Administering Avaya one-X® Agent with Central Management

Release: 2.5
Issue: 1.0
May 3, 2011

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 Web sites 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 Web site: 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, 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 End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License type

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 Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: 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 Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Introduction to Avaya one-X Agent Central Management

Introduction

Avaya one-X® Agent Central Management (Central Management) is an optional Web-based solution that Avaya one-X Agent customers can deploy based on their management requirement. It manages users' profiles at contact centers running Avaya one-X Agent and provides the ability to manage all Avaya one-X Agent features.

Central Management manages endpoints, Avaya one-X Agent users, and agent configuration data from a central location. It has a task-based Web interface that helps in efficient and effective management of Avaya one-X Agent users and their settings. The Web interface is consistent with the Avaya one-X Agent client user interface for the respective settings, and therefore, is easy to configure.

Central Management features

Following are some of the salient features of Central Management:

- Provides secure and role-based access.
- Provides centralized control of endpoints.
- Allows creating global settings for all users.
- Allows creating parent and child templates. The administrators can assign these templates to agent groups based on user roles and business area.
- Provides integrated options to control agent from accessing various critical client settings.
- Imports multiple agent profiles, with their customized settings from a setup.
- Supports Active Directory authentication.
- Provides options to store agent-created settings and applies the settings in the subsequent agent login.
- Provides options to store and manage pre-defined location data, and links the desktop client to Communication Manager, thereby, enabling administrators to hot-desk the agents.
- Provides options for administrators to select preferred profile for agents.

Related topics:

Supported browsers on page 10

Accessing online help on page 10

Supported browsers

The Central Management Web interface supports the following browsers:

- Internet Explorer 7.x or later
- Firefox 3.x or later

Accessing online help

Prerequisites

Switch off any pop-up blocker for your browser, as it may block the online help from opening either in a new tab or in a browser window.

Click the **Help** link on the top right corner of your Web page.

The online help page opens in a separate browser window or browser tab as per your browser configuration.

Chapter 2: Getting started

Logging on to Central Management

Prerequisites

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

1. Launch 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 Central Management.

   Note:
   If you are upgrading to Central Management 2.5 and using an old Central Management 2.0, ensure that you have changed the port to 8643, as necessary.

2. Log on to the Central Management Web interface as administrator.
   The Central Management home page appears.

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

   Tip:
   If you are logging on to Central Management for the first time after the installation, 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. Upon logging on to the Central Management Web console, you can create users having a Web Administrator role for subsequent logins.

   Note:
   Ensure that the user name in the Central Management console exists in Active Directory.

The above tip is not applicable if your credential is already defined in the system as an administrative user.

4. Click **Login**.
   The system logs you in as a user in to Central Management.

Logging out of Central Management

Prerequisites

Before logging out of Central Management, ensure that you save the changes made to the page.

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

Planning a client configuration in Central Management

This section provides a general guideline that you can follow to perform a client configuration using Central Management.

Follow the instructions below to optimize your efforts in configuring a client setup.

1. Plan the setup

Determine the number of templates you need before planning the setup. You must also collect information on the number of profiles that agents may require to handle. You must identify common and distinguishing requirements for each profile and accordingly plan for creating templates.

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 Central Management that cater to those requirements. Initially, you can create only the template structure and name the template you require. You can later configure the template in detail, as the number of requirements arise. 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 one-X Agent user to groups. You can assign templates to agents or groups of agents. Upon doing this, each template creates a profile for each agent with the same name as the template. You can also do this to individual agents, or to 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 list using a CSV file.

Use the example comma separated values (CSV) file, available from the Import Users page of Central Management, to create a user list with respective user roles and templates to which the users must be assigned. This saves you from configuring each user on 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. The users cannot log on to Avaya one-X Agent, if they are not assigned to a template. Therefore, you must assign all users a high-level or the default template.

6. Import the CSV file of users

If you want to use the CSV file of users, you must import the CSV file of users into Central Management. The users get assigned to the corresponding roles and templates that you have created before importing.

7. Assign users to the appropriate groups

Assign users to the appropriate groups. Therefore, the users get distributed based on the profile that they are assigned to handle.

8. Assign supervisors to groups

The supervisors' roles will be assigned to users when they are imported from the CSV file. However, you must assign supervisors to a user group that they manage at this stage. The user group gets added to the supervisor's contact list automatically.

9. Create contact lists and assign to a template

Create contact lists of clients for whom you have created the templates. Assign each contact list to its 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.

