--	The converted PBX dialable number = 65 6666 6666.

Note:

If a user receives a voicemail from an international number, the new and saved voicemail inboxes will display caller's number in this format **<Country Code><Area/City Code><Phone Number>**. To make a call back to the caller's number by using one-X Mobile, add the appropriate Dial Plan as described in Table 1: User entered phone number to PBX dialable number conversion rules. Dial Plans for all the known international numbers should be added on the one-X Mobile administration Web site.

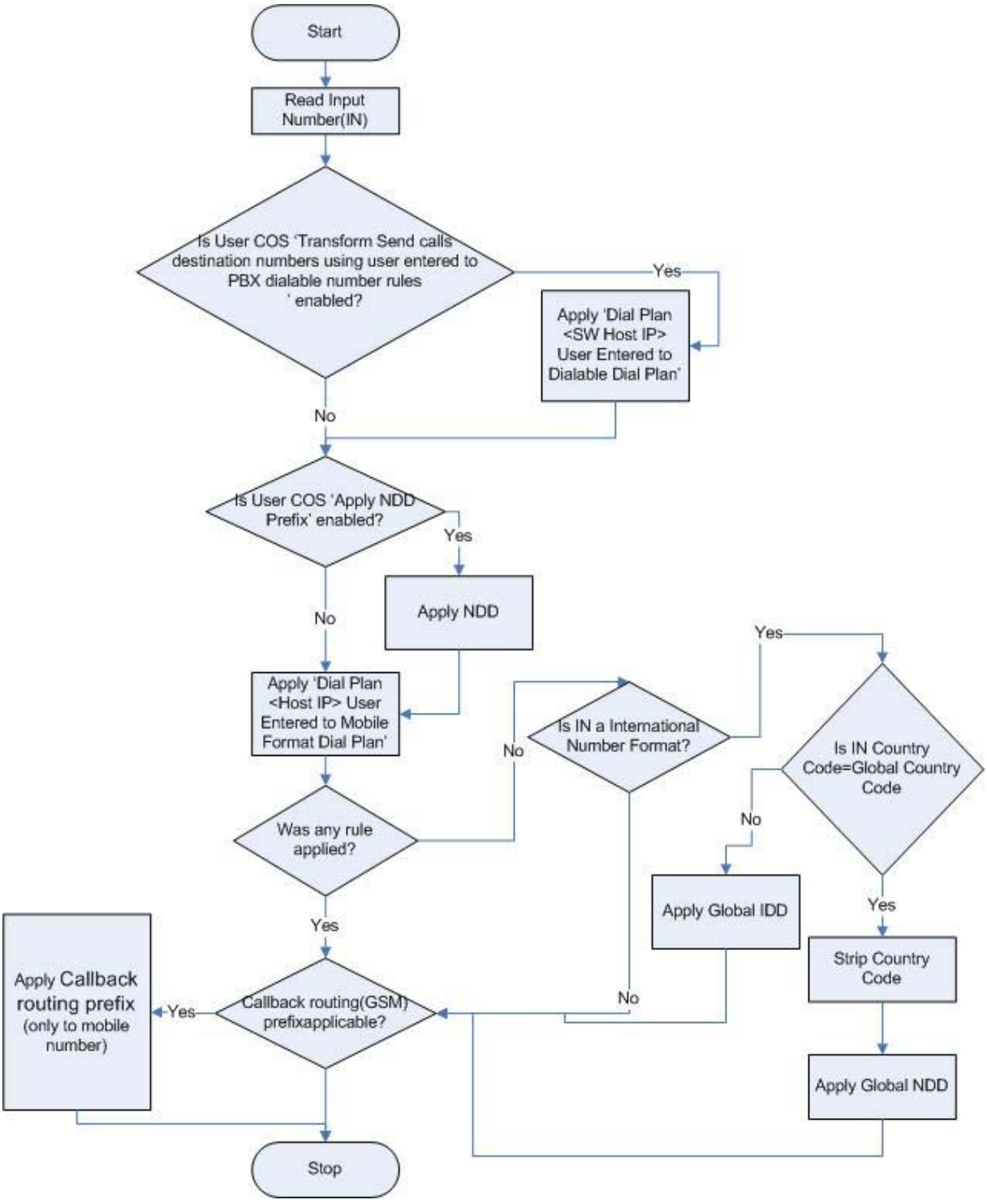
Mobile numbers and quick entries conversions for callback

Conversion rules are also applied to the mobile and quick entries numbers.

When the user initiates a callback, the "Send to calls" number is transformed.

