



Administering ACCCM for Avaya one-X® Agent Central Management

**Release 7.0 SP1
Issue 1.1
November 2013**

© 2013 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-

alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

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.

Third-party components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: <http://support.avaya.com/Copyright>. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, one-X are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Européenne) mark conforms to the European Union Radio.

Contents

Chapter 1: Introduction.....	6
ACCCM overview	6
Key features	6
Architecture overview	7
Architecture diagram	7
Deployment options	8
All-in-one server deployment	8
Remote SQL server deployment.....	8
Multi server deployment.....	9
Chapter 2: Installing Avaya one-X® Central Management in ACCCM	10
Installing Avaya one-X® Central Management on a single server	10
Installing Central Management in the distributed environment	14
Chapter 3: Using the Avaya one-X® CAM administration portal	18
Avaya one-X® Central Management URL	18
Logging on to Avaya one-X® Central Management	18
Logging out of Avaya one-X® Central Management	19
Planning a client configuration in Avaya one-X® Central Management	20
Chapter 4: Administering users	22
Importing users into Avaya one-X® Central Management	22
Adding users in Avaya one-X® Central Management	24
Deleting users	30
Filtering users.....	31
Activating or deactivating a user.....	32
Editing user details	32
Chapter 5: User groups in Avaya one-X® Central Management	35
Group assignment logic	35
Importing user groups into Avaya one-X® Central Management	36
Creating user groups.....	37
Editing user groups	39
Filtering groups.....	41
Deleting groups	41
Removing users from a group.....	42
Chapter 6: Managing the location data	43
Importing the location data.....	43

Editing the location data.....	44
Deleting the location data.....	45
Chapter 7: Managing Avaya one-X® Central Management templates	47
Creating templates	48
Finding templates	49
Editing templates	50
Deleting templates.....	50
Configuring the Telephony Login settings.....	51
Configuring Alternate Server Addresses.....	51
Configuring the Agent Login settings	52
Configuring the IM Login settings.....	52
Viewing Phone Numbers.....	53
Configuring the Work Handling settings.....	53
Configuring the Audio Greetings settings	54
Configuring the Screen Pop settings	54
Configuring the Launch Application settings	55
Configuring the Directory settings	56
Configuring the Work Log settings	57
Configuring the Voice Mail Integration settings.....	57
Configuring the Reason Code settings	58
Importing Codes.....	59
Configuring the Event Logging settings	59
Configuring the Outlook Contacts settings.....	60
Configuring the Dialing Rules settings	61
Configuring the Touch Tone Shortcuts settings.....	62
Configuring the Video - Basic settings	63
Configuring the Video - Advanced settings.....	64
Configuring the IM settings	64
Configuring the IM Responses settings	65
Configuring the TTY - General settings.....	66
Configuring the TTY- Abbreviations settings	66
Configuring the Call Handling settings	67
Configuring the User Interface settings.....	68
Chapter 8: Managing contacts	69
Importing multiple contacts	69
Adding a contact list	72
Adding members to contact list	72
Editing contact list member details.....	73

Deleting contact list members	73
Attaching contact list to templates.....	74
Filtering and sorting the contact list table.....	75
Detaching a contact list from a template	75
Chapter 9: Authentication modes and LDAP integration	77
Standard Authentication	77
LDAP Root	79
LDAP Credentials – Mixed Authentication	82
Chapter 10: Installing multiple configuration services	85
Chapter 11: Integrating the Avaya one-X® Central Management portal with ACCCM	90
Integrating Avaya one-X® Central Management with ACCCM	90
Managing agents and users from ACCCM	91
Creating agents from ACCCM	92
Creating users in Central Management from ACCCM.....	93
Managing permissions from ACCCM	93

Chapter 1: Introduction

This chapter covers:

- [ACCCM overview on page 6](#)
- [Key features on page 6](#)
- [Architecture overview on page 7](#)
- [Deployment options on page 8](#)

ACCCM overview

The Avaya Contact Center Control Manager (ACCCM) system is a centralized operational administration solution that provides a comprehensive solution for administrators to support day-to-day operations. ACCCM complements the entire Avaya Contact Center suite by combining and integrating key management and administration tasks of a wide range of contact center entities.

With the ACCCM system, administrators can unify, streamline, and centralize the management of Avaya Aura® Contact Center (AACC) operations. In addition, the administrator can track events and take necessary action to meet customer needs. The ACCCM system is for Avaya customers using different Avaya Contact Center Business Unit (CCBU) products and solutions. The ACCCM system integrates with a Unified Communication infrastructure based on Avaya Aura® Communication Manager (CM) and Avaya Aura® Session Manager. ACCCM integrates with and supports operational administration of Avaya Contact Center suite, including the following:

- Avaya Modular Messaging (MM)
- Avaya AUDIX Messaging
- Avaya Call Management System (CMS)
- Avaya IQ (IQ)
- Avaya Aura® Call Center Elite Multichannel (EMC)
- Avaya Interaction Center (IC)
- Avaya Voice Portal (AVP)
- Avaya Aura® Experience Portal (AAEP)
- Avaya Proactive Contact (PC)
- Avaya Proactive Outreach Manager (POM)
- Avaya Aura® System Manager
- Avaya Aura® Messaging
- Avaya Aura® Session Manager
- Avaya Aura® Application Enablement Services
- Avaya one-X® Agent (one-X Agent)
- Avaya Aura® Workforce Management
- Avaya Aura® Contact Center (AACC) with Elite customers who are interested using a blended environment (Voice on Elite with Multimedia on AACC)
- Non-Avaya third-party Workforce Optimization (WFO) solution

Key features

- Centralized management and administration of all contact center applications.

- Personalized thin client application interface.
- Real-time monitoring and historical analysis of agents, skills, Vector Directory Numbers (VDNs), campaigns, and other business data.
- Visual call flow design and vector management.
- Role-based permissions and multi tenancy support.
- Full Microsoft Active Directory integration with single sign-on (SSO) functionality.

Architecture overview

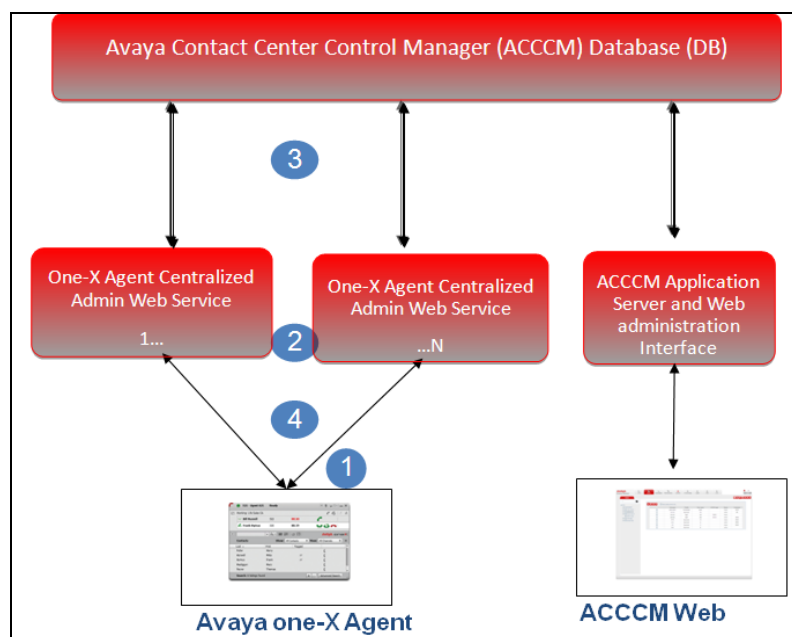
The Avaya one-X® Central Management feature is part of ACCCM and includes the following three components:

Component	Description
Central Management Database	A database that stores the configuration of Avaya one-X® Agent clients.
Configuration Service	A Web service that communicates with Avaya one-X® Agent clients for authentication and retrieving and storing client data.
Administration Portal	A Web portal for administrators to manage the Avaya one-X® Agent client profiles and other administrative parameters.

You can install the components on a single server or distribute the components across servers in your environment. For more information on deployment options, see [Deployment options on page 8](#).

Architecture diagram

The following diagram illustrates the ACCCM-one-X® Agent CAM architecture:



1. The Avaya one-X® Agent client sends an HTTP or HTTPS request to the centralized admin Web service layer. You can distribute the Web services across the 1-N servers.

2. Each Web service request reaches the ACCCM database with the user credentials.
3. The Database layer retrieves the entire configuration of the required agent.
4. Avaya one-X® Agent receives the configuration data as an XML file that the application layer generates.

Deployment options

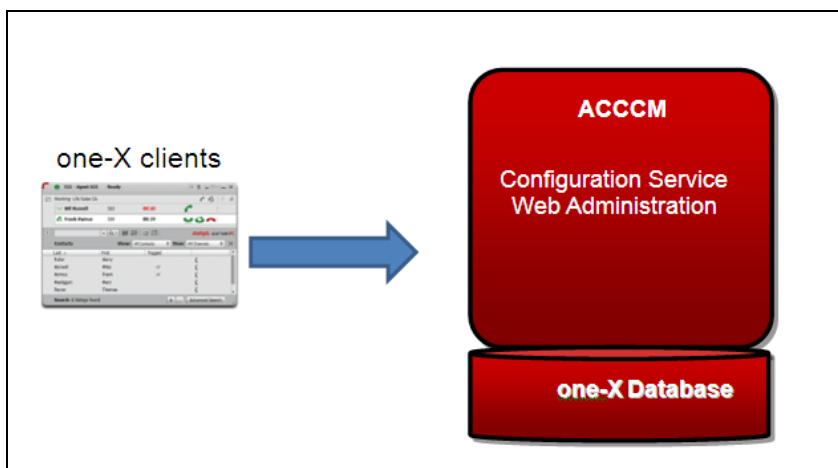
You can deploy Avaya one-X® Central Management in several architectures.

The following are the available deployment options:

- [All-in-one server deployment on page 8](#)
- [Remote SQL server deployment on page 8](#)
- [Multi server deployment on page 9](#)

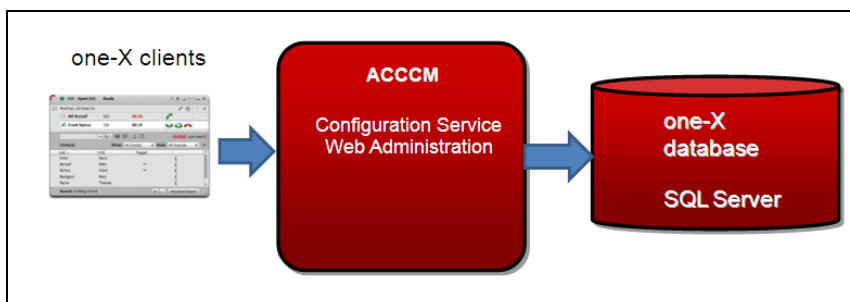
All-in-one server deployment

With the all-in-one server deployment, you can deploy all Avaya one-X components on a single server. A single server can also deploy all ACCCM components.



Remote SQL server deployment

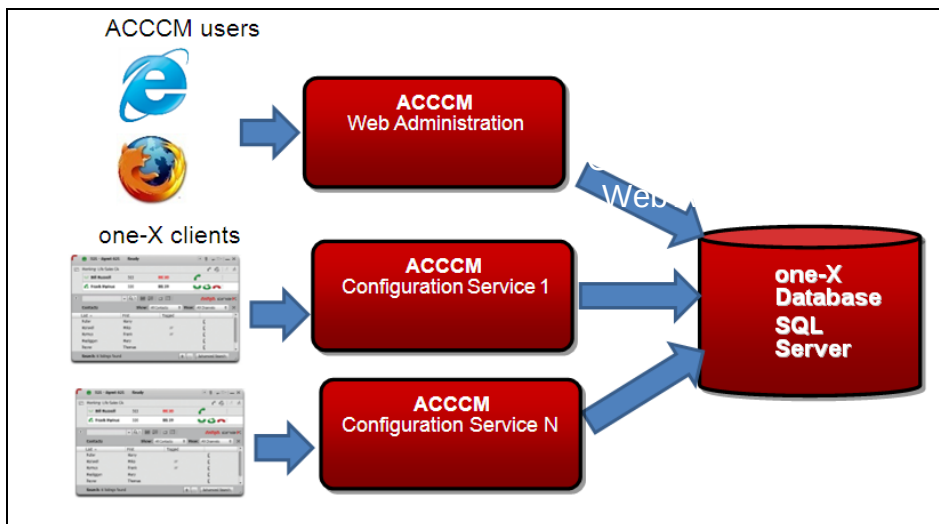
With the remote SQL server deployment, you can deploy the Avaya one-X Configuration Service and Web Administration on a single server. You can also deploy all ACCCM components using the remote SQL server. A remote SQL Server stores the Avaya one-X® Agent database.



Multi server deployment

With the multi server deployment, you can deploy as many Avaya one-X® Agent Configuration Services as you want. A central database server hosts the AVAYA ONE-X® CENTRAL MANAGEMENT database. You can also install multiple servers that host the Web administration interface.

Use the multi server deployment option for High Availability (HA) that is required for the Avaya one-X® Central Management features.



Chapter 2: Installing Avaya one-X® Central Management in ACCCM

This chapter includes:

- [Installing Avaya one-X® Central Management on a single server on page 10](#)
- [Installing Central Management in the distributed environment on page 14](#)

Installing Avaya one-X® Central Management on a single server

You can install the following components as part of the Avaya one-X® Central Management installation process:

Component	Description
one-X Database	one-X Database is different from the ACCCM database. You can use the one-X Database only for Avaya one-X® Agent configuration and authentication of the Avaya one-X® Agent clients.
one-X Administration website	Administrators can use this website to manage the Avaya one-x Agent client profiles, templates, and other configurations related to Avaya one-X® Agent clients. The website name is ACCCMONEX .
one-X Configuration Services	This Web service is installed as a website on the Microsoft Internet Information Services (IIS) Web server. Avaya one-X® Agent clients use the one-X Configuration Services to authenticate user credentials, retrieve client configuration, and store contact history. The Web service the name is ACCCMONEXCFG. In case of SSO, the name is ACCCMONEXSSO.

Prerequisites

- .NET Framework 4.0
- Microsoft MVC

Perform the following steps to complete the installation procedures for installing Avaya one-X® Central Management in the ACCCM system on a single server.

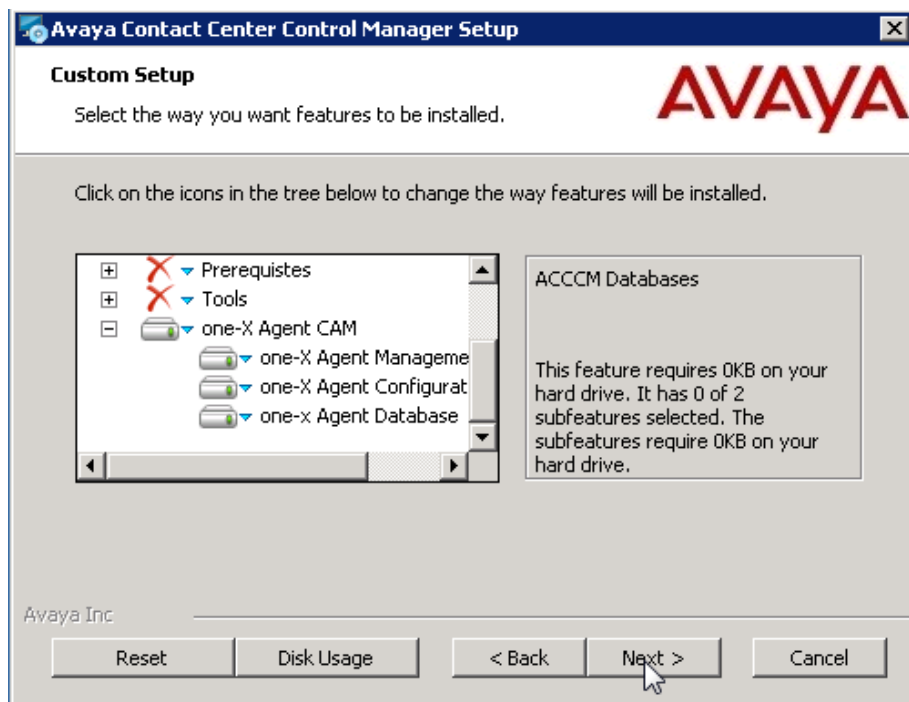


1. To open the ACCCM installation wizard, click the ACCCM installation wizard.
The system displays the following screen:



2. Click **Next**.

The system displays the following screen:



3. In the Custom Setup wizard, select the required CAM components and click **Next**.

The system displays the following screen:

Avaya Contact Center Control Manager Setup

SQL Database

Configure SQL Connection to your SQL Server

AVAYA

Server: accm61qa1

Port: 1433

Username: sa

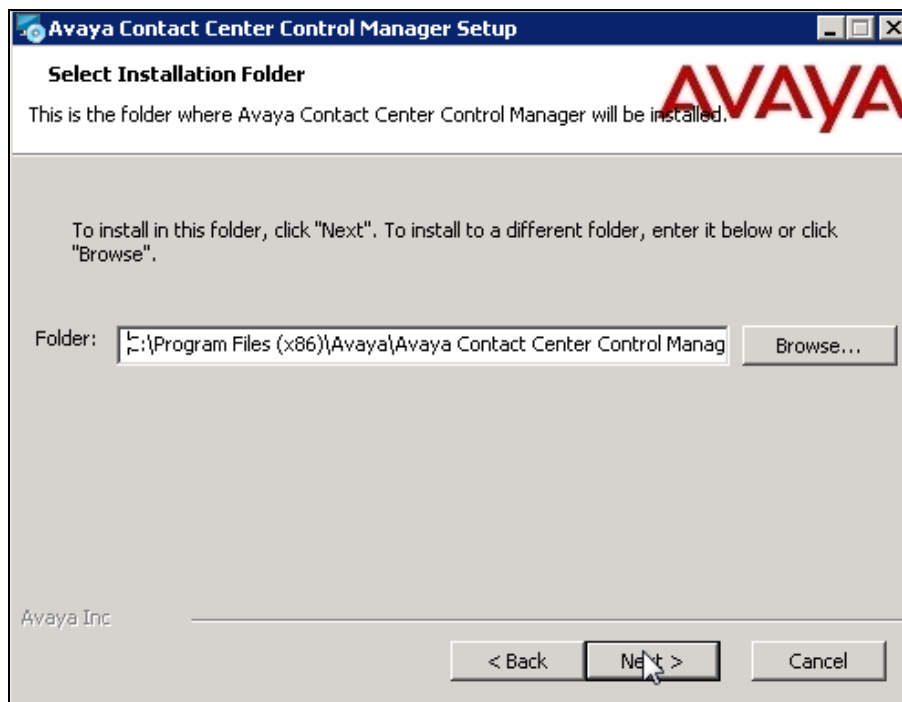
Password: ••••••••

ACCCM DB: acccmayp

Avaya Inc

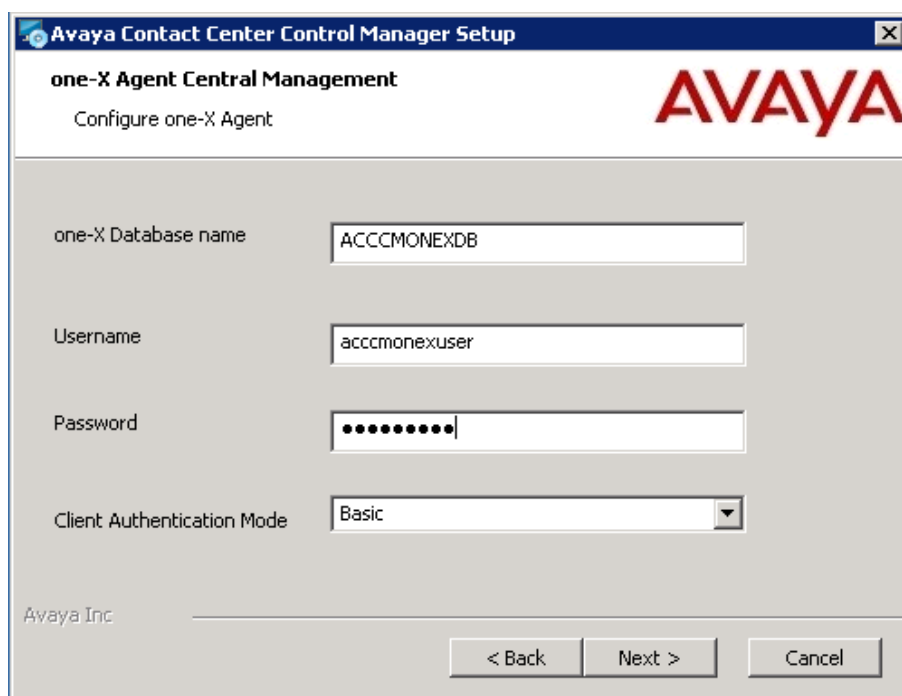
< Back Next > Cancel

4. In the SQL Database window, perform the following steps:
 - a. In the **Server** field, enter the host name or the IP address of the server that hosts the SQL server.
 By default, the system uses the host ACCCM server address. If you are using a database instance, enter the instance name. For example, enter the database name as **accmServer\sqlinstance**.
NOTE: The ACCCM default SQL Server installation does not install a special instance. You must enter the server name or the IP address.
 - b. In the **Port** field, enter the port number of the SQL server.
 The SQL server uses **1433** as the default port.
 - c. In the **Username** field, enter the database user name that you use for connecting to the SQL server.
 You must use **SA** as the user name. If you do not have the SA user, you must use a user that has DBO access rights on the master database.
 - d. In the **Password** field, enter the password of the user.
 - e. In the **ACCCM DB** field, enter the name of the ACCCM database.
5. Click **Next**.
 The system displays the following screen:



6. Click **Browse** to navigate to the location where you want to install the one-X Agent Central Management components, and click **Next**.