Configuring the Single Sign-on setup

You can configure Central Management to use the Windows Kerberos credentials and the SPNEGO (Simple and Protected GSS-API Negotiation) protocol for Single Sign-on (SSO). By doing so, users can bypass the user name and password authentication for each server component. Central Management uses a JBoss authentication module called JBoss Negotiation to integrate with the JBoss container that Central Management runs on.

Note:

If you are using Windows Server 2008 as Active Directory, ensure that you have applied Service Pack 2 or the Kerberos specific hot-fix from http://support.microsoft.com/kb/951191. Avaya recommends Windows 2003 R2 Service Pack 2 for Active Directory on Windows 2003 server.

Prerequisites

You must complete the SSO configuration after installing Central Management. The steps below assume a working system installed using the procedures described in the *Installing Server Applications for Avaya one-X® Agent* guide.

1. In the forward lookup zone, under the domain name, add the Central Management server to DNS and ensure that the server gets Active Directory in the reverse lookup zone.

   Important:

   Central Management and Active Directory must be in the same domain.
2. Create a new *Active Directory* user account for Central Management.

   The account must be a user account with the user login name configured as the host name of Central Management (for example, **`vmcamdeployed`**) with the following options:

   - User cannot change password
   - Password never expires

   Note:

   Ensure that a computer name is not present for Central Management. The computer name—which is basically the Central Management server name—is not listed as a computer account in the computers in Active Directory. But, you must add a user account with computer name (the Central Management server name) in the Users field in Active Directory.
3. Enable the **Do not require the Kerberos pre-authentication** option using the following steps:

a. Open the Properties window of the newly created user account.

b. Select the **Account** tab.

c. Select **Do not require Kerberos pre-authentication** from the **Account options** list.

4. Create another user as an administrator in Active Directory. For example, a user with `ssouser01` as the user name.

   Ensure that the account option in Active Directory is set to **Password never expires** for the corresponding user.

5. Log on to the Central Management Web interface as administrator.

   By default, Central Management runs in the Form mode. If FQDN does not work, then the machine from which you launch the URL must not be in the same domain as that of Central Management.

6. To log on to the Central Management Web interface as a Web Administrator in the SSO mode you must create a new Central Management user with a Web Administrator role, for example, `ssouser01@AUSTEST.AVAYA.COM`, with DOMAIN in uppercase.

   Note:

   This user account must exist in Active Directory.

   a. Access the Central Management Web Interface in the Form mode.

   b. In the Central Management Web interface and navigate to the **Manage Users** page.

   c. Create a new user for SSO, check the Web Administrator role, and assign a user profile to the user.

   d. Enter the full account name in the **Username** field, for example, enter `ssouser01@AUSTEST.AVAYA.COM`. with DOMAIN in uppercase.

   Tip:

   To avoid the system being logged out of the Web application, you must create the new Web Administrator account using the full account name in the **Username** field, for example, `ssouser01@AUSTEST.AVAYA.COM`.

7. To log on to the Avaya one-X Agent client in the SSO mode, create an SSO user through the Central Management user interface in the Form mode:

   a. In the **Manage Users** section, create an SSO user with Avaya one-X Agent role and assign a profile to the user.

   b. In the **Username** field, enter the full account name, for example, enter `ssouser02@AUSTEST.AVAYA.COM`. with the domain name in uppercase.

   If a user is already created using the Central Management user interface, then the user must re-configure SSO to use the `<User Name>@<DOMAIN NAME>.COM` format with the domain name in uppercase.

8. Note down the following critical values:
    - Host name of Active Directory (FQDN of Active Directory server): <hostname of the Active Directory server>.austest.avaya.com
    - Domain name of Active Directory (Long Form): austest.avaya.com
    - Domain name of Active Directory (Short Form): AUSTEST
    - Host name of Central Management (FQDN of Central Management): <hostname of the Central Management server>.austest.avaya.com
9. At the prompt, run the following commands on Active Directory:

```
setspn.exe -a host/<hostname of the Active Directory
Server>.austest.avaya.com vmcamdeployed
setspn.exe -a HTTP/<hostname of the Active Directory
Server>.austest.avaya.com vmcamdeployed
ktpass  -princ host/oxacm hostname@DOMAIN.COM -ptype KRB5_NT_PRINCIPAL -
pass * -mapuser DOMAIN\oxacm hostname -out C:\oxacm hostname.host.keytab
```

Note:

The system generates the last command `C:\vmcamdeployed.host.keytab`.