The two COS attributes enable the application of dial plan rules for off-PBX (mobile and quick entry) numbers:

- Transform Send calls destination numbers using user entered to PBX dialable number rules
- Apply National Direct Dialing Prefix to send calls destination numbers


Start
Read Input Number(IN)
Is User COS 'Transform Send calls destination numbers using user entered to PBX dialable number rules ' enabled?
Yes
Apply 'Dial Plan <SW Host IP> User Entered to Dialable Dial Plan'
No
Is User COS 'Apply NDD Prefix' enabled?
Yes
Apply NDD
No
Apply 'Dial Plan <Host IP> User Entered to Mobile Format Dial Plan'
Was any rule applied?
No
Is IN a International Number Format?
Yes
Is IN Country Code=Global Country Code
No
Apply Global IDD
Yes
Strip Country Code
Apply Global NDD
Yes
Apply Callback routing prefix (only to mobile number)
Yes
Callback routing(GSM) prefixapplicable?
No
Stop

When the user initiates a callback, the "Send to calls" number is transformed as described in Table 2.

Examples for mobile numbers and quick entries conversions

The examples for user entered number to mobile (EC500) format conversion are discussed in Table 2.

Note:

Do not select these two COS attributes for callbacks for all the examples listed in table 2.

For example, the **User entered number to mobile (EC500) format** option is selected for all the dial plan rules in table 2.

Table 2: User entered number to mobile (EC500) format conversion rules

Examples	Input	Dial Plan Rules	Output
Example 1	User entered number = 4085555555	User entered number to the mobile (EC500) format dial plans for callback: Min Length = 10 Max Length = 10 Pattern = 408 Strip digits = 3 Prefix = 1-408	The converted mobile (EC500) format = 1-4085555555
Example 2	User entered number = 408 5555555	User entered number to the mobile (EC500) format dial plans for callback: Min Length = 10 Max Length = 10 Pattern = 408 Strip digits = 3 Prefix = 1-408	No rule is applied. The converted mobile (EC500) format = 14085555555

Examples	Input	Dial Plan Rules	Output
Example 3	User entered number = 441234567890	User entered number to the mobile (EC500) format dial plans for callback: Min Length = 12 Max Length = 12 Pattern = 44 Strip digits = 2 Prefix = 011-44	The converted mobile (EC500) format = 011-44-1234567890 The dashes in the converted mobile EC500 format represent the separation of the Off-PBX Dial Prefix, Country Code, and Phone Number. Therefore, up to 15 numbers are allowed for the Off-PBX Phone Number.
Example 4	User entered number = +441234567890	User entered number to the mobile (EC500) format dial plans for callback: The configurations are applied from the Global configurations on page 77.	The converted mobile (EC500) format = 011441234567890

Examples for user entered to mobile dial plan rules conversions

The user entered number to mobile (EC500) format conversion rules are defined with examples in Table 3.

The user entered number conversion is based on the dial plan defined in the **User entered number to mobile (EC500) format** section and the COS attributes.

Table 3: Phone number to mobile (EC500) format conversion rules

Examples	Input	Dial Plan Rules	Output
Example 1	User entered number = 408 555 5555	User entered number to the mobile (EC500) format dial plans for callback: Number Length = 11 Matching Pattern = 1	The NDD is applied. In this example, **Apply National Direct Dialing Prefix to send calls destination numbers** (COS attribute) is selected. The converted mobile (EC500) format = 14085555555 You can use the same rule when you select the **Transform Send calls destination numbers using user entered to PBX dialable number rules** option.