The system displays the following screen:



7. In the one-X Agent Central Management window, perform the following steps:
 - a. In the **one-X Database name** field, enter the name of the Avaya one-X® Central Management database.
By default, the database name is **ACCCMONEXDB**.
 - b. In the **Username** field, enter the name of the Avaya one-X® Central Management database user.
By default, the user name is **acccmonexuser**.

- c. In the **Password** field, enter the password of the database user.
- d. From the **Client Authentication Mode** drop-down list, choose the authentication type.

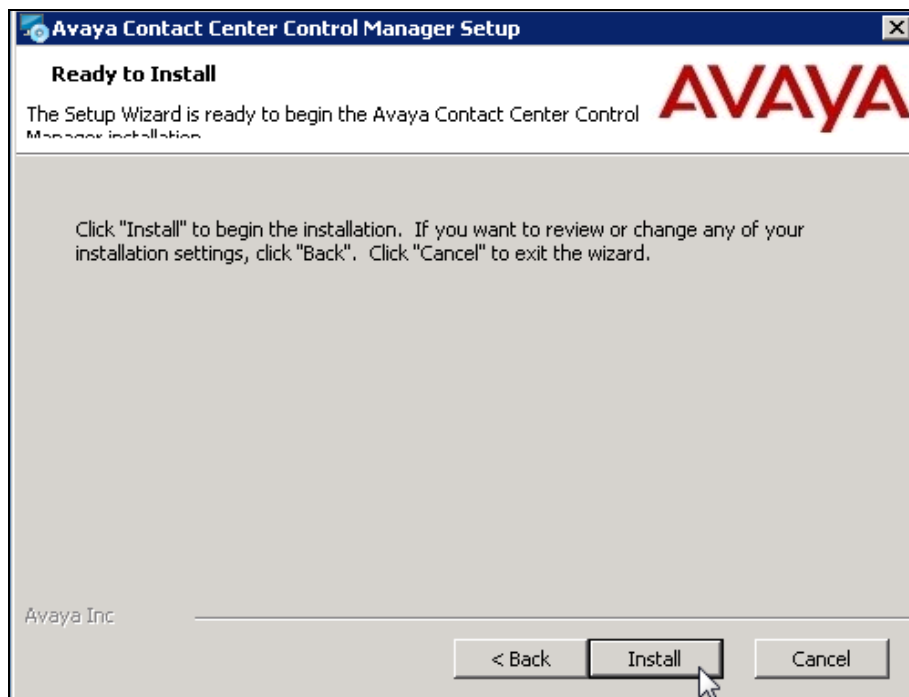
The authentication type corresponds to the type of authentication the Avaya one-X® Agent clients use. The following authentication options are available:

- **Basic:** Uses the user name and password to authenticate the one-X Agent database.
 - **SSO:** The SSO authentication validates the user with the active directory.
- e. From the **Version** drop-down list, choose the appropriate version of Avaya one-X® Agent.

The available options are 2.0 and 2.5.

8. Click **Next**.

The system displays the following screen:



9. Click **Install** to complete the installation.



Installing Central Management in the distributed environment

To distribute the Avaya one-X® Agent components across several servers, you can install the components separately.



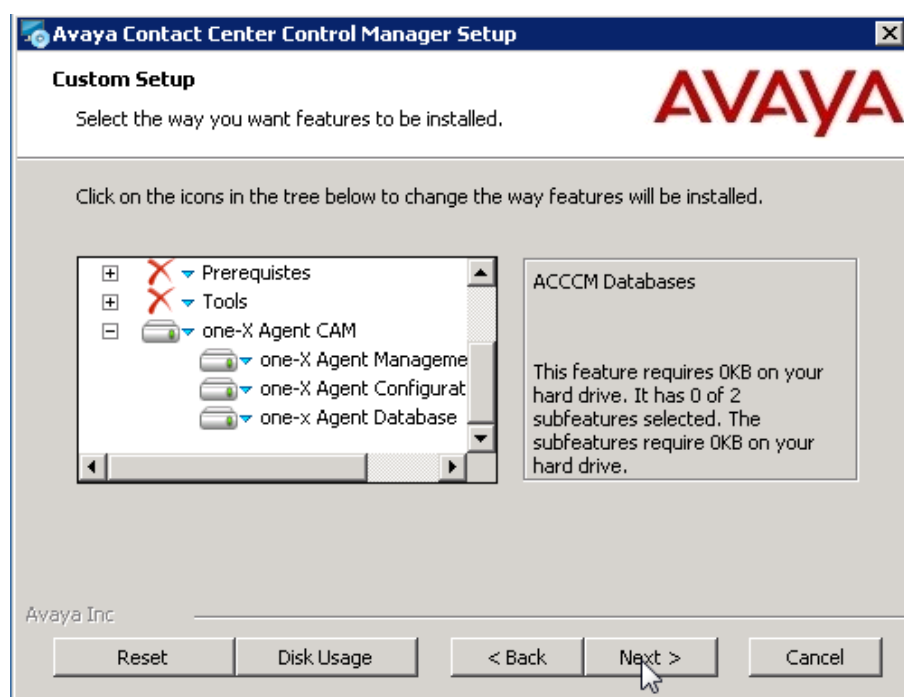
1. Open the ACCCM installation wizard.

The system displays the following screen:



2. Click **Next**.

The system displays the following screen:



If the one-X Agent database is already installed in your environment, you must enter the details of the connection to the database.

3. Click **Next**.

The system displays the following screen:

4. In the one-X Agent Central Management window, perform the following steps:

- a. In the **one-X Database name** field, enter the name of the Avaya one-X® Central Management database.

By default, the database name is **ACCCMONEXDB**.

- b. In the **Username** field, enter the name of the Avaya one-X® Central Management database user.

By default, the user name is **acccmonexuser**.

- c. In the **Password** field, enter the password of the database user.

- d. From the **Client Authentication Mode** drop-down list, select the authentication type.

The authentication type corresponds to the type of authentication the Avaya one-X® Agent clients use. The following authentication options are available:

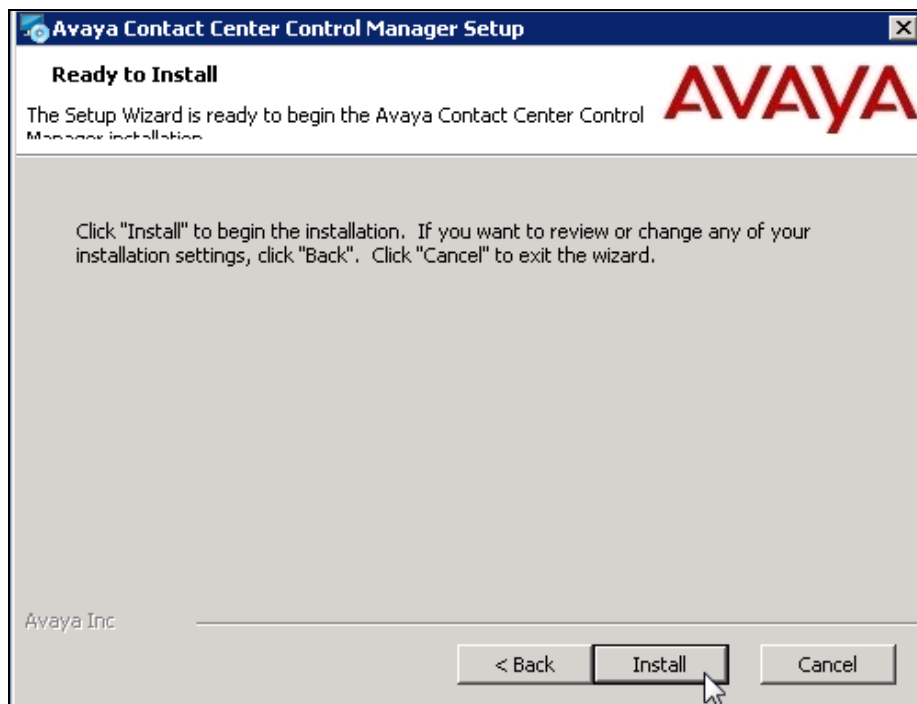
- **Basic:** Uses the user name and password to authenticate the one-X Agent database.
- **SSO:** The SSO authentication validates the user with the active directory.

- e. From the **Version** drop-down list, choose the appropriate version of one-X Agent.

The available options are 2.0 and 2.5.

5. Click **Next**.

The system displays the following screen:



6. Click **Install** to begin the installation and follow the on-screen information.



Chapter 3: Using the Avaya one-X® CAM administration portal

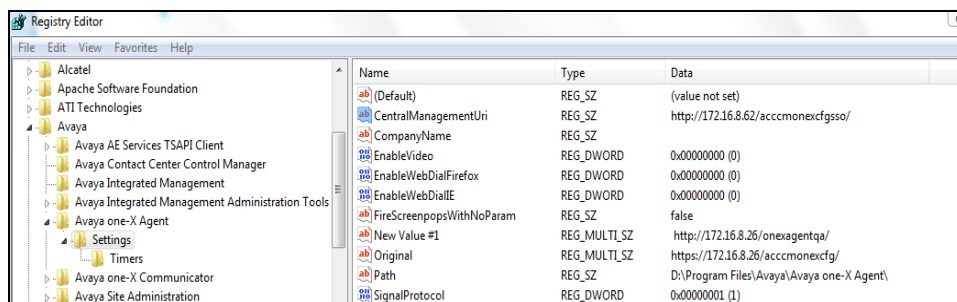
This chapter includes:

- [Avaya one-X® Central Management URL on page 18](#)
- [Logging on to Avaya one-X® Central Management on page 18](#)
- [Logging out of Avaya one-X® Central Management on page 19](#)
- [Planning a client configuration in Avaya one-X® Central Management on page 20](#)

Avaya one-X® Central Management URL

The Avaya one-X® Agent client stores the path to the Avaya one-X® Central Management URL in a registry key on the Avaya one-X® Agent client server.

The registry key is stored in: **HKEY_LOCAL_MACHINE > SOFTWARE > Avaya > Avaya one-X Agent > Settings**. The key name is **CentralManagementUri**.



The value that appears is `http://ip of the acccm onex server/acccmonex/`.

If you configured the ACCCM system to work with Avaya one-X® Agent in SSO mode, the URL is `http://ip of the acccm onex server/acccmonexcfgsso/`.

Logging on to Avaya one-X® Central Management

Prerequisites

- Obtain the user name and password for Avaya one-X Avaya one-X® Central Management.
- Ensure that you install one of the following browsers:
 - Internet Explorer 7.x or later
 - Mozilla Firefox 3.x or later



1. Open the Web browser and in the address bar, type

https://<host>:8643/oneXAgentCM, where <host> is the Fully Qualified Domain Name (FQDN) or the IP address of Avaya one-X® Central Management.

If you are upgrading to Avaya one-X® Central Management 2.5 and using an earlier Avaya one-X® Central Management 2.0, ensure that you have changed the port to 8643, as necessary.

2. Log on to the Avaya one-X® Agent Central Management Web interface as an administrator.

The system displays the following screen:

The image shows the login interface for the Avaya ONE-X AGENT MANAGEMENT PORTAL. At the top left is the red AVAYA logo. To its right, the text 'ONE-X AGENT MANAGEMENT PORTAL' is displayed. Below the header, there are two input fields: 'User Name' and 'Password'. A 'Login' button is positioned below the password field. The entire interface is enclosed in a thin red border.

3. Enter the user name and password in the **User name** and **Password** fields.

The user name and password is itnv.

TIP: If you are logging on to Avaya one-X® Central Management for the first time after installing the application or if you do not have user credentials assigned, you can log in either as **onexagentcm** or **sroot** with **oxacm01** or **sroot01** as password, respectively. After logging on to the Avaya one-X® Central Management Web console, you can create users with the Web Administrator role for subsequent logins.

NOTE: Ensure that the user name in the Avaya one-X® Central Management console exists in Active Directory if your credential is not defined in the system as an administrative user.

4. Click **Login**.

The system logs you into the Avaya one-X® Central Management Web application as a user.



Logging out of Avaya one-X® Central Management

Prerequisites

- Before logging out of Avaya one-X® Agent, ensure that you save the changes made to the page.



- Click **Log off** on the top left corner of the page.



Planning a client configuration in Avaya one-X® Central Management

This section provides guidelines that you can follow to perform a client configuration using Avaya one-X® Central Management.

Use the follow instructions to optimize your efforts in configuring a client setup:

1. Plan the setup

Collect information about the number of profiles that agents might handle. Identify common and distinguishing requirements for each profile and accordingly plan for creating templates. Before the setup, determine the number of templates required.

2. Create the templates

After determining the client requirements and the profiles that agents need to handle, create templates in the Manage Templates section of Avaya one-X® Central Management that cater to those requirements. Initially, you can only create the template structure and name the required template. You can later configure the template in detail, as the number of requirements arises. The templates that you create serve as profiles for each agent handling calls for your specific profile.

3. Create agent groups

Create agent groups and assign Avaya one-X® Agent users to groups. When you assign templates to agents or groups of agents, each template creates a profile for each agent with the same name as the template. You can also assign templates to individual agents or a group.

4. Assign templates to agent groups

Assign the corresponding template to each agent group. The groups inherit the user configurations and other settings of the template and share a common configuration for the assigned profile.

5. Define your users

Define your users by individually creating user details from the Manage Users screen. You can also create user lists using a comma separated values (CSV) file. Use the example CSV file, available from the Import Users page of Avaya one-X® Central Management, to create a user list with respective user roles and templates to which the users must be assigned.

By creating the user list, you can save the configuration efforts of each user on Avaya one-X® Central Management. You must ensure that you assign role and templates correctly in the CSV file. A typographical error may prevent the user from getting assigned to a correct role or template. Users cannot log on to Avaya one-X® Agent if you do not assign users to a template. Therefore, you must assign all users a high-level template or the default template.

6. Import the CSV file of users

To use the CSV file of users, you must import the CSV file into Avaya one-X®

Central Management. The system assigns the users to the corresponding roles and templates that you created before importing.

7. Assign users to the appropriate groups

Assign users to the appropriate groups based on the profile.

8. Assign supervisors to groups

The system assigns the supervisor roles to users when the system completes importing the roles from the CSV file. However, you must assign supervisors to a user group that they manage at this stage. The system adds the user group to the supervisors contact list automatically.

9. Create contact lists and assign to a template

Create contact lists of clients for whom you created the templates. Assign each contact list to the corresponding template. Thus, the agent groups assigned to the templates inherit the contact list.

10. Configure templates

Assign features and permissions to the template according to the contact center setup and the client profiles for which the template was created.

11. Set up any hot-desking locations

Set up any hot seating locations using the Manage Location Data page.

Chapter 4: Administering users

This chapter includes:

- [Importing users into Avaya one-X® Central Management on page 22](#)
- [Adding users in Avaya one-X® Central Management on page 24](#)
- [Deleting users on page 30](#)
- [Filtering users on page 31](#)
- [Activating or deactivating a user on page 32](#)
- [Editing user details on page 32](#)

Importing users into Avaya one-X® Central Management

With Avaya one-X® Central Management, you can perform a bulk user import, with respective user credentials, roles, templates, and groups. To perform a bulk import, the user data must be available in a tab-delimited file.

NOTE: For a sample tab-delimited file, see the example link on the Import Users page. Click the example link, save the CSV file to your computer as a Unicode Text file, and add the user details to the file. The Unicode Text file saves the data in the tab-delimited format.

If you saved the user details to a local computer as a CSV file, you can import users with the relevant data to Avaya one-X® Central Management by saving the CSV file as a Unicode Text file and importing the file.

NOTE: When the system imports a user from the Unicode Text file that already exists on Avaya one-X® Central Management, the system adds the roles, templates, and groups. The import of existing users does not replace, delete, or duplicate the users from the list of users in the Manage Users section of Avaya one-X® Central Management console.

TIP: Create groups and templates that you plan to assign to the users before importing users. You can then directly add template names in the tab-delimited file and configure or modify the templates later.

Prerequisites

To import users, you must first save the user credentials in a Unicode Text file. The order of column headings in the tab-delimited file must be as follows:

Column heading	Description
User name	The Avaya one-X® Agent user name to be stored in Avaya one-X® Central Management.
First Name	User's first name.
Last Name	User's last name.
Email	User's email address.
Role: one-x Agent	To assign a user to an Avaya one-X® Agent role, enter Y or Yes in the Role: one-x Agent column. If not, leave this field blank.
Role: one-x Agent Supervisor	To assign a supervisor to an Avaya one-X® Agent role, enter Y or Yes in the Role: Avaya one-X® Agent Supervisor column. If not,

Column heading	Description
	leave this field blank.
Role: Web Administrator	To assign a supervisor to an Avaya one-X® Agent administrator, enter Y or Yes in the Role: Avaya one-X® Agent Administrator column. If not, leave this field blank.
Template: <default>	As indicated, substitute <default> with the template name that you want to assign to the user. Enter Y or Yes in this column against the user name to assign the template. Multiple columns can correspond to the templates in Avaya one-X® Central Management. However, ensure that the template names match the names in Avaya one-X® Central Management.
Group: <group name>	Replace <group name> with the exact name of the user group in Avaya one-X® Central Management. You can create multiple columns for the groups in Avaya one-X® Central Management to which you want to assign users. However, the group names must exactly match the names in Avaya one-X® Central Management. Enter Y or Yes in the group columns against the user name to assign the user to the group.

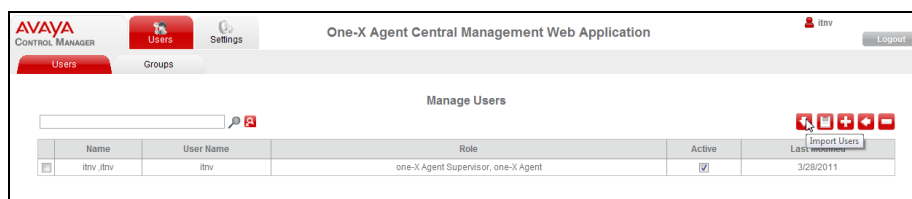
CAUTION: When you are adding data to a file, do not delete or overwrite the header row of the Unicode Text file.

To use the import option, ensure that the format of the Unicode text file conforms exactly to the specification mentioned in the table and then perform the following tasks:



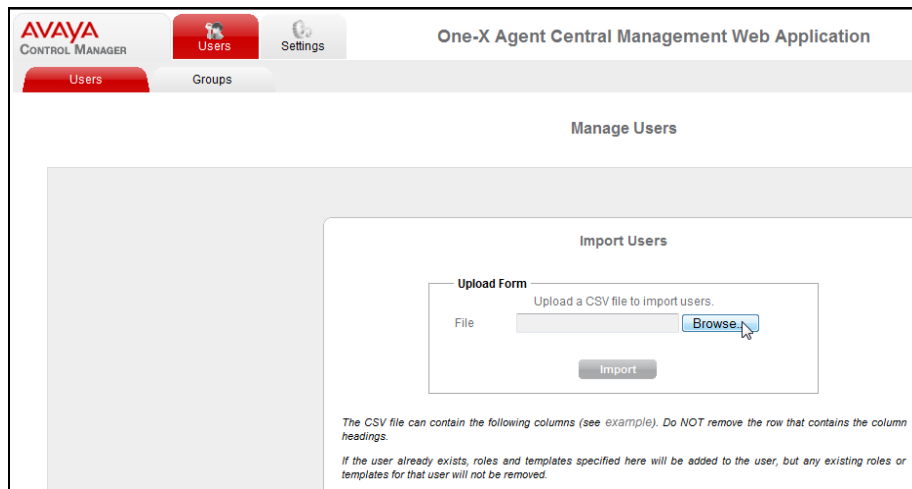
1. From the Avaya one-X® Central Management navigation menu, click **Import Users**.