10. At the prompt, run the command: `setspn -l vmcamdeployed`.

    The following output appears:

```
host/vmcamdeployed
host/vmcamdeployed.austest.avaya.com
HTTP/vmcamdeployed.austest.avaya.com
```

If you have multiple domain controllers, use the following command to eliminate a warning message:

`WARNING: Type and account type do not match. This might cause problems.`

```
ktpass-princ host/oxacm hostname@DOMAIN.COM -ptype KRB5_NT_PRINCIPAL -
pass * -mapuser DOMAIN\oxacm hostname -out C:\oxacm hostname.host.keytab
```

Note:

To use the ktpass command, you must download Active Directory and install Windows Server 2003 R2 support tools, or a version that matches your Active Directory.

11. If your Active Directory does not have JDK 1.6 update 11 or above, transfer the generated keytab file to a Windows machine that has JDK 1.6 update 11 or above, and run the following command:

```
ktab -k C:\vmcamdeployed.host.keytab -a vmcamdeployed@AUSTEST.AVAYA.COM
```

This command updates the keytab file.

12. Rename the `vmcamdeployed.host.keytab` host file to `oxacm.host.keytab`.

13. Copy the `oxacm.host.keytab` host file as binary to the Central Management server `/etc` directory.
14. Ensure that the Linux server, on which Central Management is running, synchronizes its time with Active Directory using NTP.
15. From the Central Management machine, stop the OXACM service using the following command,

    ```
    service oxacm stop
    ```

16. Navigate to the `/opt/Avaya/OneXAgentCM/bin` directory, and perform the following steps:

    Type the following commands to run the Central Management SSO setup script:

    ```
    chmod 754 oxacmssosetup.sh
    ./oxacmssosetup.sh
    ```

    - When the system prompts for Active Directory (FQDN) name, enter <hostname of the Active Directory server>.austest.avaya.com
    - When the system prompts for Active Directory domain (long Form), enter `austest.avaya.com`.

    The following output appears:

    ```
    vmcamdeployed@AUSTEST.AVAYA.COM
    ```

17. On the Central Management server, start the OXACM service using the following command:

    ```
    service oxacm start
    ```

18. Access the Central Management server with a standard Web browser through the `https://oxacm server FQDN:8643/jboss-negotiation-toolkit/SecurityDomainTest`, and click the **Test** button.
    The following output appears after a successful SSO configuration:

    ```
    Negotiation Toolkit
    Security Domain Test
    Testing security-domain 'host'
    Authenticated
    Subject:
    Principal: host/SSODC2@OXACMDC.COM
    Private Credential: Ticket (hex) = 0000: 61 82 01 04 30 82 01 00 A0 03 02
    01 05 A1 0D 1B a...0........... 0010: 0B 4F 58 41 43 4D 44 43 2E 43 4F 4D
    A2 20 30 1E .OXACMDC.COM. 0. 0020: A0 03 02 01 02 A1 17 30 15 1B 06 6B 72
    62 74 67 .......0...krbtg 0030: 74 1B 0B 4F 58 41 43 4D 44 43 2E 43 4F 4D
    A3 81 t..OXACMDC.COM.. 0040: C7 30 81 C4 A0 03 02 01 17 A1 03 02 01 02 A2
    81 .0.............. 0050: B7 04 81 B4 BF 17 2C D6 DA 8F 3E 45 3D 59 1F
    DB ......,...>E=Y.. 0060: DF B5 61 1A AF 4B DC A2 C9 51 0D CE 15 17 B5
    18 ..a..K...Q...... 0070: 06 FB 5C 95 0C 30 18 13 8C 41 A2 73 38 D7 F4
    96 ..\..0...A.s8... 0080: DE C0 D6 0B D3 A2 EE AF 2E 33 F7 AE 0F 93 79
    29 .........3....y) 0090: AB 3B 1D 66 AF BB 8D 12 3A E7 0B 6C 65 AA C7
    CD .;.f....:..le... 00A0: 0F A1 72 5E A5 49 09 84 BF 54 33 5F 71 2C BF
    72 ..r^.I...T3_q,.r 00B0: 42 04 67 9C F9 FD 3E 63 56 79 A5 E3 57 A1 81 E3
    B.g...>cVy..W... 00C0: 6C 5C 1A AF B5 3F Active Directory 06 B2 7F 45 3E
    04 1E AB BE l\...?....E>.... 00D0: F2 0A C8 1D 10 DA 37 63 8F 00 86 62 15
    A5 F8 AE ......7c...b.... 00E0: EB 54 CB 83 F8 19 EC 44 D5 50 D7 57 ED 52
    66 A4 .T.....D.P.W.Rf. 00F0: 21 35 6A 01 DB 1C BF E9 70 96 1D BB DF F3 DE
    74 !5j.....p......t 0100: 66 02 29 D9 2C 0F 08 05 f.).,...
    ```

```
Client Principal = host/SSODC2@OXACMDC.COM
Server Principal = krbtgt/OXACMDC.COM@OXACMDC.COM
Session Key = EncryptionKey: keyType=23 keyBytes (hex dump)= 0000: 41 56
72 10 37 44 8C 26 56 A3 07 05 FF 25 7F 0D AVr.7D.v%..
Forwardable Ticket false
Forwarded Ticket false
Proxiable Ticket false
Proxy Ticket false
Postdated Ticket false
Renewable Ticket false
Initial Ticket false
Auth Time = Wed Nov 03 13:17:54 PDT 2010
Start Time = Wed Nov 03 13:17:54 PDT 2010
End Time = Wed Nov 03 23:17:54 PDT 2010
Renew Till = null
Client Active Directorydresses Null
Private Credential: Kerberos Principal host/SSODC2@OXACMDC.COMKey Version
4key EncryptionKey: keyType=23 keyBytes (hex dump)= 0000: 2B B6 8A 70 B0
4E 8D F7 77 53 30 F9 01 14 BB A5 +..p.N..wS0.....
```