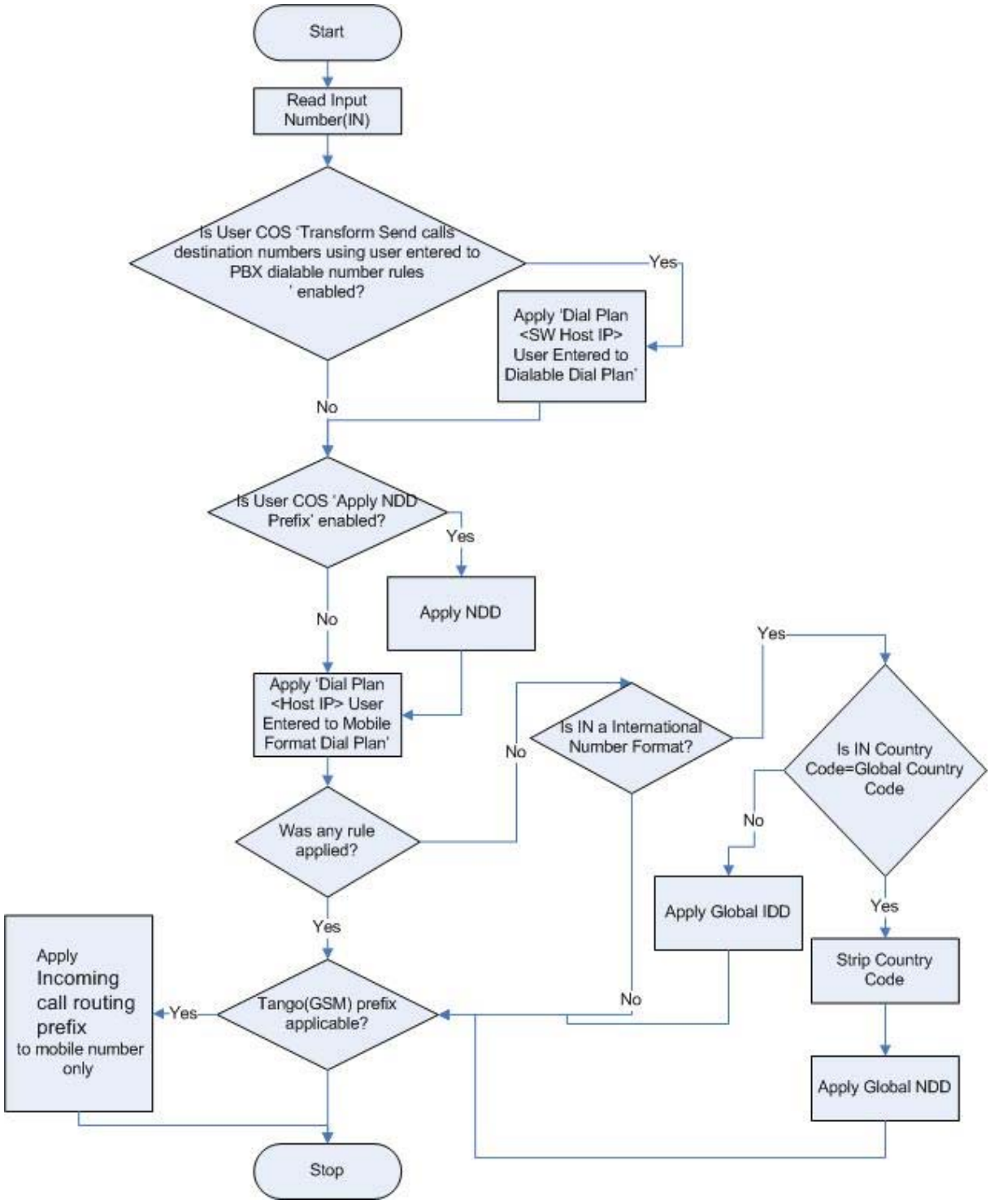
Note:

You can select both options (**Transform Send calls destination numbers using user entered to PBX dialable number rules** and **Apply National Direct Dialing Prefix to send calls destination numbers**) at the same time.

Mobile numbers and quick entries conversions on incoming call

The Tango prefix (or Incoming Call Routing Prefix) is an administrative setting. Tango prefix applies only to mobile numbers and managed user configuration is not required.

In this flow chart, mobile numbers and quick entries conversions on incoming call are described.



Example for applying the Tango (Incoming Call Routing) prefix

The user entered number to mobile (EC500) format conversion rules for Tango prefix (or Incoming Call Routing Prefix) are defined with examples in Table 4.

Table 4: Phone number to mobile (EC500) format conversion rules for Tango prefix (or Incoming Call Routing Prefix)

Examples	Input	Dial Plan Rules	Output
Example 1	User entered number = 1 425 555 5555	User entered number to the mobile (EC500) format dial plans for Tango prefix (or Incoming Call Routing Prefix): **Number Pattern**: Min Length = 12 Max Length = 12 Matching Pattern = 91 Strip digits = 2 Add Prefix = 011-91- CM Profile, Incoming Call Routing Prefix= 6 **Dial Plan settings**: In this example, **Transform Send Calls destination numbers using user entered to PBX dialable number rules** option (User COS Dial Plan Settings) is not selected. In this example, **Apply National Direct Dialing Prefix to send calls destination numbers** option (User COS Dial Plan Settings) is not selected.	The converted mobile (EC500) format = In this example, the user entered number does not match the Dial Plan rule. The Incoming Call Routing Prefix (Communication Manager Profile) is applied. Converted number is: 614255555555

GSM Prefixes (Tango Prefix for incoming calls and LCR Prefix for callback)

These prefixes are applied only to the off-net number numbers. The corresponding prefixes should be configured in Communication Manager to affect routing to a specific trunk. On the other end of the trunk, there is either a tango server or a GSM gateway.

The transformations applied to mobile and quick entry numbers for callback-with and simulring are similar. The difference is in the type and value of the GSM prefix that is applied.