The system displays the following page:

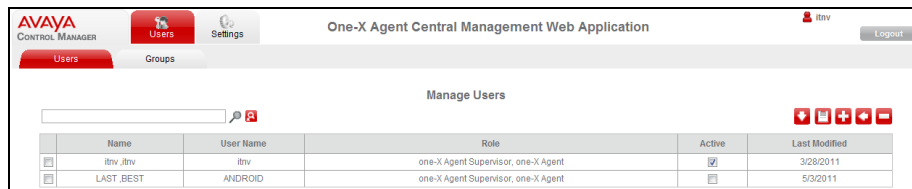


2. In the **File** field, click **Browse** to locate the Unicode Text file.

The system displays the following page:



3. Click **Import** to import users listed in the Unicode Text file.



The system imports all the users in the user list.



Adding users in Avaya one-X® Central Management

Prerequisites

- Ensure that you define in Active Directory, all users that you add to or import from the CSV file into Avaya one-X® Central Management.



1. On the Avaya one-X® Central Management navigation menu, click **Manage Users**.

The system displays the Manager Users page.

2. Click the **Add user** link.

The system displays the following page:

The screenshot shows a web interface for managing user details. It has two tabs: 'Details' (active) and 'Group Membership'. The 'Details' tab contains a form with the following fields and sections:

- *User Name (text input)
- *First Name (text input)
- *Last Name (text input)
- *Password (text input)
- Email (text input)
- *Authentication Type (dropdown menu, currently set to 'DB User')
- Domains (dropdown menu, currently set to 'select domain')
- Contact Center Roles** (checkboxes):
 - ☐ One-X Agent
 - ☐ One-X Agent Supervisor
- Web Admin Roles** (checkboxes):
 - ☐ Web Administrator

A note at the bottom of the form reads: "Note: Roles assigned via membership of a group can only be removed by first removing the user from that group".

3. In the **User Details** panel, click the **Add user** link.
4. In the **Details** tab, perform the following steps.
 - a. In the **Username** field, enter the contact name.
 - b. In the **First Name** field, enter the contact's first name.
 - c. In the **Last Name** field, enter the contact's last name.
 - d. In the **Password** field, enter the password.
 - e. In the **Email** field, enter the email address of the contact.

NOTE: The **Username**, **First Name**, **Last Name**, and **Password** are mandatory fields.

- f. From the **Authentication Type** drop-down list, select an appropriate option.

ACCCM one-X supports three different authentication methods:

Authentication type	Description
DB User Standard	Use the DB User Standard option if the authentication type is set as database user name and password authentication with the information stored in the ACCCM Avaya one-X® Agent database.
LDAP Root	Use the LDAP Root option if the authentication type is set as SSO with the user domain credentials. For LDAP root authentication, you must configure the Avaya one-X® Agent client to support SSO. <i>See Installing and configuring Avaya one-X® Agent.</i>

LDAP Credentials	Use the LDAP Credentials option for mixed authentication that uses the username and password entered by a user and authenticates the users with the organizations LDAP source.
-------------------------	--

For more information, see [Chapter 9: Authentication modes and LDAP integration on page 77](#).

- g. (Optional) method, select an appropriate domain from the Domain drop-down list.

For more information, see to [LDAP Root on page 79](#) and [LDAP Credentials – Mixed Authentication on page 82 in Chapter 9: Authentication modes and LDAP integration on page 77](#).

- h. To assign user roles, select any of the following options in the **Contact Center roles** and **Web Admin Roles** panels:

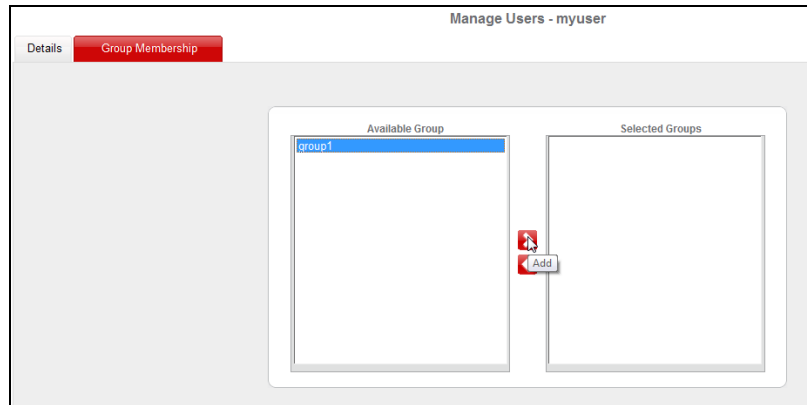
Use role	Privileges
one-X Agent	Assign the one-X Agent role to users using Avaya one-X® Agent in a contact center. Users with one-X Agent role have the following rights and restrictions: • Users can use all the privileges assigned through Avaya one-X® Central Management but do not have permission to modify the privileges. • Users can modify their settings on the Avaya one-X® Agent user interface if the fields are marked as modifiable from Avaya one-X® Central Management. Users with one-X Agent role do not have access to the Avaya one-X® Central Management Web interface.
one-X Agent Supervisor	Assign the one-X Agent Supervisor role to users who are responsible for Managing and Service Observing agents in their My Team group. Users with the one-X Agent Supervisor role also have all privileges of the Avaya one-X® Agent role and access to the Avaya one-X® Central Management Web interface.
Web Administrator	Assign the Web Administrator role to users who perform all the tasks on the Web Administrator interface. Web Administrators are also responsible for troubleshooting any technical issue. Although Web Administrators have all the privileges of Avaya one-X® Central Management, the administrators do not have access to Avaya one-X® Agent, since they are not the intended end users.

You can select multiple user roles for the user. After selecting the one-X Agent roles, the system displays the **Profiles assigned** tab. If you select **Supervisor Role**, then the system displays the **My Team** tab. The system does not display the **My Team** tab for other roles.

5. If you click **Save** without selecting any roles, then the system saves the user details without any roles assigned to the user.
6. To assign user groups, perform the following steps:

- a. Click the **Group Membership** tab.

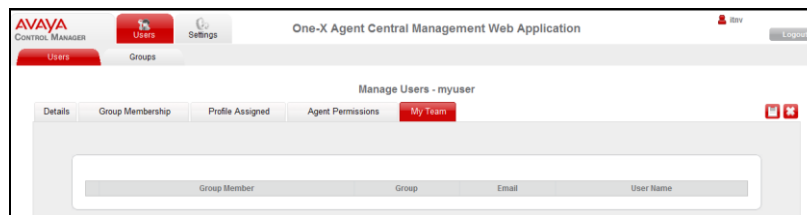
The system displays the following page:



- b. In the **Group Membership** tab, select the appropriate group and click **Add**.

The system assigns the user to the selected group. Repeat the step to assign multiple user groups.

If you have assigned a **one-X Agent Supervisor** role to a user, the system displays the **My Team** tab as follows:



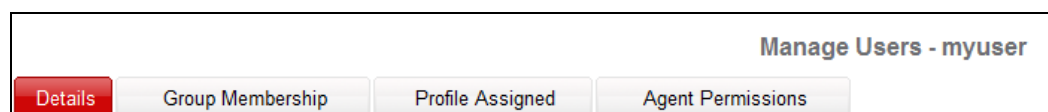
7. Click the **My Team** tab to view the members of the user group assigned to the user.

The **My Team** tab has details of group member, groups, email, and user name. You can sort the **Group member**, **Email**, and **Username** columns in ascending and descending order and the corresponding details get aligned accordingly. Click the **First**, **Prev**, **Next**, and **Last** links to navigate the list of team members if the list is long.

NOTE: To view child profiles in the Profile name list, you must create child profiles in the Manage Templates section. To create a child profile, in the default parent profile, click **Add**. Then enter the child profile name and click **Save**. You can repeat the step to create additional child profiles.

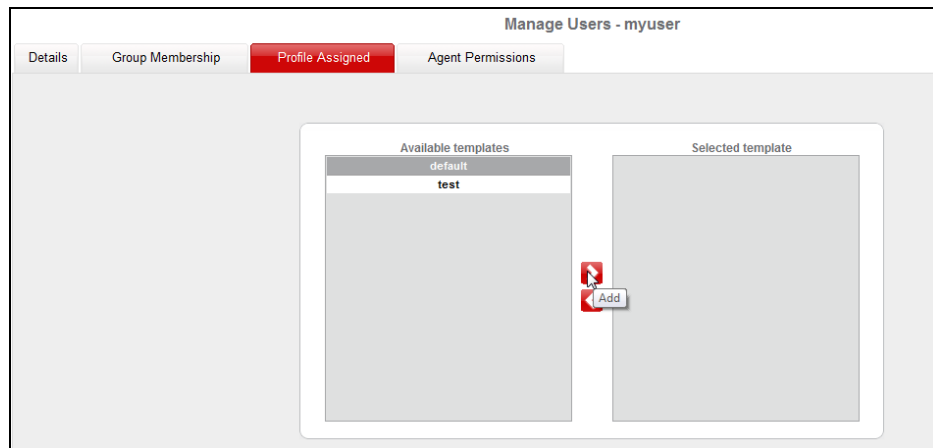
NOTE: When you assign a template to a user, the system generates a profile for the user with the same name as the assigned template.

8. If you assign the user to Avaya one-X® Agent role, then the system displays the following tabs:



9. To assign a template to a user, perform the following steps:
 - a. Click the **Profile Assigned** tab.

The system displays the following page:



- b. Select a profile from the **Profile name** list.

The system lists the parent and child templates in a cascading manner and displays the child templates indented under the parent profile names. When you assign the template to the corresponding user, the system generates a profile for the corresponding user with the same name as the template that was assigned. The system also marks the profile as Preferred.

- c. Click **Add**.
- d. To assign multiple templates to the user, repeat the step 9a to 9c.

A user cannot log on to Avaya one-X® Agent unless you assigned a template to the user. Upon assigning multiple templates to the users, the system generates multiple profiles for corresponding user with the same names as the respective template that was assigned. The Preferred profile remains unchanged. In other words, the first template that the system assigns to the profile is marked as the **Preferred** profile.

NOTE: If you created a hot-desking user, the system overwrites the location data in the assigned template (login extension and password) with the location data at which the user logs on.

10. To customize the user profile for the selected user, click the **Profile Settings** link in the **Edit** column of the **Profiles assigned** tab.

The system displays the profile editor screen. Customize the assigned profile for the selected user.

11. Select **Automatically execute all logins for the selected profile**, if you want the system to execute auto login for users into the services automatically.
12. Select **Disable local profile Administration**, if you do not want the user to modify the preferred selection during the user login.

If you do not enable the **Disable local profile Administration** option and only assign a profile, the system skips the profile selection window and logs the user directly with the preferred profile. However, if you assigned multiple profiles to the corresponding user, the system displays the profile selection window so that you can select a profile other than the preferred profile.

13. To set permission for a user, click the **Agent Permissions** tab.

The system displays the following page:

You can set appropriate permissions based on the information in the following table. The permissions are divided into **Agent Permissions** and **General Settings**.

The **Agent Permissions** tab provides access permissions that you can control. Users can gain access to various features based on the settings selected in the panel:

Option	Description
IM Contacts Not in System Contact List	With this option, users can send instant messages to contacts outside their contact list.
Allow Desktop Sharing	Select the Allow Desktop Sharing option if you want the agent to share the desktop with the other user through the IM session, or internal telephone calls within Contact List and Presence Services.
Window Size	Use the Window Size option in conjunction with Allow Desktop sharing to set the window size of the desktop sharing window. You can select from the following sizes: • Actual size • Full screen • 25% • 50% To use the Window Size option, you must select the Allow Desktop sharing option.

The **General Settings** tab lists the settings for actions that CAM must perform when a user logs out of a system.

Field name	Field description
Save agent settings from desktop on exit	Use this option to save the Avaya one-X® Agent current profile of the agent on the local computer and to upload the changes to Avaya one-X® Central Management when an agent logs out. If the agent is unable to log on to Avaya one-X® Central Management, the Save agent settings from desktop on exit option allows the agent to log on using the last

Field name	Field description
	used profile. The system saves the previous settings to the local cache and then uses the same to authenticate the agent and log on to Avaya one-X® Agent. The system prompts the agent to select the Use emergency configuration option to log on to Avaya one-X® Agent.
Delete agent log on exit	Use the Delete agent log on exit option if you want the system to delete the agent's work log stored locally on the agent's system when the agent logs out of Avaya one-X® Agent. The work log contains critical log of agent work.
Delete contact lists on exit	Use the Delete contact lists on exit option if you want the system to delete the agent's contact list stored locally on the agent's system when the agent logs out of Avaya one-X® Agent. The contact list contains critical information on agent contacts.
Time between client configuration saves	Use the Time between client configuration saves option if you want the system to specify the interval between saves of the user profile data changes to Avaya one-X® Central Management while logged in.

14. Click **Save** to add the user to Avaya one-X® Central Management.



Deleting users

Perform the following steps to delete a user from Avaya one-X® Central Management.



- On the Avaya one-X® Central Management menu, click **Manage Users**.
The system displays the Manage Users page with the user list.
- On the Manage User page, click the **Users** tab.

The system displays the following page:

Users

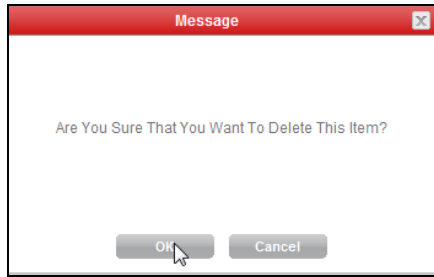
Groups

Manage Users

	Name	User Name	Role	Active	Last Modified
☐	itnv_itnv	itnv	one-X Agent Supervisor, one-X Agent	☒	3/28/2011
☐	LAST_BEST	ANDROID	one-X Agent Supervisor, one-X Agent	☐	5/3/2011
☒	willson_barry	myuser	one-X Agent	☒	5/3/2011

- In the users list, select a user and click **Delete (-)**.

The system displays the following page:



4. Click **OK** to confirm.



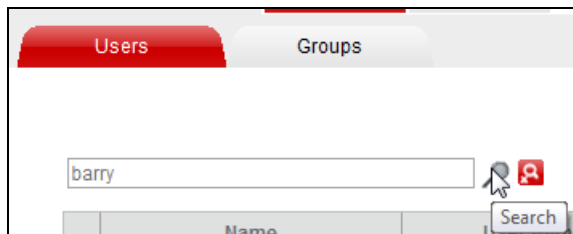
Filtering users

Avaya one-X® Central Management provides a quick filtering option to find users from the Central Management user list. You can filter users by names, roles, templates, or their active state.



1. On the Avaya one-X® Central Management menu, click **Manage Users**.
The system displays the Manage Users page with the user list.
2. To find a user by name, in the **Filter** field, enter the first name or last name of the user or the user name.

The system filters the keywords matching the field and displays the keywords in the user list.



3. To find a user by assigned roles, select one of the following roles.

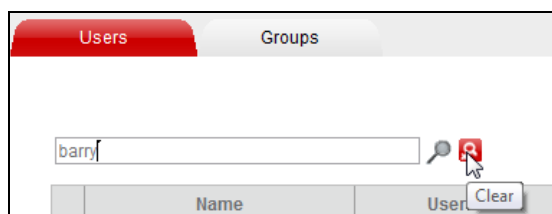
Options	Description
one-X Agent	To filter only one-X Agent users.
one-X Agent Supervisor	To filter only one-X Agent supervisors.
Web Administrator	To filter only one-X Agent Web administrators.

By default, the system applies the By role filter criteria. The system filters the keyword matching the role and displays keywords in the user list.

4. To find a user by name and role, enter the first or last name of the user in the **Filter** field, and select an appropriate role from the list.
The system filters the user list based on the name and role criteria.
5. To find a user by template, select a template from the **By template** list.
6. To find a user status, select one of the following list items from the **All users** drop-down list. By default, the system displays only activated users.

- Only activated users
- Only deactivated users
- All users

7. To clear the search result and search again, click the **Clear** button.



Activating or deactivating a user

Administrators can prevent or grant access to an Avaya one-X® Central Management navigation and Avaya one-X® Agent for users by adjusting the Activation or Deactivation fields.

When administrators deactivate a user, the system displays an Operation Failed message when the user attempts to log on to Avaya one-X® Agent. But all configurations remain attached to the user. On activation, agents can log in using the last saved configuration data.

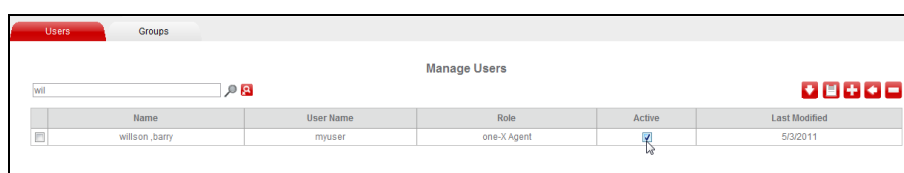
Prerequisites

Ensure that user details are present in Avaya one-X® Central Management.



1. On the Avaya one-X® Central Management navigation menu, click **Manage Users**.

The system displays the following page:



2. Perform one of the following steps:
 - To deactivate a user, clear the **Active** option corresponding to the user name.
 - To activate a user, select the **Active** option corresponding to the user name.



Editing user details

The Web administrator can edit the following user details:

- All details on the **User Detail** tab.
- User groups assigned on the **Group membership** tab.
- User profile assigned on the **Profiles assigned** tab.
- User permissions assigned on the **Agent permissions** tab.

Prerequisites

The user must be a Web Administrator and must have appropriate permission to edit user details.



1. On the Avaya one-X® Central Management navigation menu, click **Manage Users**.
2. In the user list, select a user in the **Name** column to edit.

The system displays the following page:



3. On the User Detail page, perform the following steps:
 - a. To edit the user name, and email address, click the **Details** tab.
 - b. To remove groups, click the **Group membership** tab, and then click the **–** button next to **Add / Remove**. To assign groups, click the drop-down list under the **Group name** column, select a group, and click the **+** button next to **Add / Remove**.
 - c. To remove profiles, click the **Profiles assigned** tab, and then click the **–** button next to **Add / Remove**. To assign profiles, click the drop-down list under the **Profile name** column, select a profile and click **+** button next to **Add / Remove**.
 - d. If you attempt to remove a profile that is the only profile assigned to the user, the system displays the following message:

A profile is required to log onto one-X agent and you are deleting the only profile for this user. Are you sure you want to delete this profile? If you click "Yes", the profile will be deleted.

However, if you have assigned multiple profiles to a user and you are attempting to delete a **Preferred** profile, then the system marks the previously assigned profile as the **Preferred** profile.
 - e. To customize a user profile for the selected user, click the **Profiles assigned** tab, and then under the **Edit** column, click the **Profile settings** link.

The system displays the profile editor screen.
 - f. To modify permissions, click the **Agent permissions** tab to change the appropriate settings.

4. Click **Save**.

The system applies the changes to the user setting and saves the user settings to Avaya one-X® Central Management.

NOTE: If the user is a member of a group, you cannot remove the roles and templates assigned to the user through the group. To remove roles and templates, you must first remove the user from the group, and then remove the user role or template for the corresponding user.



Chapter 5: User groups in Avaya one-X® Central Management

A user group in Avaya one-X® Central Management is a collection of users having either the same role or handling the same business area. You can create a group and assign one or more supervisors, roles, and templates to the group. The system applies the group assignments to each member of the group. Therefore, administrator can define the CM properties. The system adds the supervisors assigned to the group to the contact list of each member of the group in My Supervisors under a new My Supervisors entry on the one-X Agent Contact List window.

You can create, edit, delete, and filter groups using Avaya one-X® Central Management. You can also use a CSV file to perform bulk import of group definitions with assigned templates and users.

This chapter includes:

- [Group assignment logic on page 35](#)
- [Importing user groups into Avaya one-X® Central Management on page 36](#)
- [Creating user groups on page 37](#)
- [Editing user groups on page 39](#)
- [Filtering groups on page 41](#)
- [Deleting groups on page 41](#)
- [Removing users from a group on page 42](#)

Group assignment logic

When you assign a user to a group, the user inherits the configuration from the group. The following section explains in detail the logic behind the group assignment process.

The table describes what happens when you assign a role to a user. The first two columns represent the user state before the assignment to the group and the two last columns represent the user state after the assignment.