If the SSO configuration fails, an error message appears.

19. Switch the Central Management server to authenticate using the SSO authentication by running the following commands:

```
chmod 754 /opt/Avaya/OneXAgentCM/bin/oxacmauthselect.sh sso
./opt/Avaya/OneXAgentCM/bin/oxacmauthselect.sh sso
```

Note:

To confirm the Central Management server in the SSO mode, navigate to the `/opt/Avaya/ OneXAgentCM/jboss-4.2.3.GA/server/default/deploy` directory, and locate the `HostedCCAll-sso.ear` file. You can switch from the SSO mode to the Form mode by running the following commands:

```
chmod 754 /opt/Avaya/OneXAgentCM/bin/oxacmauthselect.sh form
./opt/Avaya/OneXAgentCM/bin/oxacmauthselect.sh form
```

To confirm the Central Management server in the Form mode, navigate to the `/opt/Avaya/ OneXAgentCM/jboss-4.2.3.GA/server/default/deploy` directory, and locate the `HostedCCAll-form.ear` file.

20. To verify if the Web administrator can log on to Central Management in the SSO mode, add a Windows XP client machine to the same domain server as Central Management.

Related topics:

[Configuring Mozilla Firefox for SSO with Central Management](#) on page 18
[Configuring Internet Explorer for SSO with Central Management](#) on page 19

Configuring Mozilla Firefox for SSO with Central Management

To use SSO with Mozilla Firefox, you must use the following steps to configure the settings:

1. Enter the URL: `about:config` in the Firefox address bar.
   The configuration options appear for Firefox.
2. Set the **Filter** to `network.negotiate` to reduce the list to the options that relate to negotiation.
3. Double-click **network.negotiate-auth.trusted-uris**, and set the *Value* property to the URL of Central Management.
4. Click **OK**.
5. To ensure that no proxy is set:
   a. In the **Firefox** browser, click **Tools** > **Options** > **Advanced**.
      The **Options** dialog box appears.
   b. Click the **Network** tab.
   c. Click the **Settings** button, and select the **No Proxy** option.

Configuring Internet Explorer for SSO with Central Management

To use SSO with Internet Explorer you must use the following steps:

1. Click **Tools** > **Internet Options**.
2. Select the **Security** tab.
3. Select the **Local Intranet** zone.
4. Click the **Advanced** button.
5. Enter the URL of the Central Management server to the zone.
6. Click **Add** and then **Close**.
7. Click **OK** to complete the configuration.