Caller ID related transformations

If available, external number rules are applied to obtain and display a full E-164 number. This does not affect the number to be dialed. This affects the display of the call history number for both callback and incoming calls.

Appendix C: Acceptance Testing

This appendix provides the procedure for performing acceptance testing. Acceptance testing of the one-X Mobile server is performed after configuration or after upgrading the one-X Mobile server.

To confirm that the one-X Mobile server installation or upgrade is successful and Avaya one-X Mobile is working properly, ensure the following:

- Validate that you can access the admin and end user one-X Mobile Web client
- From the one-X Mobile end user Web Client
  - configure Send Calls to the Desk Phone and Mobile Phone and check that inbound calls are routed to these endpoints
  - verify that the one-X Mobile client displays the call in the Call log
  - send a voicemail and check that the one-X Mobile displays voicemail in Saved Voicemail and you can retrieve the voicemail
  - check that you can search contacts in the Corporate Directory
  - verify that you have the Carrier, Mobile Phone Model, and Mobile Phone Manufacturer listed in the Manage Mobile tab of the one-X mobile Web client
  - verify that the one-X Mobile update completes successfully when you click Update Avaya one-X Mobile
  - verify that you receive an SMS on your mobile device with the URL to download the one-X Mobile client
  - verify that calls from the one-X Mobile Web client and one-X Mobile client exists in the call logs
  - verify that call back works by using quick entry in the one-X Mobile Web client and one-X Mobile client
  - verify that you are able to dial 'direct dial' PBX extension ranges within your PBX dial plan

Using a mobile device check that:

- You are able to route inbound calls to appropriate endpoints
- one-X Mobile client displays a new voicemail message on the mobile device and you are able to save and delete voicemails
- one-X Mobile client displays contact entries in the Corporate Directory under the Corporate Directory menu on the mobile device
- You are able to make a callback to a calling number by using the:

- voicemail inbox
- corporate directory
- callback screen

Appendix D: Enhanced scalability by Tomcat tuning

To support 1500 one-X Mobile users, configure Tomcat with the following changes:

Reduce the logging

Logging can be reduced by removing the duplicate logging handler from the Tomcat logging.properties file. This file is available in <1XM Install Drive>\Edge\Utilities\apache-tomcat-5.5.23\conf\.

Change the line from:

handlers = 1catalina.org.apache.juli.FileHandler, java.util.logging.ConsoleHandler

Change the line to:

handlers = 1catalina.org.apache.juli.FileHandler

Optimize Java

Run the tomcat5w.exe located in <1XM Install Drive>\Edge\Utilities\apache-tomcat-5.5.23\bin.

In the Apache Tomcat Properties window, change the values of Java tab to:

1. In the **Java Virtual Machine** field, enter **C:\Program Files\Java\jdk1.5.0_10\jre\bin\server\jvm.dll**.
2. In the **Java Options** field, enter **Djava.io.tmpdir=C:\Edge\Utilities\apache-tomcat-5.5.23\temp-XX:NewRatio=2**.
3. In the **Initial memory pool** field, enter *128*.
4. In the **Maximum memory pool** field, enter *256*.
5. In the **Thread stack size** field, enter *64*.
6. Click **OK**.

Optimize the Tomcat server

You can optimize the Tomcat server by changing server.xml file in **1XM Install Drive>\Edge\ Utilities\apache-tomcat-5.5.23\conf**. Make the following changes in the server.xml file:

Change configuration from	Change configuration to
<Connector acceptCount="100" connectionTimeout="20000" disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="8080" redirectPort="8443" URIEncoding="UTF-8" />	**<Connector acceptCount="300" compression="4096" connectionTimeout="3" disableUploadTimeout="true "enableLookups="false" maxHttpHeaderSize="8192" maxKeepAliveRequests="1" maxSpareThreads="50" maxThreads="400" minSpareThreads="50" socketBuffer="65536" port="8080" redirectPort="8443" URIEncoding="UTF-8"/>**
<Connector acceptCount="100" clientAuth="false" disableUploadTimeout="true" enableLookups="false" keystoreFile="./webapps/WebLM/ WEB-INF/weblmserver.p12" keystorePass="password" keystoreType="PKCS12" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="8443" scheme="https" secure="true" sslProtocol="TLS" URIEncoding="UTF-8"/>	**<Connector acceptCount="100" clientAuth="false" disableUploadTimeout="true" enableLookups="false" keystoreFile="./webapps/ WebLM/WEB-INF/ weblmserver.p12" keystorePass="password" keystoreType="PKCS12" maxHttpHeaderSize="8192" maxSpareThreads="25" maxThreads="150" minSpareThreads="10" port="8443" scheme="https" secure="true" sslProtocol="TLS" URIEncoding="UTF-8"/>**