Existing profile	Existing role	Updated profile	Updated role
None	None	Group profile	Group role
Yes	None	Original profile	Group role
Yes	Yes	Original profile	Group role
None	Yes	Group profile	Group role

When you remove a user removed from a group, the user keeps the assigned profile and assigned role.

Importing user groups into Avaya one-X® Central Management

You can import bulk group definitions into Avaya one-X® Central Management and then assign agents to the group definition. You can also assign agents to existing groups.

Use the import option when you have to create large number of groups, assign various roles to each group, and assign groups to various templates in Avaya one-X® Central Management.

You can create all the required groups outside Avaya one-X® Central Management, and then import the groups into Avaya one-X® Central Management. The import option saves time from creating individual groups in Avaya one-X® Central Management and assigning them roles and templates.

You must create the group names and assign appropriate roles and templates in the Unicode Text file. If you have an earlier CSV file with data, you must save the file as a Unicode Text file. The system adds the user roles and templates to the CSV file in addition to any existing roles and templates group members already possess.

TIP: Avaya recommends that you determine the groups and then assign templates for each group before importing groups. By doing so, you can directly add template names in the CSV file and save your effort of assigning templates post import.

You might edit or configure the templates later.

Prerequisites

- To import groups, the group file must be available as a CSV file.
- If the group CSV file does not exist, perform the following steps to create a group list:
 - i. On the Avaya one-X® Central Management navigation menu, open the Import Groups page.
 - ii. Click the example link, and export the file to your computer.
 - iii. Open the groupsexample.csv file, and enter the following details:

Column heading	Description
Group name	Enter the name of the group.
Role: one-X Agent	Enter Y or Yes if the group has the one-X Agent role. If the group has the one-X Agent role, enter Y or Yes
Role: one-X Agent Supervisor	Enter Y or Yes if the group has the one-X Agent Supervisor role. If you leave the field blank, the system will not grant access for Avaya one-X® Agent.
Role: Web Administrator	Enter Y or Yes if the group has the Web Administrator role. If you leave the field blank, the system will not grant access for Web Administrator.
Template: <template name>	Ensure that the template name on the form matches the name that you assigned to the template when you added the template to the system. Multiple columns can correspond to the templates created in Avaya one-X® Central Management. However, ensure that the template names match

Column heading	Description
	the names in Avaya one-X® Central Management.

CAUTION: When you add data to the file, do not delete or overwrite the header row of the CSV file.

- iv. Save the file with a different name.

While saving the file, ensure that you save the file as a CSV file with a .csv extension.

Perform the following steps to import group data.



1. On the Avaya one-X® Central Management navigation menu, click **Import Groups**.
2. In the **File** field, enter the CSV file path, or locate the CSV file by clicking **Browse**.
3. Click **Import** to import groups listed in the CSV file.

The system imports the groups into Avaya one-X® Central Management.



Creating user groups

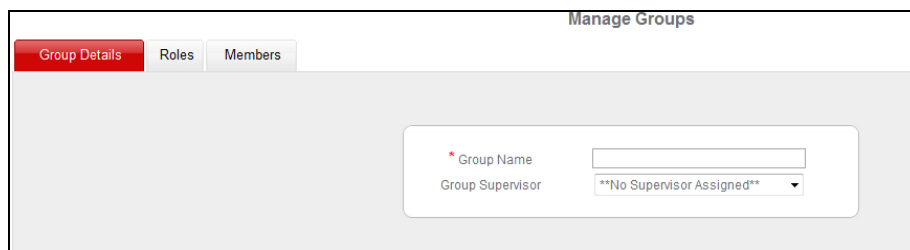


1. On the Avaya one-X® Central Management navigation menu, click **Manage Groups**.



2. On the **Manage Groups** page, click **Add Group**.

The system displays the Group Detail tab at the bottom of the page with the Group details, Roles, Templates, and Member tabs. The Template tab is for the Web Administrator role only.



3. On the **Group details** tab, perform the following steps:

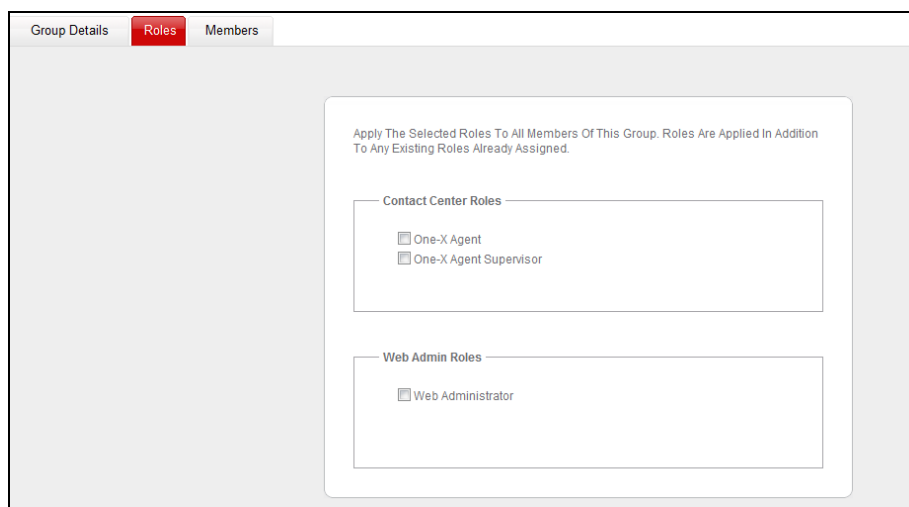
- a. In the **Group name** field, enter a name for the group.
- b. From the **Group supervisor** drop-down list, select a supervisor.
Group supervisor is an optional step. If you assign a supervisor, the system displays all the group members in the **My Team** list of the supervisor.
- c. If you select a supervisor for the group, select the **Add supervisor to speed dial** option to add the name of the supervisor to the speed-dial list and view the list in the Avaya one-X® Agent Contact List window under **My Supervisors**.

By default, the system activates the Add supervisor to speed dial option but is disabled until you select a supervisor from the Group supervisor drop-down list.

You can clear the Add supervisor to speed dial option to remove the supervisor from the speed-dial list and from the My Supervisors entry of the Contact List window.

- d. To add members to the group:
 - i. In the Group details tab, click **Add/Remove Members**.
 The system displays the Add/Remove Members window with users.
 - ii. Select a user to add to the group by selecting the **Group member** option corresponding to a user.
TIP: You can use the Filter option to filter the user group based on Name, Role, and Member or Non-group member parameters.
 When you select a contact from the group, the system displays a message at the bottom of the window.
 - iii. Click Close.
 The **Group Detail** tab displays the number of active members added to the group.

4. To assign selected roles to all members of the group, click the **Roles** tab, and select the appropriate user roles.

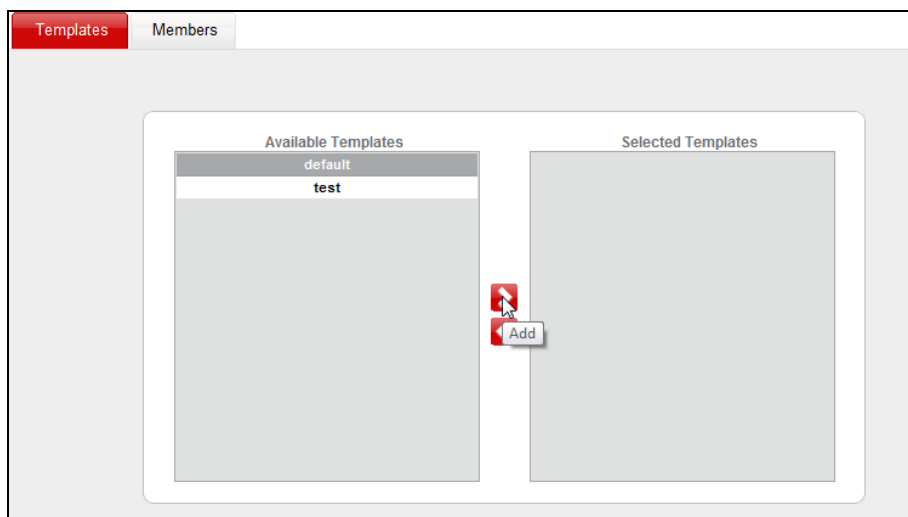


You can assign multiple roles to the group, namely, **one-X Agent** and **one-X Agent Supervisor** roles. The system adds these roles in addition to any other roles already assigned to the members.

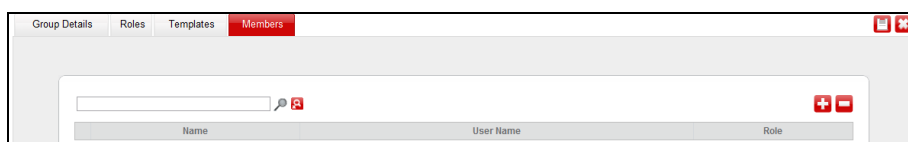
If you select the **one-X Agent** or **one-X Agent Supervisor** role, the system adds the **Templates** tab.



NOTE: The system does not display the **Templates** tab if you are creating a group with the **Web Administrator** role.



5. To assign a template for **one-X Agent** or **one-X Agent Supervisor** roles, click the **Templates** tab and perform the following steps:
 - a. From the **Template name** drop-down list, select an appropriate template, and click **Add** from the **Add/Remove** column.
 The system assigns the template to the group and displays the template in the row.
 - b. To view the template settings, click the **Template settings** link corresponding to the assigned template in the **View** column.
 The system displays a new window with the template settings. To modify, see [Central Management templates on page 41](#).
6. To view the newly added members of the group, click the **Members** tab.
7. To add or remove group members, use the Add/Remove members link.



8. To save the group with the given name and assigned details, click **Save**.



Editing user groups

You can change the following group details:

- Group name and supervisor
- User roles assigned to the group

- The number of group members

Perform the following steps to make the necessary changes in the group details:



1. On the Avaya one-X® Central Management navigation menu, click **Manage Groups**.

The system displays the Manage Groups page.

2. From the **Group** column, select a group.

The system displays the **Group Detail** tab at the bottom of the page with the group details.

3. To modify the group, on the **Group Details** tab, make the appropriate changes in the **Group Name** field or the **Group Supervisor** drop-down list.

The **Add supervisor to speed dial** option works in conjunction with the **Group Supervisor** drop-down list. To remove one or more supervisors from the speed-dial list, clear the **Add supervisor to speed dial** option for the supervisor selected in the **Group Supervisor** drop-down list. When you log in to one-X Agent as one of the group members, you see that the speed-dial icon does not appear next to all the group members under the **My Supervisors** entry of the Contact List window.

4. To modify roles to the selected group, click the **Roles** tab and select the appropriate option.

You can select one of the following Contact Center or Web Administrator roles:

- one-X Agent
- one-X Agent Supervisor
- Web Administrator

You can apply the selected roles to all members of a group. You can apply the roles in addition to any existing roles already assigned.

5. To add or remove a template, click the **Templates** tab, and perform the following steps:

- To add a template, select the appropriate template from the **Template name** list and, click **Add** in the **Add / Remove** column.
- To remove a template, click the corresponding delete button on the **Templates** tab, and click **Remove** in the **Add / Remove** column.
- To view the template settings, click the corresponding **Template** settings link in the **View** column.

The system displays the read-only view of template settings in the new window.

6. To add or remove group members, click the Members tab and perform the following steps:

- a. Click the **Add/Remove Members** link.

The system displays the user list in a new window with options next to each user.

- b. Select the options that you want to add, and clear the options that you

want to remove.

You can add or remove only one user at a time.

c. Click **Close**.

7. Click **Save**.



Filtering groups



1. On the Avaya one-X® Central Management navigation menu, click **Manage Groups**.

The system displays the Manage Groups page.

2. To find groups by name, in the **Filter** field, enter a group name.

The system displays the keyword matching the group name in the list.

3. To find groups by role, select a user role from the **Filter** drop-down list.

The system displays the keyword matching the group role in the list.

4. To find groups by template, select a template from the **By template** drop-down list.

The system displays the keyword matching the template in the list.

5. To find groups based on both group name and user role, enter the group name in the Filter list, and select a user role from the list.

The system displays the keyword matching both the criteria group in the list.



Deleting groups

The ACCCM wizard does not remove the system databases during the ACCCM removal process. You must remove the database manually.

Perform the following steps to remove the system database manually:



1. On the Avaya one-X® Central Management navigation menu, click **Manage Groups**.

The system displays the Manage Groups page.

2. Locate the group that you want to delete and click the **Delete** button from the corresponding group.

The system deletes the selected group.

NOTE: Deleting a group does not delete users or roles from the Avaya one-X®

Central Management server.

The system does not remove the roles assigned to users after deleting the group.



Removing users from a group

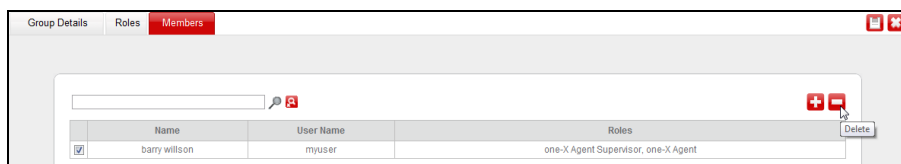
The ACCCM wizard does not remove the ACCCM databases during the removal process of the ACCCM system. You must remove the ACCCM databases manually.

Perform the following steps to remove the ACCCM database manually:



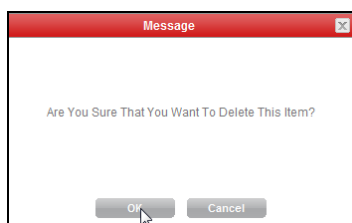
1. On the Avaya one-X® Central Management navigation menu, click **Manage Groups**.

The system displays the following page:



2. Locate the group and select the user that you want to delete from the group.
3. Click **Delete**.

The system displays the following confirmation window:



4. Click **OK**.



Chapter 6: Managing the location data

With location data, you can allow agents to hot-desk. That is, agents can log on to the Avaya one-X® Agent client from any desk or location and retrieve their profiles with customized settings and user data.

Using Avaya one-X® Central Management, you can pre-define the location data for desktops that you know can be used for hot-desking. For each desktop, you can specify a Host Name, Extension, Password, and Call Server address.

When the system authenticates an agent at user login from a desktop identified as a hot-desk, the Avaya one-X® Agent client updates the Extension and Password fields on the Login window with the telephone settings at the new desk. The agent can begin work immediately after assuming full configuration. After you log out from the system, the central server stores all user data.

This chapter includes:

- [Importing the location data on page 43](#)
- [Editing the location data on page 44](#)
- [Deleting the location data on page 45](#)

Importing the location data

Prerequisites

- Before importing location data, you must create a CSV file. The example CSV file is available in the Import Location Data page. You must save the sample excel file to the local directory as a .csv file, open the locationexample.csv file, and assign the location data, as appropriate.

NOTE: Rename the locationexample.csv file to prevent instances of similar files in the system. You can use the file for future use.

The locationexample.csv file contains the following columns:

Column	Description
Host Name	The host name is the name of computer that agents use.
Extension	The extension number of the endpoint associated with the host, for example, type the extension as 1234.
Password	The extension password. For example, you must type the password as password while importing the location data and set the actual password in the editing location data. Otherwise, the system prompts an agent for password on login.
Call Server Address	The IP address or FQDN of Call Server, for example, pbx.example.com.

IMPORTANT: Do not remove the row that contains the column headings.



1. On the Avaya one-X® Central Management navigation menu, click **Import Location Data**.

The system displays the following page:

2. In the **File** field, click **Browse** to locate the CSV file that contains the location data.

The system displays the following page:

Column Heading	Description
Host Name	The Host name specified as either: A Fully Qualified Domain Name (FQDN) e.g. agent37.voicecompany.com, or IP address e.g. 135.27.66.23
Extension	The extension number of the endpoint associated with the host.
Password	The password for the extension.
Call server address	The IP address or host name for the Call Server

3. Click **Import**.

The system imports the location data to the database. You can check the new location data in the Manage Location Data page. If the system does not import the data correctly or if there is an error message, you must verify the CSV file.



Editing the location data

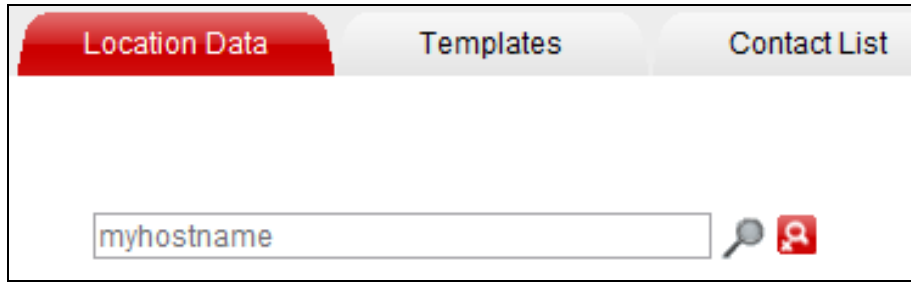
Prerequisites

- The location list must be present on Avaya one-X® Central Management.



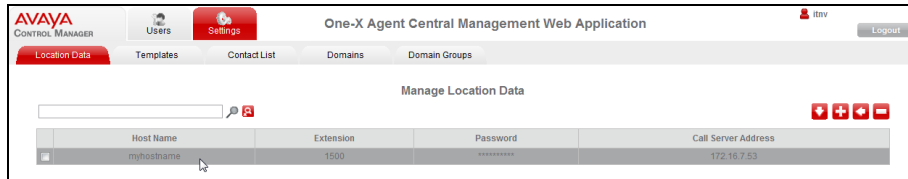
1. On the Avaya one-X® Central Management navigation menu, click **Manage Location Data**.

The system displays the following page:



2. Locate the location data.

The system displays the following page:



3. Double-click the location data record or click **Edit** and make the necessary changes.
4. Click **Save**.



Deleting the location data

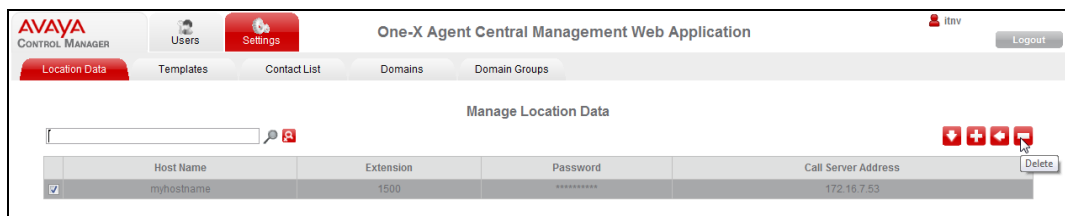


1. On the Avaya one-X® Central Management navigation menu, click **Manage Location Data**.

The system displays the Manage Location Data page with a list of administered locations.

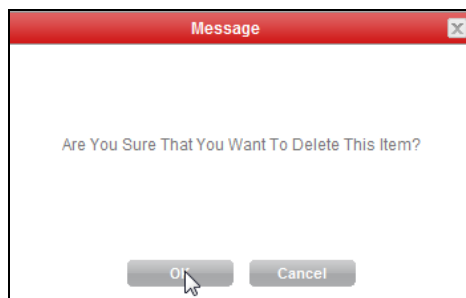
2. Navigate to **Settings > Location Data**.
3. Search for the Location Data Record.
4. Select the record you want to delete.

The system displays the following page:



5. Click **Delete**.

The system displays the following page:



6. Click **OK**.



Chapter 7: Managing Avaya one-X® Central Management templates

A template is a collection of user settings. Using templates, you save time and effort in user configuration. As an administrator, you can create a template and assign the template to an individual user or a user group. When you assign a template to a user, the system generates a user profile with the same name as the template. The system applies the saved template settings to the generated profile for a user.

You can restrict the users from changing all or specific profile settings. You can create parent and child templates based on the business requirement and expertise. If you make a change to a parent template, the child template inherits the changes automatically. However, if an agent changes the fields in the profile generated by a template, these changes permanently override the original profile settings generated from the original template assignment.

For example, if you create a template containing a value that is not optimal for an agent, the agent can override the value in the agent profile by editing that value on the desktop. The system changes the modified value back to Central Management in the respective profile of an agent. The agent can then edit fields that are not set as read-only but can take advantage of all the other settings that you configured. The system displays the read-only fields with a check box. If you do not see a check box adjacent to the fields, the Avaya one-X® Agent client user can edit these fields.

In some configurations, only **All on this page** option is available, which sets all the fields for the corresponding page as read-only. Administrators must mark the read-only fields to avoid inconvenience to users who might use the various features of the Avaya one-X® Agent client daily.