   Note:
   To enable SSO for Internet Explorer on Windows 2008, Windows 7, and Windows XP, add the `SuppressExtendedProtection` key under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa` in Windows Registry and set the value to `3` as these platforms have Extended Protection for Authentication. For more information, visit the Microsoft Web site at http://support.microsoft.com/kb/968389

Chapter 3: User administration

Importing users to Central Management

Central Management allows you to 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. A sample tab-delimited file is also available from the **example** link on the Import Users page. You must click the **example** link, save the CSV file to your computer as a Unicode Text file, and add the user details to this file. The Unicode Text file saves the data in the tab-delimited format.

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

Note:

If the system imports a user from the Unicode Text file that already exists on Central Management, it 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 Central Management console.

Tip:

Avaya recommends that you create groups and templates that you plan to assign to the users before importing users. By doing so, you can directly add template names in the tab-delimited file. You can 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:

Sequence	Column names	Column values
1	User name	The Avaya one-X Agent user name to be in Central Management.
2	First Name	User's first name.
3	Last Name	User's last name.
4	Email	User's e-mail address.

Sequence	Column names	Column values
5	Role: one-X Agent	Enter `Y` or `Yes` in this column if user must be assigned to a one-X Agent role. You can leave this field blank, otherwise.
6	Role: one-X Agent Supervisor	Enter `Y` or `Yes` in this column if user must be assigned to a one-X Agent Supervisor role. You can leave this field blank, otherwise.
7	Role: Web Administrator	Enter `Y` or `Yes` in this column if user must be assigned to a Web Administrator roleYou can leave this field blank, otherwise.
8	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. There can be multiple columns corresponding to the templates in Central Management. However, ensure that the template names match exactly to those in Central Management.
9	Group: <group name>	Replace <group name> with the exact name of the user group in Central Management. You can create multiple columns for the groups in Central Management to which you want to assign users. However, the group names must exactly match the names in 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 a data to the file, do not delete or overwrite the header row of the Unicode Text file.

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

1. From the Central Management navigation menu, click **Import Users**.
2. In the **File** field, click **Browse** to locate the Unicode Text file.
3. Click **Import** to import users listed in the Unicode Text file.

Next steps

You can view the imported users on the **Manage Users** page.

Adding users in Central Management

Prerequisites

Ensure that all users added to or imported from the CSV file into Central Management have their user names defined in Active Directory.

1. On the Central Management navigation menu, click **Manage Users**.
   The **Manage Users** page appears.
2. Click the **Add user** link.
   The **User Detail** panel appears at the bottom of the page.
3. 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 **Email** field, enter the contact's e-mail address.

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

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

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

You can select multiple user roles for the user. See Central Management roles on page 30 to know more about user roles.

After selecting the one-X Agent roles, the **Profiles assigned** tab appears. If you select **Supervisor Role**, then the **My Team** tab appears. This will not appear for other roles.

4. If you click **Save** without selecting any one of the one-X Agent roles, then the system saves the user details without any roles assigned to the user.
5. To assign user groups, perform the following steps:
   a. Click the **Group membership** tab.
   b. From the **Group name** list, select appropriate group.
   c. Click **Add**.
   The system assigns the user to the selected group. You can repeat the above steps to assign multiple user groups.
6. If you have assigned a **one-X Agent Supervisor** role to the user, the **My Team** tab appears. 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, e-mail, and user name. You can sort the **Group member**, **Email**, and **Username** column in ascending and descending order and the corresponding details get aligned accordingly. Click the **First**, **Prev**, **Next**, and **Last** links to navigate in the list of team members if there is a long list of team member names added to a group.

   Note:
   In order to view child profiles in the Profile name list, you must create child profiles in the Manage Templates section. To create a child profile, under the *default* the parent profile, click **Add**. Then, name the child profile 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.
7. To assign a template to the user, perform the following steps:
   a. Click the **Profiles assigned** tab.
   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. Upon assigning the template to this user, it generates a profile for the corresponding

user with the same name as the template that was assigned. The system also marks this profile as Preferred.

c. Click **Add**.

Repeat the above steps to assign multiple templates to the user. A user cannot log on to Avaya one-X Agent unless you have 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 will be marked as the **Preferred** profile.

Note:

If you have 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.

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

The profile editor screen appears. Customize the assigned profile for the selected user.

e. Select **Automatically execute all logins for the selected profile**, if you want the system to execute auto login for users into the services automatically.

f. Select **Disable local profile Administration**, if you do not want the user to modify the preferred selection during the user login.

If you have not enabled this option and you only have a profile assigned, the system skips the profile selection window and logs the user directly with the preferred profile. However, if you have multiple profiles assigned to this user, the system displays the profile selection window allowing you to select a profile other than the preferred profile.