You can edit the template that is already assigned to users. The system saves the templates immediately and applies the changes to the templates in the subsequent logon. The system applies the changed settings with other settings to the profile when the user logs on to the application. Similarly, the system updates any change made to the profile through the Avaya one-X® Agent client and applies the new profile in the next successful log on.

TIP: The system also displays the **Reset** button on all the configuration panels. The Reset button clears all the entries you apply to the data fields.

This chapter includes:

- [Creating templates on page 48](#)
- [Finding templates on page 49](#)
- [Editing templates on page 50](#)
- [Deleting templates on page 50](#)
- [Configuring the Telephony Login settings on page 51](#)
- [Configuring Alternate Server Addresses on page 51](#)
- [Configuring the Agent Login settings on page 52](#)
- [Configuring the IM Login settings on page 52](#)
- [Viewing Phone Numbers on page 53](#)
- [Configuring the Work Handling settings on page 53](#)

- [Configuring the Audio Greetings settings on page 54](#)
- [Configuring the Screen Pop settings on page 54](#)
- [Configuring the Launch Application settings on page 55](#)
- [Configuring the Directory settings on page 56](#)
- [Configuring the Work Log settings on page 57](#)
- [Configuring the Voice Mail Integration settings on page 57](#)
- [Configuring the Reason Code settings on page 58](#)
- [Configuring the Event Logging settings on page 59](#)
- [Configuring the Outlook Contacts settings on page 60](#)
- [Configuring the Dialing Rules settings on page 61](#)
- [Configuring the Touch Tone Shortcuts settings on page 62](#)
- [Configuring the Video - Basic settings on page 63](#)
- [Configuring the Video - Advanced settings on page 64](#)
- [Configuring the IM settings on page 64](#)
- [Configuring the IM Responses settings on page 65](#)
- [Configuring the TTY - General settings on page 66](#)
- [Configuring the TTY- Abbreviations settings on page 66](#)
- [Configuring the Call Handling settings on page 67](#)
- [Configuring the User Interface settings on page 68](#)

Creating templates

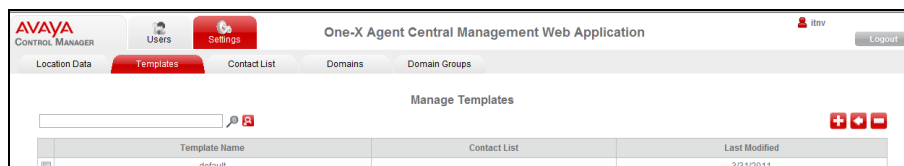
Avaya one-X® Central Management provides a default template from which you can derive child templates. You can also define other root nodes, if required. You can refer the procedures for configuring the template in the following sections.

To derive a new child template, click the Add button next to the existing parent template. Perform the following procedure to create parent and child templates:



1. On the navigation menu, click **Manage Templates**.

The system displays the following page:



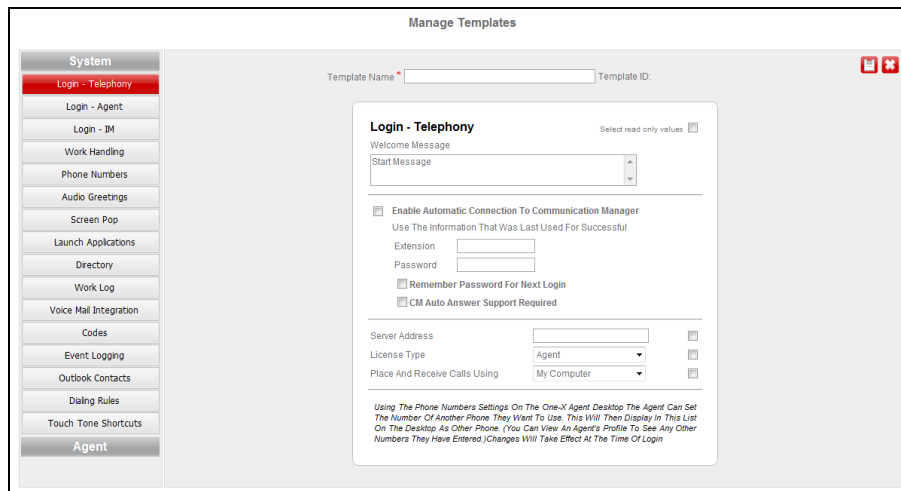
NOTE: If you have logged on to the Avaya one-X® Central Management Web interface for the first time, the system displays only the default template.

2. Click the **Add** button in the corresponding template.

The system adds a <new template> file and displays the new template as a child

template under the default or the new parent template.

The system displays the following page:



NOTE: The system adds a new template, but you cannot see the template unless you name the new template and then click the **Save** and **Close** button.

3. In the **Template name** field, enter a unique template name.
4. In the **Welcome Message** field, enter an additional welcome message.

NOTE: The text you enter in the **Welcome Message** field appears on the Welcome Avaya one-X® Agent client window. You can click the **Revert** arrow, if you want the system to revert to the inherited settings.

5. Click **Save**.

The system adds the new template file and displays the new template as a child template under default or new parent template.



Finding templates



1. In the Avaya one-X® Central Management navigation page, click **Manage Templates**.
The system displays the Manage Templates page with a list of parent or child templates.
2. In the **Search** field, enter the text by which you want to filter the template names.
The system displays the templates matching the search key on the page.
3. To find the filtered templates, click the **Previous Result** or **Next Result** link.



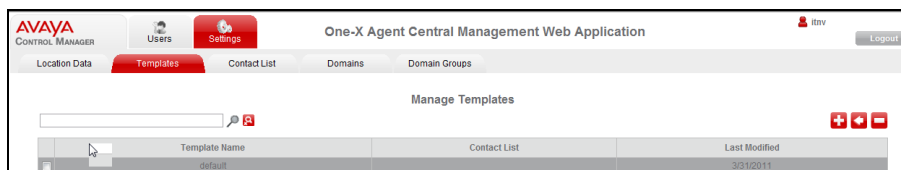
Editing templates



1. In the Avaya one-X® Central Management navigation page, click **Manage Templates**.

The system displays the Manage Templates page with a list of parent or child templates. Select **Settings > Template**

The system displays the following page:



2. Double-click the template you want to edit or click **Edit**.



Deleting templates

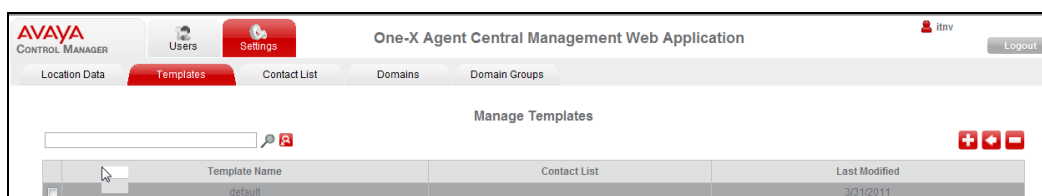


1. In the Avaya one-X® Central Management navigation page, click **Manage Templates**.

The system displays the **Manage Templates** page with a list of parent or child templates.

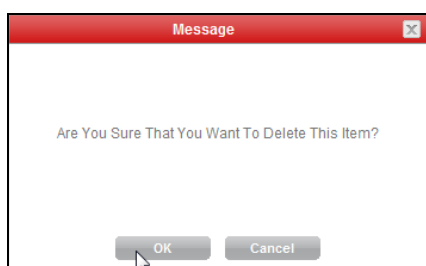
2. Select **Settings > Template**.

The system displays the following page:



3. Select the check box next to the template that you want to delete, and click **Delete**

The system displays the following page:



4. Click **OK** to confirm.



Configuring the Telephony Login settings

Perform the following steps after selecting the template to configure the Telephony Login settings.

The system displays the Template Detail page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **Login - Telephony**.
The system displays the Login - Telephony window.
2. Make the necessary changes to the fields.
3. To mark all fields as read-only for one-X Agent client users, select the **Select read only values** option.
4. Click **Save**.



Configuring Alternate Server Addresses

With the Alternate Server Address feature, you can specify alternate registration servers, if the main registration server defined on the telephony login screen is not available.

NOTE: The Alternate Server Address feature is independent of the Alternate Gatekeeper function available in the Communication Manager server. Communication Manager computes the Alternate Gatekeeper List at each registration and provides to the endpoint during a successful Registration, Admission and Status (RAS) process. The Alternate Server feature, on the other hand, is to set up a successful RAS session to begin with.

Prerequisites

- Obtain all alternate server addresses.



1. In the **Template Details** page, click **Alternate Servers**.
The system displays the Alternate Servers page.
2. Click **Add Server**.
3. In the **Server Address** field, enter the IP Address or FQDN of the alternate server.
The system displays the IP address in the **Alternate Servers** fields.
4. To add more servers to the list, repeat Step 1 to Step 3.
5. In the **Maximum Attempts for each server** field, specify the number of attempts the system must make to connect to each server before switching to the next

defined server.

6. Use the **Up** and **Down** buttons to arrange the order of the servers the system must try in a sequence.
7. To mark the **Server Address** field as read-only, in the Avaya one-X® Agent user interface, select the **Select read only values** option.
8. Click **Save**.



Configuring the Agent Login settings

Perform the following steps after selecting the template to configure.

The system displays the Template Detail page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **Login - Agent**.
The system displays the Login - Agent page.
2. Makes the necessary changes to the fields.
3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
4. Click **Save**.



Configuring the IM Login settings

Perform the following steps after selecting the template to configure.

The system displays the Template Detail page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **Login - IM**.
The system displays the Login - IM page.
2. Makes necessary changes to the fields.
3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
4. Click **Save**.



Viewing Phone Numbers

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.

You can only view or specify the phone numbers that the agent has set to use as **Other Phone** for receiving calls. Phone numbers relate to a specific user, and can only be set in a **User** profile. To add a phone number, go to **Manage Users**, select a user, add or select a profile, and then edit the user profile to add the **Other Phone** configuration that the user can use.

Prerequisites

- The agent must add additional phone numbers to view the numbers on the page.



1. In the **Template Details** page, click **Phone Numbers**.

The system displays the **Phone numbers** window with phone numbers if an agent has added the phone number as Other Phone.

2. Select a number from the **Phone numbers** list.

The system displays the name and number in the **Phone name** and **Phone number** fields, respectively.

3. To prevent agents from adding their own phone numbers from the Avaya one-X® Agent user interface, select the **Select read only values** options.

As an administrator, you can add phone numbers by editing a user profile on the Manage Users page.

4. Click **Save**.



Configuring the Work Handling settings

These settings control how the agents must receive calls on the Avaya one-X® Agent client.



1. In the **Template Details** page, click **Work Handling**.

The system displays the Work Handling page.

2. Select the appropriate options to set the required work handling behavior.

3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.

4. Click **Save**.



Configuring the Audio Greetings settings

Agents can record prerecorded audio greetings as standard responses for specific clients or skills for which the template is developed. An agent can configure greeting triggers to play a specific audio greeting on receiving calls from specific numbers, VDNs, or Prompted Digits.

Prerequisites

- Agents must add a greeting to the system.

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **Audio Greetings**.
The system displays the Audio Greetings window.
2. Click **Add Audio Greeting** to define a new audio greeting.
The system displays the <new entry> file in a list format.
3. In the **Name** field, enter the audio greetings.
4. In the **Description** field, describe the audio greetings.
5. Make other changes to the fields.
6. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
7. Click **Save**.



Configuring the Screen Pop settings

Screen Pops are applications, Web pages, or information that the system displays to agents when a call arrives. Screen Pops can appear to an agent at a specified stage of the call, for example, while ringing, when answered, when missed, or when released.

You can also set Screen Pops to appear for outbound calls. The system triggers Screen Pops for incoming and outgoing calls for specific numbers and VDNs.



1. In the **Template Details** page, click **Screen Pop**.
The system displays the Screen Pop window.

2. Click **Add Screen Pop**.

The system displays a <new entry> Screen Pop in the list box.

3. To enable a screen pop for the current template, select **Enable selected Screen Pop for this profile**.
4. In the **Screen pop menu** field, enter a name for the screen pop.
5. In the **Address or URL of program** field, perform one of the following steps:
 - To open a remote application containing reference to a Web application as a screen pop, type a valid Web address, for example, type `http://www.mycompany.com/data?tel`.
 - To use a windows application as a screen pop, specify a valid directory path of a windows application, for example, type `C:\Program Files\Adobe\Acrobat 7.0\Acrobat\Acrobat.exe`.
6. In the **Command line parameters** field, add the parameter value. Each call can contain a called name (%n), number (%m), prompted digits (%p), VDN (%v), UUI (%u), Start time (%s), or Date (%d). For example, if you want the screen pop to start for a call originating from a VDN number, type `http://www.mycompany.com/data?tel=%v`.
7. To set a screen pop trigger for inbound calls, select one of the following options from the Inbound call:
 - Ringing
 - Answered
 - Missed
 - Released
8. To set a screen pop trigger for outbound calls, select one of the following options from the Outbound call:
 - Connected
 - Released
9. If you want the screen pop to start when an incoming call appears on a specific VDN, select the **Trigger only when VDN is** option and enter a VDN in the text box.

CAUTION: On Communication Manager, create VDNs that are not more than 15 characters long so that a VDN can match with multiple VDNs.
10. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
11. Click **Save**.



Configuring the Launch Application settings

You can set the applications that an agent can launch from the **Launch Application** icon on the Avaya one-X® Agent client interface. These applications can be important for accounts or skills for which the template is created.

IMPORTANT: While specifying the application path, ensure that you have stored the applications at the specified location across all Avaya one-X® Agent client systems.



1. In the **Template Details** page, click **Launch Applications**.
The system displays the Launch Applications window.
2. Click **Add Application**.
The system displays an <untitled> application.
3. In the **Application name** field, select the untitled application item and enter a name.
4. In the **File, folder, or URL to launch** field, enter the application file, folder path, or URL.
5. In the **Description** field, describe the application.
6. (Optional) Perform the following steps:
 - In the **Parameter to pass** field, enter additional values at the command line for the third-party application to be launched from the client interface.
 - In the **Default Directory** field, enter the default directory path to assign a default directory to execute a launch item from the client interface.
7. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
8. Click **Save**.



Configuring the Directory settings

Use Public Directory to gain access to a corporate or public directory services. The directory functions as a Lightweight Directory Access Protocol client (LDAPv2 or LDAPv3). You must create and configure the service with Avaya one-X® Agent to import or search a contact in the public directory (LDAP).

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **Directory**.
The system displays the Directory window.
2. Click **Add Directory**.
The system displays an untitled item in the directory list.
3. Makes necessary changes to the fields.
4. To mark all fields as read-only for Avaya one-X® Agent client users, select the

Select **read only values** option.

5. Click **Save**.



Configuring the Work Log settings

You can configure the system to save the work record types on the IM transcripts for IM interactions in Work Log.



1. In the **Template Details** page, click **Work Log**.
The system displays the Work Log window.
2. Makes necessary changes to the fields.
3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
4. Click **Save**.



Configuring the Voice Mail Integration settings

You can integrate the voice mail support with a template. The voice mail system is available to all the users who are assigned to the template and have the ability to send and receive voice mails.

The service is available only if an extension that a user is registered has a Message Waiting Light defined.

Prerequisites

- Voice Mail Integration is only available for those extensions that have a Communication Manager Message Waiting Lamp translated.

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.

You can associate the voice mail messages with a telephone, an application, or a Web browser.



1. In the **Template Details** page, click **Voice Mail Integration**.
The system displays Voice Mail Integration window.
2. In the **Voice Mail Integration** panel, make necessary changes to the fields.
3. To mark all fields as read-only for Avaya one-X® Agent client users, select the

Select read only values option.

4. Click **Save**.



Configuring the Reason Code settings

Following are the types of codes that agents can send to Communication Manager in conjunction with their work.

Code	Description
Agent Auxiliary Work Codes	Agents select from the set of codes to specify the reason they are entering the Auxiliary Agent state. For example, agents may be away to attend team meetings, trainings, for lunch, or other miscellaneous activities. You must ensure that you create codes for all practical reasons for which agents need to stay in auxiliary status.
Agent Logout Codes	Agents select from the Agent Logout Codes set of codes to provide reasons for logging out of Communication Manager CD. The user can stay connected, but not logged on to the ACD as an agent. For example, an agent might log out for end of shift, change of desks, medical emergency, and so on. While creating the Logout codes, you must anticipate the reasons for which agents can use a logout codes and create the logout codes accordingly.
Call Work Codes	Agents select the Call Work Codes to add to ACD tasks that describe details about the call in such a way through the codes that an enterprise can track the calls. The following examples are reported as digit strings to Communication Manager, similar to all the other types of codes: bad audio, unhappy customer, repeated calls from the customer for the same problem, or an agent needs assistance to resolve a customer problem.
Supervisor	Supervisors select codes from the Supervisor category to assign reasons at the supervisor level. You must anticipate supervisor activities while creating these codes and associated reasons.

You can create child code under each of the basic code category and each child group can have multiple child groups or codes. Ensure that you assign a unique code to each child group that you create.

NOTE: For traditional code entry, these codes must be numeric. The Avaya one-X® Agent client associates the names to these numeric codes to assist the agent in selecting the appropriate codes. The system sends only the numeric code assigned to each text string to Communication Manager and the reporting systems.

In Avaya one-X® Central Management, you can import codes from a CSV file by downloading the prescribed CSV format from the reason code example link on the Codes page. You can store the file locally and create codes and assign reasons under the relevant categories.

Subsequently, you can export the existing codes in the CSV format, edit the file, if required, and then import the CSV file again to update the existing codes.

Read the CSV file column descriptions on the Codes page and create codes accordingly. You must create correct parent child groups and codes so that agents get the correct code in the relevant category.

Importing Codes

You can import codes into a template from a properly formatted CSV file. An administrator can use this sample CSV file. These codes are made available to users who have profiles generated from the template, that is, users having the template assigned to them specifically or to any group to which the users belong.

Central administrators can only add and edit code content through the CSV file import mechanisms.



1. In the **Template Detail** page, click **Codes**.

The system displays the Codes windows.

2. To import codes, follow the instructions in the **Codes** panel and proceed to the next step.
3. Click **Browse** and locate the Unicode Text file you want to import.

After selecting the Unicode Text file, the path of the Unicode Text file appears in the File field.

4. Click **Import**.

The system imports the CSV file and displays the number of codes in Reason Code Counts.

NOTE: If you view a template that has inherited codes from another template, the Codes imported for the template show the number of inherited codes.

5. Click **Save**.



Configuring the Event Logging settings

Configure event logging to record event logs of various levels for Avaya one-X® Agent application.

NOTE: The event logging error and information relate to the Avaya one-X® Agent application. The logs are useful only for maintenance engineers.

Prerequisites

- Ensure that you know the various logging levels and the remote host

address where the logs must be logged.



1. In the **Template Details** page, click **Event Logging**.
The system displays the Event Logging window.
2. Select the appropriate **Logging level** and **Appender** from the lists. See the [Event Logging panel field descriptions on page 91](#) for more information.
3. In the **Remote host for central logging** field, enter the host name or IP address for central logging of event logs.
You can use the Remote host for central logging field only if Remote syslog logging is set up. If the Remote host for central logging field is blank, the system stores the error or event logs on the agent's computer.
4. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
5. Click **Save**.



Configuring the Outlook Contacts settings

You can import Outlook Contacts into the agent Avaya one-X® Agent Contact List. You can configure the Outlook Contacts to a template assigned to an agent or a group of agents or directly edit a user profile.

Prerequisites

- Obtain all the required credentials and location addresses.



1. In the **Template Details** page, click **Outlook Contacts**.
The system displays the Outlook Contacts window.
2. In the **Exchange Server Address** field, enter the Microsoft Outlook exchange server address.
3. In the **User Name** and **Password** fields, enter the exchange server user name and password, respectively.
4. In the **Domain** field, specify the exchange server domain name.
5. In the **Timeout** field, specify the time-out in seconds.
The system sets the time interval after which a search for contact expires.
6. Click **Save**.



Configuring the Dialing Rules settings

The dialing rules depend on the country and location of your Communication Manager. The dialing rules help the system to distinguish extensions from trunk calls, based on the length of the dialing string. The dialing rules ensure that the system uses the right Automatic Route Selection (ARS) code, and if needed, modifies the digits in keeping with Communication Manager and the PSTN requirements.

Avaya one-X® Agent 2.5 supports authorization and carrier code, which is mandatory in some countries. Dialing Rules is an optional feature used to prevent access to expensive telephony resources, often international calling, by unauthorized users.

You or an Avaya one-X® Agent user can enter an authorization code in a user profile, and the types of telephone calls that require the authorization. The Avaya one-X® Agent client automatically appends the authorization code as required so the user does not have to enter the authorization code each time a call is made.

Perform the following steps to configure the dialing rules for the selected template:



1. In the **Template Details** page, click **Dialing Rules**.
The system displays the Dialing Rules window.
2. In the **Number to dial to access outside line** field, specify the number to access an outside line. In North America, the number is set to 9. In Europe, the number is set to 0. For example, type 9 to access the outside line for agents located in North America.
3. In the **Your Country Code** field, specify the country code of Communication Manager. For example, type 1, for agents accessing Communication Manager from North America.
4. In the **Local Calling Area Codes** field, type the area or city code of Communication Manager. For example, type 785.
In regions that support multiple local calling area codes, enter the area codes as a comma-separated list. For example, type 305,720 to make local calls to both these area codes.
5. In the **Number to dial for long distance calls** field, type the long distance prefix number of Communication Manager. For example, type 1 for agent in North America.
6. In the **Number to dial for international calls** field, enter the prefix that is required by your country for international calls. For example, type 011 for agents in North America.
7. In the **Extension Length for internal extension calls** field, type the length of the internal extension calls. If you specify the multiple extension lengths, the Avaya one-X® Agent client on the agent's desktop performs the exact matches. When you assign the length of the internal extension number, the Avaya one-X® Agent client treats the dialed number consisting of the selected number of digits as an internal extension.
Communication Manager can have multiple length extension numbers. For example, if your company supports internal three-digit, five-digit, and seven-digit extensions, type 3, 5, and 7. You must use a comma to separate the values.
8. In the **Length of national phone numbers (including City/Area code)** field,

type the length of the national long distance number. The number must also include the code used to identify a city or an area. For example, type 10, for agents in North America.

If agents are accessing Communication Manager, where the region supports variable national phone numbers, specify the length of the valid telephone numbers as a comma separated list. For example, if the region supports both telephone numbers with 10-digit and 11-digit telephone numbers, type the values as 10, 11.

9. Select **Include area/city code when making a local call**, if you want the system to prefix the area code with a number when an agent makes a local call. For example, if an agent dials a telephone number, the system prefixes the area code number defined in the Local Calling Code field and dials the telephone number.
10. Select **Add long distance prefix on local calls**, if you want the system to prefix the area code before an agent makes a local call. For example, if an agent dials a local telephone number, the system prefixes a long distance code number defined in the Number to dial for long distance calls field, and dials the local telephone number.
11. Select **Display confirmation window before dialing a number**, if you want the system to confirm before the agent dials the number.
12. In the **Time Period of Pause (Comma) in dialing (in seconds)** field, specify the period for each comma character in the dialing field before dialing the next digit. By default, the value is set to 2 seconds. You can specify any value between 1 to 10 seconds.
13. To define authorization and carrier code, perform the following steps:
 - a. Select the **Enable authorization code** option to enable an authorization code.
 - b. In the **Authorization code** field, type an authorization code for the corresponding profile. Authorization codes are administered in Communication Manager.
 - c. If you want an agent to make an external call using authorization and carrier code, select one or all of the following options, as appropriate:
 - To make local calls using authorization code, select **On local calls**.
 - To make national long distance calls using authorization code, select **On national long distance calls**.
 - To make international calls using authorization code, select **On international long distance calls**.
14. To make all fields read-only for the user, select the **All on this page** option.
15. Click **Save**.



Configuring the Touch Tone Shortcuts settings

The Touch Tone shortcuts are available to the agents on their **Dialpad** window. Perform the following steps to configure how the touch tone shortcuts must appear on the Avaya one-X® Agent client.



1. In the **Template Details** page, click **Touch Tone Shortcuts**.
The system displays the Touch Tone Shortcuts window.
2. Click **Add Shortcut**.
The system displays an untitled shortcut on the Touch Tone Shortcuts list.
3. In the **Name** field, select an untitled shortcut and type a name.
4. In the **Number** field, enter the associated telephone number.
5. Repeat Step 2 through Step 4 to create multiple Touch Tone Shortcuts.
6. Select the read-only values option to mark all fields as read only for the agent.
7. Click **Save**.



Configuring the Video - Basic settings

You can configure the basic video permissions, such as, enabling or disabling agents from using the video calls. In addition, you can set the default behavior of the video window for agents making or receiving a call.

Prerequisites

- The agent must have a Web camera.
- The agent must enable the Video support during the client installation.

Perform the following steps after selecting the template to configure. The system displays the Template Detail page. The system displays a Revert icon next to each field when you change the field value and resets the field to the previous value when you click the Revert icon.



1. In the **Template Details** page, click **Video - Basic**.
The system displays the Video-Basic window.
2. Select the appropriate options based on the following descriptions:

Options	Description
Enable video calls	Enables the video call feature on the Avaya one-X® Agent client. The Enable video calls option is available for users of the profile or template where video is administered.
Broadcast video	Starts the video broadcast immediately after the agent accepts the call on the Avaya one-X® Agent client.
Close video window	Closes the video window immediately after the agent ends the video call on the Avaya one-X® Agent client.
Open video window	Opens the video window in the preview mode automatically when the agent logs on to the Avaya one-X® Agent client.

Options	Description
Allow playing video	With this option, an agent can share a video file on the video file session on the Avaya one-X® Agent client.

3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
4. Click **Save**.



Configuring the Video - Advanced settings

The configuration set for the video template is available to all agents assigned a video template.

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **Video - Advanced**.
The system displays the Video - Advanced window.
2. Configure the video settings.
3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
4. Click **Save**.



Configuring the IM settings

You can configure an IM message that is sent as a greeting message when an agent begins an IM session. In addition, this section also explains how you want the system to alert an agent for an incoming IM request.

Prerequisites

- Presence Services must be a part of the server installation for contact center.

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **IM - Settings**.
The system displays the Instant Messaging - Settings window.
2. Select the appropriate options from the following fields:

Options	Description
Display main window	Displays the Avaya one-X® Agent main application window with an incoming IM request on the Avaya one-X® Agent client.
Display IM window	Displays the IM window with the incoming message on the Avaya one-X® Agent client.
Flash icon	Flashes the Avaya one-X® Agent icon on the task bar for an incoming IM request on the Avaya one-X® Agent client.
Greeting	Configures an automated greeting response for the template. When an IM session starts, the system sends the pre-configured message to the other participant on IM window.
Show IM status as "Away" after	Sets the agent's IM status to Away when there is no action on the desktop from the time interval specified in the Show IM status as "Away" after field.

3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
4. Click **Save**.



Configuring the IM Responses settings

The text you define here serves as a commonly used response that the agents can use. You can customize the responses for specific skills or clients for which the template is created. Conversely, you can also view the responses that agents have set if you allow agents to modify the field.

Prerequisites

- Install Presence Services to use Instant Messaging and related settings.

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **IM - Responses**.
The system displays the Instant Messaging - Responses window.
2. Click **Add Response**.
The system displays a <new entry> text.
3. In the **Response** field, rename the IM response.

4. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
5. Click **Save**.



Configuring the TTY - General settings

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **TTY- General**.
The system displays the TTY - General window.
2. In the **Greeting** field, enter the greeting message and suffix with the abbreviation GA. For example, to greet a TTY caller with a Good Morning message, in the Greeting field, type Good Morning — GA.
3. Select the **Always show TTY button in voice interaction** option if you want the agent desktop to display the TTY button for every call.
4. Select the **Show TTY window on every voice call** option if you want the system to invoke the TTY window for every incoming call to an agent.
5. Select the **Show TTY window when a call comes for a number listed** option if you want the system to display the TTY only for calls originating from the specified numbers in the panel, and perform the following steps:
 - a. Click **Add Phone Number**.
The system displays a new entry in the TTY panel.
 - b. In the **Phone number** field, click the new entry and type a telephone number.
 - c. Select the new entry field.
The system adds the number to the TTY panel list.
 - d. Repeat steps a through c to add multiple TTY numbers.
6. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
7. Click **Save**.



Configuring the TTY- Abbreviations settings

Central Management provides a set of pre-defined abbreviations that are commonly used during a typical TTY interaction in North America. Since the abbreviations are standard for TTY interactions, you cannot modify the standard abbreviations.

Perform the following steps after selecting the template to configure. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **TTY - Abbreviations**.
The system displays the TTY - Abbreviations window.
2. Click **Add TTY abbreviation to add a new abbreviation**.
The system displays a new entry in the abbreviations list.
3. Select the blank new entry and configure the following details:
 - a. In the **Short Key** field, enter the abbreviation.
 - b. In the **Meaning** field, enter the meaning of the abbreviation.
 - c. In the **Literal Meaning** field, enter the expansion of the abbreviation.
Literal Meaning can be a literal text to derive the abbreviation. For instance, the short form for Be Right Back can be BRB and Go Ahead can be GA.
 - d. In the **Description** field, enter additional information, if any. You can repeat step 3 to add multiple abbreviations.
4. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
5. Click **Save**.



Configuring the Call Handling settings

You can configure certain call handling settings for agents. These include, transferring calls, adding participants to a conference, or putting a call on hold when switching between two or more calls. You can also control the incoming call settings.

Perform the following steps after selecting the template to configure. The system displays the Template Detail page and a Revert icon next to each field when you change the field value. The system resets the field to the previous value when you click the Revert icon.



1. In the **Template Details** page, click **Call Handling**.
The system displays the Call Handling window.
2. Configure the call handling settings.
3. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
4. Click **Save**.



Configuring the User Interface settings

You can set options to change features of the user interface for an agent.

Perform the following steps after you select the template to configure User Interface settings. The system displays the **Template Detail** page. The system displays a **Revert** icon next to each field when you change the field value and resets the field to the previous value when you click the **Revert** icon.



1. In the **Template Details** page, click **User Interface**.
The system displays the User Interface window.
2. Configure the User Interface settings.
3. In the **Number of entries per screen** field, specify the number of work log entries that the Work Log window must display on the agent desktop.
4. To mark all fields as read-only for Avaya one-X® Agent client users, select the **Select read only values** option.
5. Click **Save**.



Chapter 8: Managing contacts

With Contact lists, you can add a group of related contacts to one or more agent or supervisors contact list. You can create any number of contact lists in Central Management.

You can create contact lists based on the business type, account, or any other category. Contact list stores the name, telephone numbers, and address of each contact. You can also tag a contact to the favorite list or add to the speed dial list. When you assign a contact to a template, the contact lists appear in the Contact List column corresponding to the template name in the Manage Templates page. You can point the mouse in the Contact List column in the template name to view all the contact lists to the template in the tool tip text. Similarly, all the users assigned to the same template can view the contacts in the Contact List window of their respective Avaya one-X® Agent application.

You can import multiple contacts into the same contact lists in Central Management. You can also import various other contact details with the contact names, which appear on the Avaya one-X® Agent client Contact List window. With the bulk import feature, you save the effort and time required for adding individual contact to the contact list.

This chapter includes:

- [Importing multiple contacts on page 69](#)
- [Adding a contact list on page 72](#)
- [Adding members to contact list on page 72](#)
- [Editing contact list member details on page 73](#)
- [Deleting contact list members on page 73](#)
- [Attaching contact list to templates on page 74](#)
- [Filtering and sorting the contact list table on page 75](#)
- [Detaching a contact list from a template on page 75](#)

Importing multiple contacts

You can import multiple contacts into an existing contact list in Central Management. Importing multiple contacts saves the time and effort required to add individual contact with the contact details to the contact list. The system displays the new contact in the Contact List window of the Avaya one-X® Agent client user interface.

To import multiple contacts, the contacts and the respective contact details must be in a Unicode Text file in the specified sequence. You can download a sample CSV file from the example link on the Import Contacts page of Avaya one-X® Agent Central Management and save the file as a Unicode Text file. If you have an earlier CSV file with data, you can save the file as a Unicode Text file and import in Central Management.

TIP: You can create templates that you plan to assign to the contacts before importing contacts. By doing so, you can add template names in the Unicode Text file and save your time and effort of assigning templates after import. You can configure or edit templates later.

Prerequisites

- The contact lists to which you are adding contacts must exist in Central Management.

- To import contacts, you must save the contact names and other related details in a tab-delimited file. If the contacts CSV file does not exist, perform the following steps:
 - a. Open the **Import Contact** page from the Central Management navigation menu.
 - b. Click the **example** link and export the file to your computer.
 - c. Open the **contactexample.csv** file, and enter the details in the following order of column headings:

Column names	Column values
List Name	Enter the name of the contact list in Central Management to which you want to add the contact. You must specify the exact contact list name in the List Name column. If the contact list name that you specify does not match the name in Central Management, the system does not add the contact to the contact list.
First Name	Enter the first name of the contact.
Last Name	Enter the last name of the contact.
Favorite	• Type Y or Yes if you want to set the contact as a system-wide favorite. • Type N or No if you do not want the contact to be set as a favorite.
Speed Dial	• Type Y or Yes if you want the contact to be set as system-wide speed-dial. • Type N or No if you do not want the contact to be set as a speed-dial.
Work	Enter data in the two columns of Work. The first column specifies the work number and the second specifies if the work number must appear on speed-dial. In the first column, type the work phone number. In the second column, do one of the following: • Type Y or Yes if you want the contact work number to be on a speed-dial. • Type N or No if you do not want the contact work number to be on a speed-dial.
Home	There are two columns for home. The first column specifies the home phone number and the second specifies if the home number must appear on speed-dial. In the first column type the home phone number. In the second column, do one of the following: • Type Y or Yes if you want the contact home number to be on a speed-dial. • Type N or No if you do not want the contact home number to be on a speed-dial.
Mobile	There are two columns for mobile. The first column specifies the mobile number and the second specifies if the mobile number must appear on speed-dial of the agent's desktop. In

Column names	Column values
	the first column type the mobile number. In the second column, do one of the following: - Type Y or Yes if you want the contact mobile number to be on a speed-dial. - Type N or No if you do not want the contact mobile number to be on a speed-dial.
Email	Enter the email address of the contact.
IM	There are two columns for internet messaging (IM) login name. The first column specifies the IM login name. In the second column, do one of the following: - Type Y or Yes if you want the contact IM login name to be on a speed-dial. - Type N or No if you do not want the contact IM login name to be on a speed-dial.
Company	Enter the company name of the contact.
Address	The Address heading has two columns. Enter the address for the contact in the Address 1 and Address 2 columns.
City	Enter the city name of the contact.
Zip Code	Enter the zip code of the contact.
Country	Enter the country name of the contact.

You must fill the First Name and Last Name for each contact. Central Management will ignore any other blank columns in the contact details.

- d. Save the file with a different name.

NOTE: While saving the file, ensure that you save the file with a .csv extension.

CAUTION: Do not delete or overwrite the header row of the tab-delimited file when you add data to the file.

Perform the following steps to import multiple contacts saved in the Unicode Text file. Ensure that the data and structure of the Unicode Text file complies with the guidelines.



1. Click **Import Contacts** from the Central Management navigation menu.
2. In the **File** field, enter the Unicode Text file path or locate the tab-delimited file by clicking **Browse**.
3. Click **Import** to import users listed in the Unicode Text file.

The system imports the contacts to Avaya one-X® Central Management.



Adding a contact list



1. On the Central Management navigation menu, click **Manage Contact Lists**.
The system displays the Manage Contact Lists page.
2. Click **Create contact list**.
The system displays the Contact List Details page at the bottom of the page with the following tabs:
 - Contact list details tab
 - Members tab
 - Templates tab
3. In the **Contact list details** tab, enter the list name in the **Contact list name** field and click the **Add contact list member** link. The Contact list name is a mandatory field.
4. Click **Save**.
The system displays the new contact list in the Contact list name column.



Adding members to contact list



1. On the Central Management navigation menu, click **Manage Contact Lists**.
The system displays the Manage Contact Lists page.
2. Click a contact list name to which you want to add members.
The system displays the Contact List Details page at the bottom with the following tabs:
 - Contact list details tab
 - Members tab
 - Templates tab
3. Click the **Members** tab.
The system displays the member list.
4. Click the **Add contact list member** link.
The system displays the Contact Details window.
5. In the **Contact Details** window, enter the appropriate contact details. The **Last name (or Company)** field is mandatory while adding a contact.
6. Select the **Favorites** option to save the contact to agent favorites.

7. Select the **Speed Dial** option and select the appropriate voice number option to save the contact to the agent speed dial lists.

8. Click **Save**.

The system displays the newly added member in the Members tab. To add new members to the list, Repeat from step 4 through step 8.

9. Click the **Templates** tab, and perform the following steps:
 - a. From the **Template name** drop-down list, select a template and click **Add** from the **Add/Remove** column.
The system displays the new template in the template list.
 - b. Click the **Template settings** link to view the template settings corresponding to the assigned template in the view column.
The system displays a new window with the template settings.
10. Click **Save**.



Editing contact list member details



1. On the **Central Management navigation** menu, click **Manage Contact Lists**.
The system displays the Manage Contact Lists page.
2. Click the **Contact List Name** option to which you want to add members.
The system displays the Contact List Details at the bottom with the following tabs:
 - Contact list details tab
 - Members tab
 - Templates tab
3. Click the **Members** tab.
4. From the member list, click the member name for which you want to make changes.
The system displays the corresponding member details in the Contact Details window.
5. In the **Contact Details** window, make the necessary changes.
6. Click **Save**.



Deleting contact list members



1. On the **Central Management navigation** menu, click **Manage Contact Lists**.
The system displays the Manage Contact Lists page.
2. Click the contact list name to which you want to add members.
The system displays the Contact List Details page at the bottom with the following tabs:
 - Contact list details tab
 - Members tab
 - Templates tab
3. Click the **Members** tab.
The system displays the Members tab with the member list.
4. Click the **Delete** button corresponding to the member name.



Attaching contact list to templates

Prerequisites

You must create templates before you create contact lists. By doing so, you can assign contact lists to existing templates.

The child template automatically inherits the contact list attached to a parent template. In addition, the users or user groups assigned with the same parent or child template can view the contact list attached to the template in their respective **Contact List** window of Avaya one-X® Agent user interface.



1. On the **Central Management navigation** menu, click **Manage Contact Lists**.
The system displays the Manage Contact Lists page.
2. Click the contact list name to which you want to add members.
The system displays the Contact List Details page at the bottom with the following tabs:
 - Contact list details tab
 - Members tab
 - Templates tab
3. Click the **Templates** tab.
4. Select a template from the Template name drop-down list, and click **Add**.
The contact list applies to the selected template.
In the Template tab:
 - With the **Template settings** link, you can view the template settings to which the contact list is attached. The system displays the template settings in a separate popup window. However, you cannot edit the

template in the pop-up window.

- The **Manage Templates** link opens the Manage Templates page to check the template hierarchy and the templates that inherit the contact list, in addition to the one that you have attached.

The system displays the attached contact list in the Contact lists column corresponding to the template name in the Manage Templates page.

If the contact list names exceed the column width, you can adjust the Contact lists column for the template name to view the contact list names in the tool tip.



Filtering and sorting the contact list table

You can find the contact list based on the contact list name and sort by name or date modified in the ascending and descending order.



1. On the Central Management navigation menu, click **Manage Contact Lists**.
The system displays the Manage Contact Lists page.
2. To find a contact list by name, type the keywords in the **Filter** field.
The system displays all names matching the keyword in the contact list.
3. To find a contact list by template, select a template from the **By template** list.
The system displays all templates matching the keyword dynamically in the contact list.
4. To sort the list, perform one of the following steps:
 - To sort by contact list name, click the **Contact list name** column header.
The list toggles between an alphabetical ascending and descending order.
 - To sort by date, click the **Last modified** column header.
The list toggles between a date-wise ascending and descending order.



Detaching a contact list from a template

You can detach a contact list from all parent templates and user groups associated with the template.



1. On the **Central Management navigation** menu, click **Manage Contact Lists**.
The system displays the Manage Contact Lists page.

2. Click the contact list name to which you want to add members.

The system displays the Contact List Details page at the bottom with the following tabs:

- Contact list details tab
- Members tab
- Templates tab

3. Click the **Templates** tab.

4. Click the **Delete** button to detach the corresponding template.

The system detaches the template from the associated contact list.