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

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

Options	Descriptions
IM contacts not in system contact list	Select this option to send IM to contacts outside their contact list. **Note:** If you do not select this option, the user will not be able to enter the IM

Options	Descriptions
	address for the contact the user may create in Contact List.
Allow Desktop sharing	Select this option if you want the agent to share the desktop with the other user through the IM session, or internal telephone calls with in Contact List and Presence Services.
Window size	Use this 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%** This option is not available if you have not selected the **Allow Desktop sharing** option.

b. The **General Settings** tab, lists the settings for actions that Central Management must perform when a user logs out from a system.

Options	Descriptions
Save agent settings from desktop on exit	Use this option to save the agent's one-X Agent current profile on the local computer and to upload the changes to Central Management when an agent logs out. If the agent is unable to log on to Central Management, this option allows the agent to log on using the last-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 work log on exit	Use this 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

Options	Descriptions
	Agent. The work log contains critical log of agent's work.
Delete contact lists on exit	Use this 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's contacts.
Time between client configuration saves	Use this option if you want the system to specify the interval between saves of the user profile data changes to Central Management while logged in.

9. Click **Save** to add the user to Central Management.

Next steps

1. Check if the new user appears in the user list on the **Manage Users** page.
2. To view **User Details**, from the user list, click the corresponding user name.

Related topics:

Editing user details on page 27
Filtering users on page 29
Activating and deactivating a user on page 30
Central Management roles on page 30

Editing user details

Prerequisites

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

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

   The **User Detail** tab appears at the bottom of the page with the selected user name.
3. On the **User Detail** page, perform the following steps:
   a. Click the **Details** tab, to edit the name, user name, and e-mail address.
   b. To remove groups, click the **Group membership** tab, and then click the **-** button under **Add / Remove**. To assign groups, click the drop-down list under the **Group name** column, select a group, and click the **+** button under **Add / Remove**.
   c. To remove profiles, click the **Profiles assigned** tab, and then click the **-** button under **Add / Remove**. To assign profiles, click the drop-down list under the **Profile name** column, select a profile and click **+** button under **Add / Remove**.

      If you attempt to remove a profile, which is the only profile assigned to the user, the system prompts you with 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.
   d. To customize users profile for the selected user, click the **Profiles assigned** tab, and then under the **Edit** column, click the **Profile settings** link.

      The profile editor screen appears.
   e. 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 it to Central Management.

   Note:

   If the user continues to be a member of the group, you cannot remove the roles and templates assigned to the users through a 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.

Next steps

1. Check if the changes appear for the user on the **Manage Users** page.
2. Click the user name from the user list to view **User Details**.

Filtering users

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 Central Management navigation menu, click **Manage Users**.
   The Manage Users page appears with the user list.
2. To find a user by name, in the **Filter** field, enter the user first name, last name, or user name.
   The system filters the keyword matching the field and displays it 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.

   The system applies the **By role** filter criterion as a default.

   The system filters the keyword matching the role and displays it 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 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**

Activating and deactivating a user

Prerequisites

User details must be present in Central Management.

Administrators can prevent or grand access to Central Management and Avaya one-X Agent for users by adjusting the Activation/Deactivation field. When administrators deactivate a user, an `Operation Failed` message appears when the user attempts to log on to Avaya one-X Agent. But, all configurations remain attached to the user. On activating, agents can login using the last saved configuration data.

1. On the Central Management navigation menu, click **Manage Users**.
   The list of users appear in the Manage Users list.
2. Perform one of the following option:
   - 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.

Central Management roles

You can assign the following user roles to users administered on Central Management. The table describes the privileges and restrictions for each role assigned through Central Management.

Role	Privileges
one-X Agent	Assign this role to users using Avaya one-X Agent in a contact center. Users with this role have the following rights and restrictions: • Users can use all the privileges assigned through 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 Central Management. Users with this role do not have access to the Central Management Web interface.
one-X Agent Supervisor	Assign this role to users who are responsible for managing and service observing agents in their My Team group. Users with this role also have

Role	Privileges
	all privileges to the one-X Agent role and access to the Central Management Web interface.
Web Administrator	Assign this role to user who are responsible for performing 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 on Central Management, they do not have access to Avaya one-X Agent, since they are not the intended end users.

User groups in Central Management

A user group in 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 all these group assignments to each member of the group, and therefore allows the administrator to define the 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 Avaya one-X Agent Contact List window.