Chapter 9: Authentication modes and LDAP integration

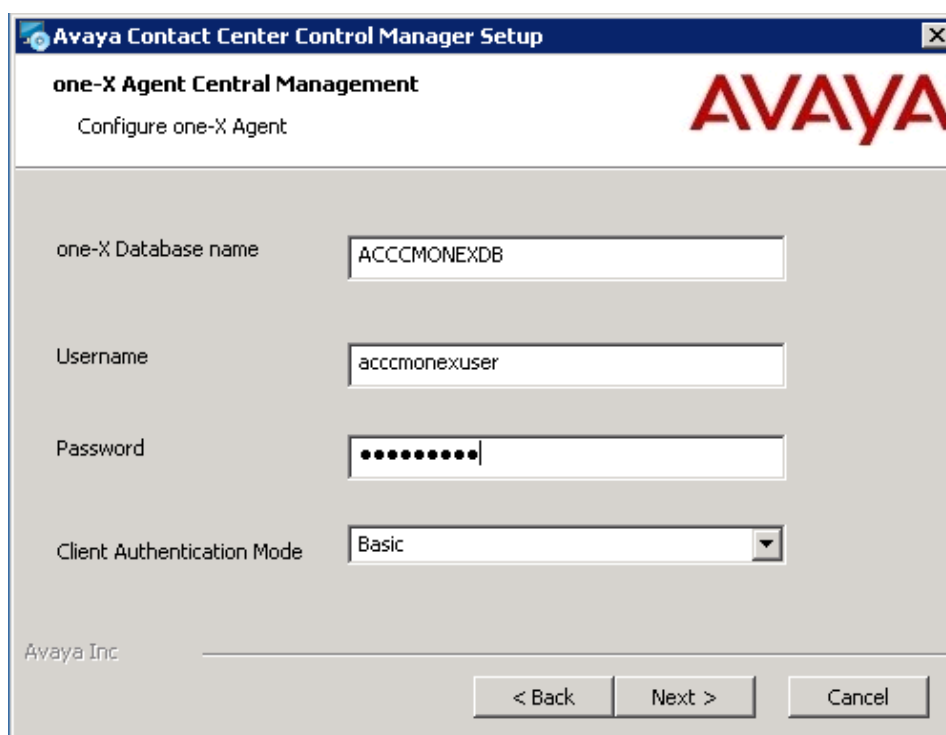
This chapter includes:

- [Standard Authentication on page 77](#)
- [LDAP Root on page 79](#)
- [LDAP Credentials – Mixed Authentication on page 82](#)

Standard Authentication

With the ACCCM installation wizard, you can select the required authentication method as part of the installation process.

The Client Authentication Mode fields include a Basic value that represents a standard authentication. It performs with the Avaya one-X® Agent user name and password. The system stores information in the ACCCM database.

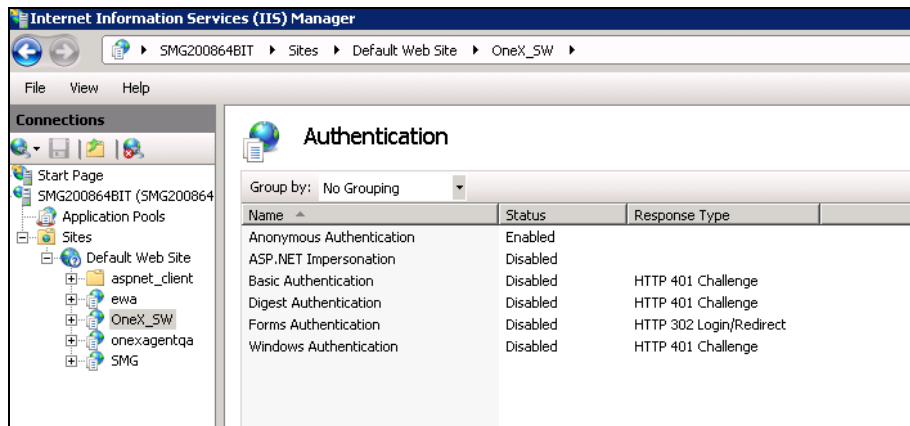


The screenshot shows the 'Avaya Contact Center Control Manager Setup' window, specifically the 'one-X Agent Central Management' section. The window title is 'Avaya Contact Center Control Manager Setup'. Below the title bar, it says 'one-X Agent Central Management' and 'Configure one-X Agent'. The Avaya logo is in the top right corner. The main area contains four fields: 'one-X Database name' with the value 'ACCCMONEXDB', 'Username' with the value 'acccmonexuser', 'Password' with masked characters '.....', and 'Client Authentication Mode' with a dropdown menu set to 'Basic'. At the bottom left is 'Avaya Inc' and at the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

To support this type of integration, the ACCCM installer configures the system as follows:

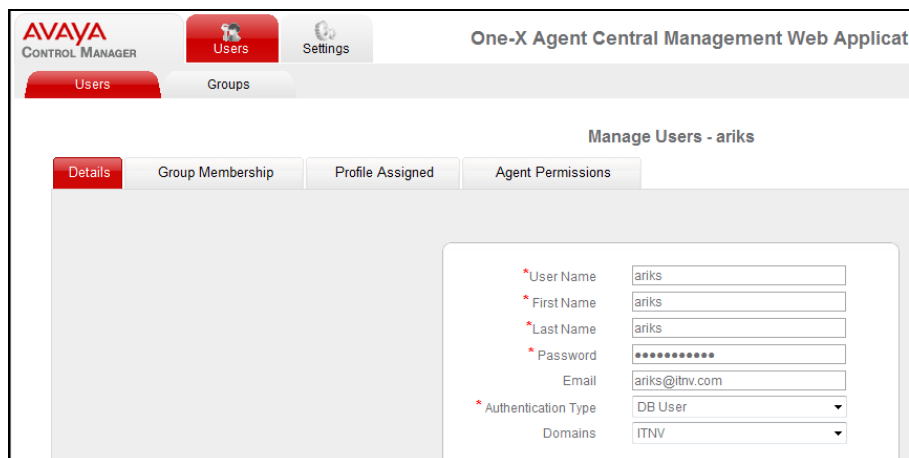


1. The ACCCM Avaya one-X® Agent central management website configuration service called ACCCMONEXCFG is configured to support anonymous access. The following figure illustrates the configuration of the configuration service website. This configuration is available in the installer.



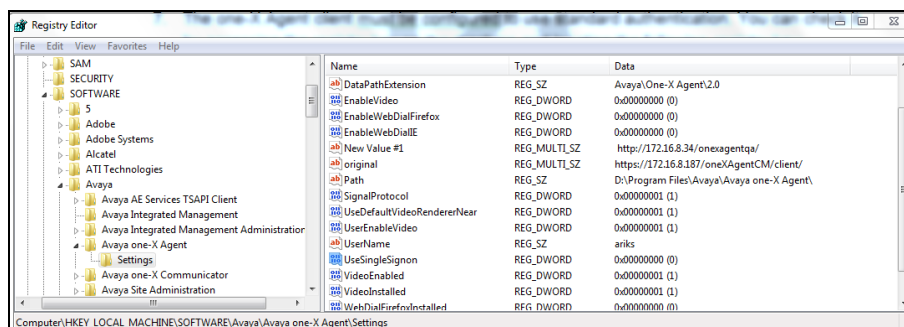
- The ACCCM Avaya one-X® Agent configuration services website files that are installed on the Web server machine including a configuration file called web.config. The installer updates the web.config configuration file.
- The web.config file includes a parameter called LoginType. The LogType parameter represents the type of authentication that the configuration service uses.
- The parameter must be set to the value of **Basic**.

```
<add key="LogInType" value="Basic"/> <!--Basic / NTLM-->
```
- You must configure the Avaya one-X® Agent user record that in the Avaya one-X® Central Management application to use the DB Only authentication mode.



- You must configure the Avaya one-X® Agent client to use the standard authentication. You can check authentication by accessing the registry key on the server and locating the following registry key:

UseSingleSignon = 0



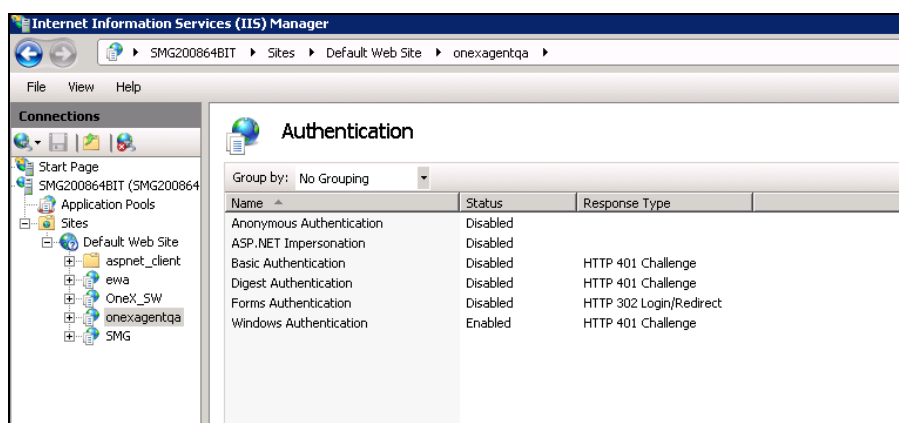


LDAP Root

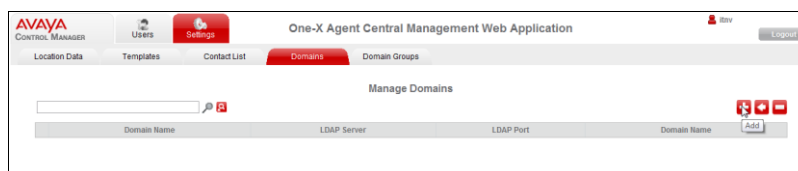
To support the LDAP Root – SSO integration, the ACCCM installer configures the system as follows:



1. The website of the ACCCM Avaya one-X® Agent Central Management configuration service (called ACCCMONEXCFGSSO) is configured to support only Windows Authentication.



2. The ACCCM Avaya one-X® Agent configuration services website files that are installed on the Web server including a configuration file called web.config that is updated by the installer.
3. The web.config file includes a parameter called “LoginType” that represents the type of authentication used by the configuration service.
4. The parameter must be set to the value of “NTLM”
`<add key="LogInType" value="NTLM"/> <!--Basic / NTLM-->`
5. Configure the domain in the ACCCM Avaya one-X® Agent Management. To configure the domain, perform the following steps:
 - a. Log in to ACCCM website as an administrator and select **Settings > Domain**
 - b. Click the add domain button.



The system displays the following page:

Manage Domains

Domain Name*	
LDAP Server*	
LDAP Port*	
LDAP Search Root*	
User Name*	
Password*	

- c. In the **Domain Name** field, type the name of the domain, for example, *ITNV*.
 - d. In the **LDAP Server** field, type the name of the LDAP server, for example, *itnvqa01.itnvqadomain.itnv.com*.
 - e. In the **LDAP Port** field, type the port number that is used by the LDAP source. The port number is either 389 or 636 (secure LDAP).
 - f. In the **Search Root** field, type the LDAP structure, where the ACCCM configuration service searches for the user, for example, *OU=OneX,DC=itnvqadomain,DC=itnv,DC=com*.
 - g. In the **Username** field, type the domain user that is used for the integration of the ACCCM configuration service and your domain. This user must have full read access rights on the LDAP tree.
 - h. In the **Password** field, type the user's password domain user that is used for the integration of the ACCCM configuration service and your domain. This user must have full read access rights on the LDAP tree.
 - i. Click **Save**.
6. The Avaya one-X® Agent user record that is created in the central management application must be configured to use the “LDAP Root” authentication mode and mapped to the domain we created in the previous step.

AVAYA
CONTROL MANAGER

Users Settings

One-X Agent Central Management Web Application

Users Groups

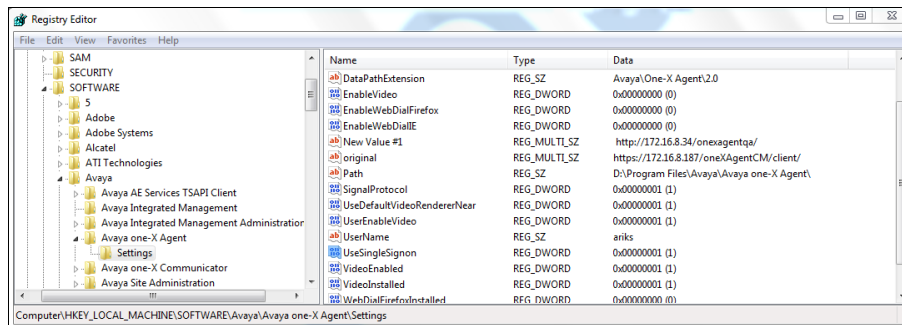
Manage Users - ariks

Details Group Membership Profile Assigned Agent Permissions

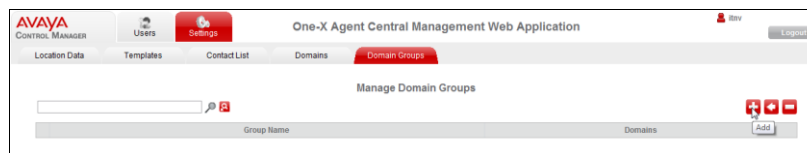
* User Name	ariks
* First Name	ariks
* Last Name	ariks
* Password	*****
Email	ariks@itnv.com
* Authentication Type	LDAP Root
Domains	ITNV

Contact Center Roles

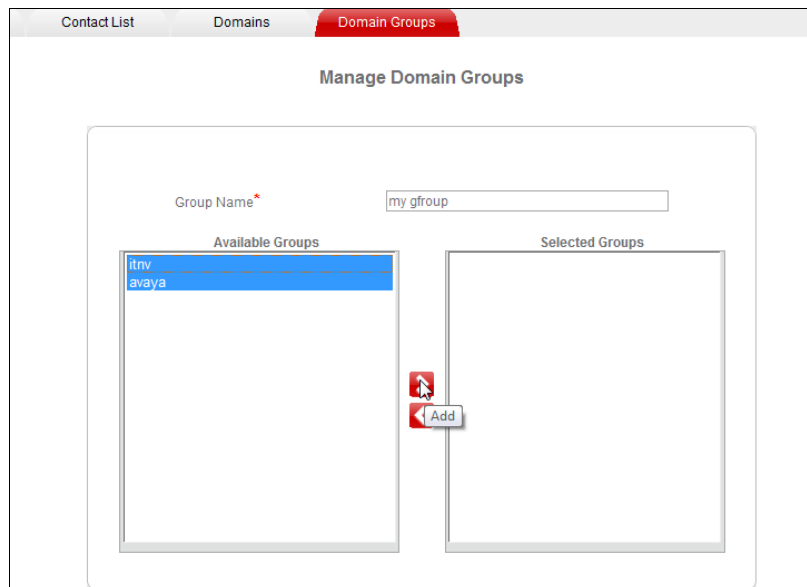
7. The Avaya one-X® Agent client must be configured to use SSO. You can check the configuration by accessing the registry key on the machine and locating the following registry key: UseSingleSignon = 1



8. You also must ensure that the ACCCM Server is a member of the domain that is used for the SSO process. If the server is not part of the domain, then the system cannot process the authentication.
9. To authenticate the user with a group of LDAP sources, create a domain group. Perform the following steps to create a domain group:
 - a. Create a domain group by navigating to the **Settings > Domain Group** tab.
 - b. Log in to ACCCM website as an administrator and select **Settings > Domain Group**.
 - c. Click the add domain button.



The system displays the following page:



- d. Enter the group name. To assign the relevant domains to the group, select WHAT and click **Add**.
- e. Assign the Avaya one-X® Agent user to the domain.

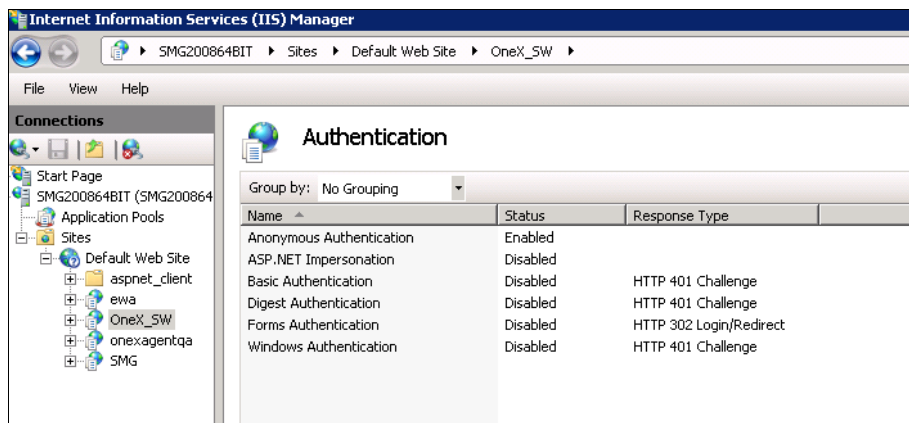


LDAP Credentials – Mixed Authentication

To support the LDAP Credentials in Mixed Authentication integration, the ACCCM installer configures the system as follows:

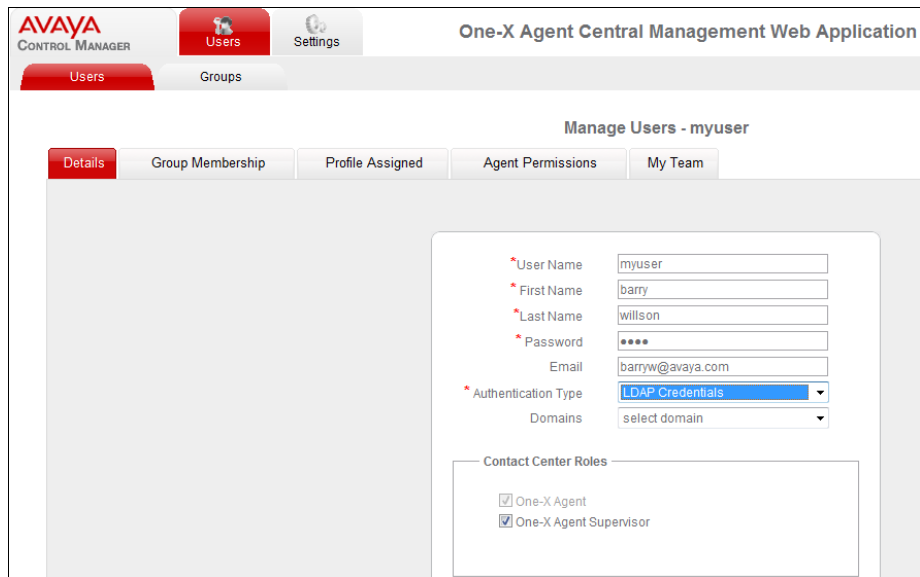


1. The website of the ACCCM Avaya one-X® Agent central management configuration service called **ACCCMONEXCFG** is configured to support only Anonymous Authentication.

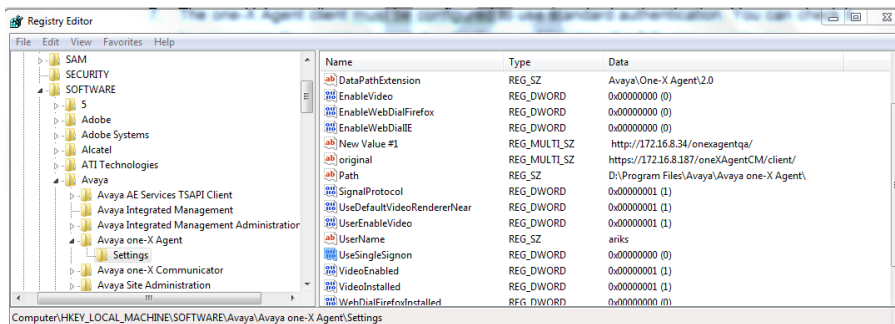


2. The ACCCM Avaya one-X® Agent configuration services Web site files that are installed on the Web server machine include a configuration file called web.config that is updated by the installer.
3. The web.config file includes a parameter called "LoginType" that represents the type of authentication used by the configuration service.
4. The parameter needs to be set to the value of "Basic"

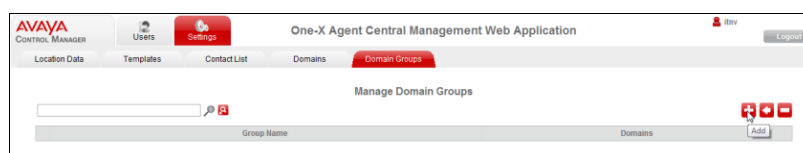

```
<add key="LogInType" value="Basic"/> <!--Basic / NTLM-->
```
5. The Avaya one-X® Agent user record that is created in the Central Management application must be configured to use the **LDAP Credentials** authentication mode.



6. You must configure the Avaya one-X® Agent client to use the standard authentication. You can check authentication by accessing the registry key on the server and locating the following registry key: UseSingleSignon = 0



7. You must also ensure that the ACCCM Server is a member of the Domain that is used for the Single Sign On process. If the server cannot be a part of the Domain, then the system cannot process the authentication.
8. To authenticate the user with a group of LDAP sources, you must create a domain group. Perform the following steps to create domain group:
 - a. Create a domain group by navigating to the **Settings > Domain Group** tab.
 - b. Log in to ACCCM website as an administrator and select **Settings > Domain Group**
 - c. Click the add domain button.



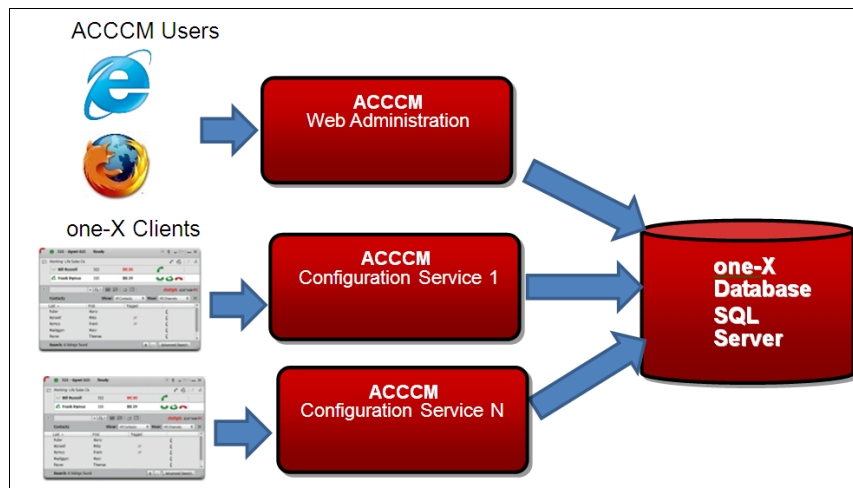
The system displays the following page:

- d. Enter the group name and assign the relevant domains to the group by selecting them and clicking **Add**.
- e. Assign the Avaya one-X® Agent user to the domain.



Chapter 10: Installing multiple configuration services

In a multi server environment, you can deploy as many Avaya one-X® Agent Configuration Services that you need. The central database server hosts the Avaya one-X® Central Management database. Use the multi server configuration in the High Availability mode for the Avaya one-X® Central Management feature.



By default, the ACCCM installation wizard installs a single Configuration Service. You can install the configuration service in the different authentication modes supported by ACCCM Avaya one-X® Agent administration.

Perform the following steps to install additional configuration services:



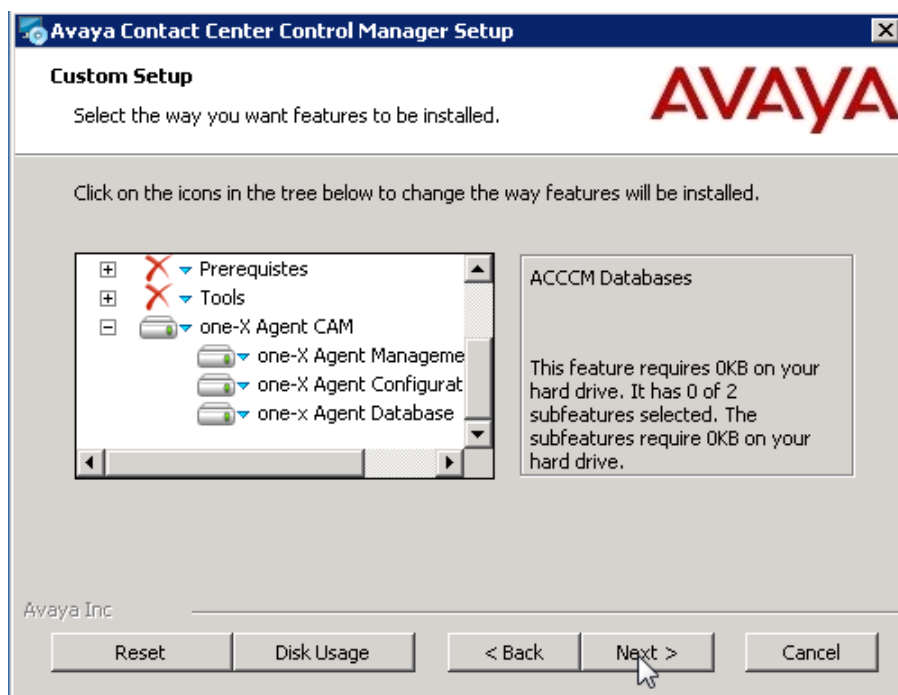
1. Open the ACCCM installation wizard.

The system displays the following screen:



2. Click **Next**.

The system displays the following screen:



3. Click **Next**.

The system displays the following screen:

Avaya Contact Center Control Manager Setup

SQL Database

Configure SQL Connection to your SQL Server

AVAYA

Server: accm61qa1

Port: 1433

Username: sa

Password:

ACCCM DB: accmavp

Avaya Inc

< Back Next > Cancel

4. In the SQL Database window, perform the following steps:

- a. In the **Server** field, enter the host name or the IP address of the server that hosts SQL Server.

By default, the system uses the host ACCCM server address. If you are using a database instance, enter the instance name. For example, enter the database name as **accmServer\sqlinstance**.

NOTE: The ACCCM default SQL Server installation does not install a special instance. Therefore, the value must be the server name or the IP address.

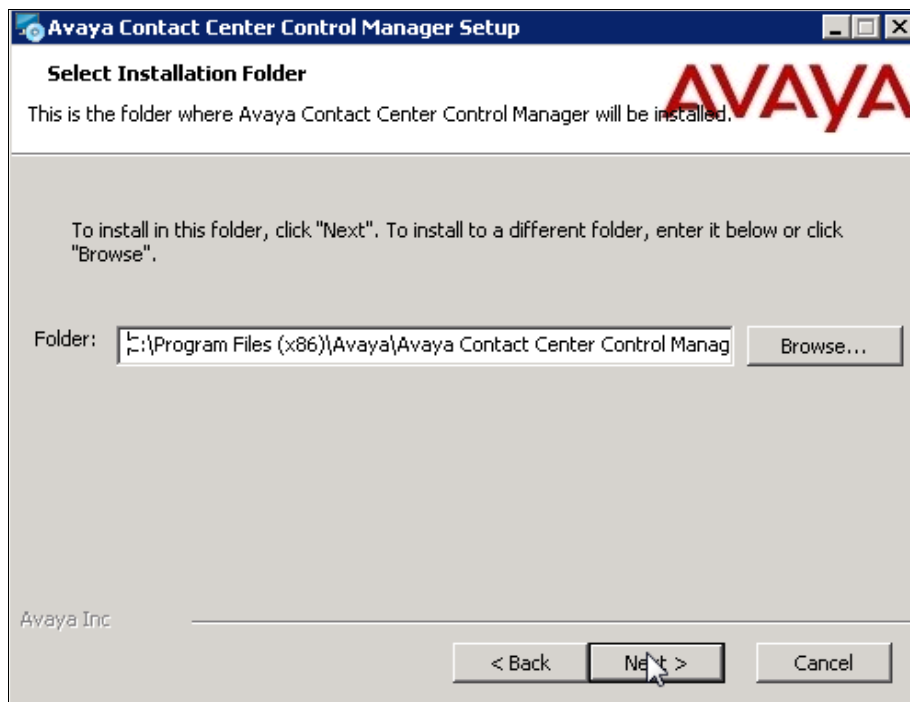
- b. In the **Port** field, enter the port number of SQL Server. The SQL Server uses **1433** as the default port.
- c. In the **Username** field, enter the database user name that is used for connecting to SQL Server.

You must use **SA** as the username. If you do not have the SA user, you must use a user that has dbo access rights on the master database.

- d. In the **Password** field, enter the password of the user.
- e. In the **ACCCM DB** field, enter the name of the ACCCM DB, that is, the original database you created for the ACCCM application. By default, the value is ACCCM.

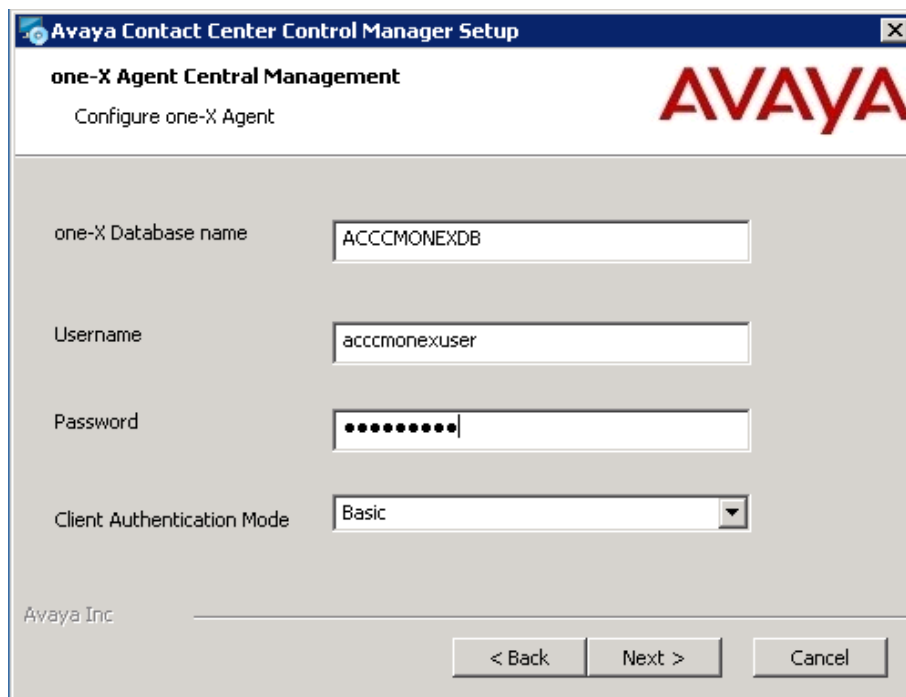
5. Click **Next**.

The system displays the following screen



6. Browse to the location where you want to install the Avaya one-X® Agent components and click **Next**.

The system displays the following screen:

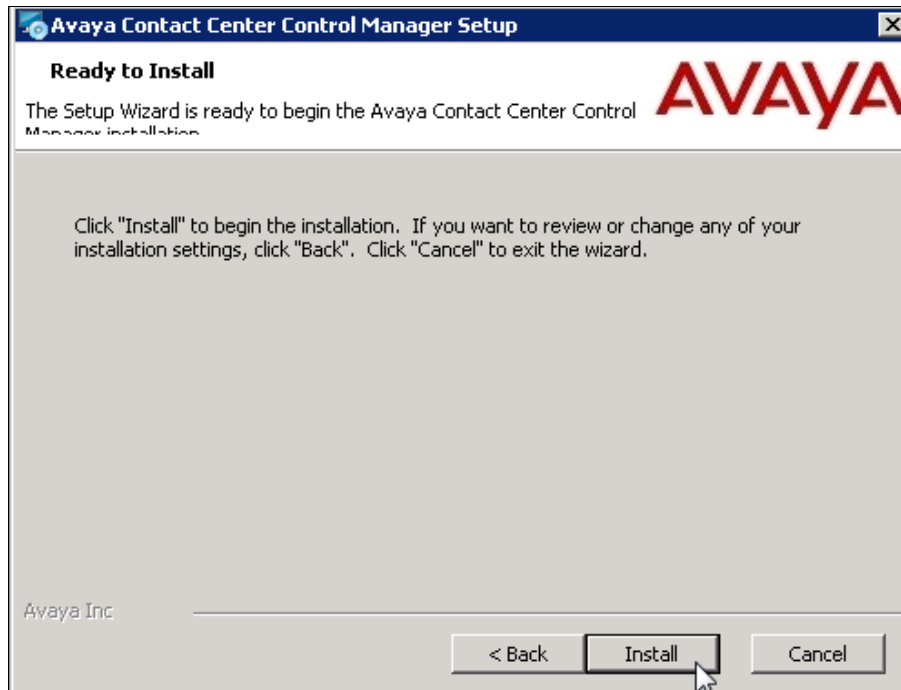


7. In the one-X Agent Central Management window, perform the following steps:
 - a. In the **one-X Database name** field, enter the name of the Avaya one-X® Central Management database that will be created as part of the installation.
By default, the database name is **ACCCMONEXDB**.
 - b. In the **Username** field, enter the name of the Avaya one-X® Central Management database user. By default the user name is

acccmonexuser.

- c. In the **Password** field, enter the password of the database user.
 - d. From the **Client Authentication Mode** drop-down list, choose the authentication type. The authentication type corresponds to the type of authentication used by the Avaya one-X® Agent clients. You can use two types of authentications:
 - **Basic:** The Basic authentication type uses the username and password to validate the one-X Agent database.
 - **SSO:** The Single Sign-On (SSO) authentication authenticates with the active directory.
 - e. From the **Version** drop-down list, choose the appropriate version of one-X Agent. The available options are 2.0 and 2.5.
8. Click **Next**.

The system displays the following screen:



9. Click **Install** to complete the installation.



Chapter 11: Integrating the Avaya one-X® Central Management portal with ACCCM

The ACCCM system installs the Avaya one-X® Central Management portal as default with local authentication. All Avaya one-X® Central Management users and agents are managed locally in the Avaya one-X® Central Management database.

With ACCCM 7.0, you can integrate Avaya one-X® Central Management with the main ACCCM portal and manage all users and agents directly from ACCCM.

If this option is enabled, you cannot login into the Avaya one-X® Central Management Web administration portal with the default Avaya one-X® Central Management users or any user that was created locally on Avaya one-X® Central Management. All agents created in Avaya one-X® Central Management are still active and can continue to work with their Avaya one-X® Agent clients.

This chapter includes:

- [Integrating Avaya one-X® Central Management with ACCCM on page 90](#)
- [Managing agents and users from ACCCM on page 91](#)
- [Managing permissions from ACCCM on page 93](#)

Integrating Avaya one-X® Central Management with ACCCM

Perform the following steps to configure the integration:



1. Navigate to the ACCCM one-X Web folder.
2. Open the web.config file in Notepad.
3. In the web config file, set the ACCCM_SSO key to *true*.
`<add key="ACCCM_SSO" value="true" />`
4. Save the web.config file.
5. Log in to the ACCCM Web Portal as administrator.
6. Navigate to the **CFG > one-X** and observe the following:
 - If you are using ACCCM 7.0, the ACCCM installation wizard system displays the following screen.

Alias	Type	Server IP	Port	Username	Database Server	Database Username	Database name
one-X Agent	one-X Agent	ACCCMGA631	1433	ACCCMONEXUSER	ACCCMGA631	ACCCMONEXUSER	ACCCMONEXDB

- If you are upgrading from a prior version, you must configure the Avaya one-X® Central Management integration in this tab manually and configure the following parameters:

Field	Description
Alias	Any given name.
Server IP	The IP address or host name of the server that hosts the ACCCMONEXDB database.
Port	The port number that the database server uses. The default SQL port number is 1433 .
Username	The database username of the ACCCMONX user. The ACCCM installation wizard creates the default user as ACCCMONEXUSER.
Password	The password of the database user.
Database server	The IP address or host name of the server that hosts the ACCCMONEXDB database.
Database name	The name of the database. The default value is acccmonexdb.
Database Username	The database username of the ACCCMONX user. The ACCCM installation wizard creates the default user as ACCCMONEXUSER.
Database Password	The password of the database user.

7. Save the configuration.
8. To assign the one-X integration to a location, perform the following steps:
 - a. Navigate to the **CFG > Location** tab.
 - b. Selected the location assigned to the one-X system.
 - c. Assign the one-X Integration record to the location.

The screenshot shows a configuration window titled 'one-X'. It is divided into two main sections: 'Available one-X' on the left and 'Chosen one-X' on the right. In the 'Available one-X' section, there is a large empty rectangular box. In the 'Chosen one-X' section, there is a list containing 'one-X Agent'. Between the two sections, there are two red arrows: a right-pointing arrow above a left-pointing arrow, indicating a selection or movement action.

- d. Repeat these steps for each location that you want to assign to the one-X integration.



Managing agents and users from ACCCM

When the ACCCM integration is activated for Avaya one-X® Central Management, you can

manage all one-X Agents and users from ACCCM.

- [Creating agents from ACCCM on page 92](#)
- [Creating users in Central Management from ACCCM on page 93](#)

Creating agents from ACCCM



1. On the **ACCCM** menu, select the **Users** tab.
2. Create a new agent or edit an existing agent record in ACCCM.
3. Select the one-X Application from the list of available applications.

Available applications			
☐ AAC	☐ ACCCM	☐ ACR	☐ AIC
☐ EMC Config	☐ CM	☐ CMS	☐ Dashboard
☐ EWA	☐ Exp. Manager	☐ IQ	☐ IVR
☒ one-X Agent	☐ PC	☐ POM	☐ QM
☐ Self Service	☐ SIP	☐ SSM	☐ Visual Vector

one-X Agent Details	
Authentication Type*	DB User
Domains	

4. Enter a username and password for the agent.
5. Select the one-X Agent authentication type.
If you are using SSO or LDAP based authentication in one-X Agent, select the Domain the agent uses.
6. Click **Save**.
7. To assign the Agent to a Avaya one-X® Agent template, perform the following steps:
 - a. Click the **one-X Agent Profile** tab.
 - b. Select the template for the agent.
 - c. Click **Save**.
8. To assign the agent to an agent role in the Avaya one-X® Agent application, perform the following steps:
 - a. Click the **Permissions** tab.
 - b. Assign the agent to the Avaya one-X® Agent application.
 - c. Click **Save** to save the agent record.



Creating users in Central Management from ACCCM



1. On the **ACCCM** menu, select the **Users** tab.
2. Create a new agent or edit an existing agent record in ACCCM.
3. Select the Avaya one-X® Agent from the list of available applications.
4. If the user is new, enter a username and password.
5. Click **Save** to add the user.
6. To assign the user to a role in the Avaya one-X® Agent application, perform the following steps:
 - a. Click the **Permissions** tab
 - b. Assign the agent to the Avaya one-X® Agent application
 - c. Click **Save** to save the agent record.

NOTE: The Role controls the user role in Avaya one-X® Agent



Managing permissions from ACCCM

By enabling the integration between the Avaya one-X® Central Management and the main ACCCM application, all permissions are inherited from the role based permission engine of ACCCM.

ACCCM supports the following permissions:

Permission name	Description
one-X Agent	This permission is assigned to Agents who login to the Avaya one-X® Agent client application.
one-X Agent Supervisor	This permission is assigned to supervisors who log in to the Avaya one-X® Agent client application. This permission is assigned with the Avaya one-X® Agent permission.
Web Administrator	This permission provides the user the ability to login into the Avaya one-X® Central Management web portal.
Add contact list member	This permission allows the administrative user to add contact list members in the Avaya one-X® Central Management portal.
Add location data	This permission allows the administrative user to add location data in the Avaya one-X® Central Management portal.
Delete contact list	This permission allows the administrative user to delete a contact list in the Avaya one-X® Central Management portal.
Delete group	This permission allows the administrative user to delete an agent group in the Avaya one-X® Central Management portal.

Edit contact list	This permission allows the administrative user to edit a contact list members in the Avaya one-X® Central Management portal
Edit group	This permission allows the administrative user to edit an agent group in the Avaya one-X® Central Management portal.
Import contact list member	This permission allows the administrative user to use the import contact list member feature in the Avaya one-X® Central Management portal.
Add domain	This permission allows the administrative user to add a new domain in the Avaya one-X® Central Management portal.
Add template	This permission allows the administrative user to add a template in the Avaya one-X® Central Management portal.
Delete contact list member	This permission allows the administrative user to delete contact list members in the Avaya one-X® Central Management portal.
Delete location data	This permission allows the administrative user to delete location data in the Avaya one-X® Central Management portal.
Edit contact list member	This permission allows the administrative user to edit contact list members in the Avaya one-X® Central Management portal.
Edit location data	This permission allows the administrative user to edit location data in the Avaya one-X® Central Management portal.
Import location data	This permission allows the administrative user to import location data in the Avaya one-X® Central Management portal.
Add domain group	This permission allows the administrative user to add a domain group in the Avaya one-X® Central Management portal.
Add user	This permission allows the administrative user to add a new user/agent in the Avaya one-X® Central Management portal.
Delete domain	This permission allows the administrative user to delete a domain in the Avaya one-X® Central Management portal.
Delete template	This permission allows the administrative user to delete a template in the Avaya one-X® Central Management portal.
Edit domain	This permission allows the administrative user to edit a domain in the Avaya one-X® Central Management portal.
Edit template	This permission allows the administrative user to edit a template in the Avaya one-X® Central Management portal.
Import users	This permission allows the administrative user to import users/agents in the Avaya one-X® Central Management portal.