You can create, edit, delete, and filter groups using Central Management. You can also perform bulk import of group definitions with assigned templates and users, by using a CSV file.

Related topics:

Importing user groups into Central Management on page 31

Creating user groups on page 33

Editing user groups on page 35

Deleting groups on page 36

Filtering groups on page 37

Importing user groups into Central Management

You can import bulk group definitions into Central Management and then assign agents to the group definition. You can also assign agents to existing groups. This option is useful when you have large number of groups to create, assign various roles to each group, and assign groups to various templates in Central Management. You can create all the required groups outside Central Management, and then import them into Central Management. This saves time from creating individual groups in Central Management and assigning them with roles and templates.

You must create the group names in a Unicode Text file and assign appropriate roles and templates in the Unicode Text file. If you have an old CSV file with data, you must save it as a

Unicode Text file. The system adds the user roles and templates to this 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 may 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 do not exist, perform the following steps to create a group list:
    a. On the Central Management navigation menu, open the **Import Groups** page.
    b. Click the **example** link, and export the file to your computer.
    c. Open the **groupsexample.csv** file, and enter the details in the order of column headings as follows:

Column Heading	Description
Group name	Enter the name for this group.
Role: one-X Agent	Enter `Y` or `Yes`, if the group has the one-X Agent role. Leaving the field blank will deny access for one-X Agent.
Role: one-X Agent Supervisor	Enter `Y` or `Yes` if the group has the one-X Agent Supervisor role. Leaving the field blank will deny access for one-X Agent supervisor.
Role: Web Administrator	Enter `Y` or `Yes` if the group has the Web Administrator role. Leaving the field blank will deny access for Web Administrator.
Template: <template name>	Enter the template name in Central Management, for example, enter `Template: default`. The template name on this form must match the name that was assigned to the template when it was initially added to the system. You can have multiple columns corresponding to the templates created in Central Management. However, ensure that the template

Column Heading	Description
	names match to those in Central Management.

Caution:
When you are adding data to the file, do not delete or overwrite the header row of the CSV file.

d. Save the file with a different name.

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

Use the following steps to import group data.

1. On the **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 Central Management.

Next steps

To view the groups that you have imported using the CSV file, go to **Manage Groups**.

Creating user groups

1. On the Central Management navigation menu, click **Manage Groups**.
2. On the **Manage Groups** page, click **Add Group**.
   The **Group Detail** tab appears at the bottom of the page with the **Group details**, **Roles**, **Templates** (for **Web Administrator** role), and **Member** tabs.
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, choose a supervisor.
      This is an optional step. If you assign a supervisor in this step, all the group members appear in the **My Team** list of the supervisor.

c. If you select a supervisor to this group, you can select the **Add supervisor to speed dial** option to add the supervisor's name to the speed-dial list and view it in the Avaya one-X Agent Contact List window under **My Supervisors**.

   By default, the system enables the **Add supervisor to speed dial** option, but is grayed out 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 Add/Remove Members window appears with users.

   ii. Select a user to add to this 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/Non-group member** conditions.

      When you select a contact from the group, a message appears indicating that the system is adding the selected user to the group 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 **one-X Agent** or **one-X Agent Supervisor** role, the system adds the **Templates** tab.

   Note:
   The **Templates** tab does not appear, if you are creating a group with the **Web Administrator** role.

5. To assign a template for **one-X Agent** and/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.
A new window appears with the template settings. To modify, refer to Central Management templates on page 41.

6. To view the newly added members to the group, click the **Members** tab.

   You can use **Add/Remove members** link to add or remove group members.
7. Click **Save** to save the group with the given name and assigned details.

Next steps

Check the **Manage Groups** page to see if the newly added group appears in the groups list with its assigned attributes.

Editing user groups

You can change the following group details:

- Group name and supervisor
- User roles assigned to the group
- Add or remove group members

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

1. On the Central Management navigation menu, click **Manage Groups**.

   The **Manage Groups** page appears.
2. From the **Group** column, select a group.

   The **Group Detail** tab appears 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** 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 into Avaya 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 choose 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 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 under the **View** column.

     A read-only view of template settings appear 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 user list appears in a new window with options against each user.
   b. Select the options against users you want to add, and clear the options against the users you want to remove.
      You can add or remove only one user at a time.
   c. Click **Close**.
7. Click **Save**.

Next steps

Select the updated group on the **Manage Groups** page, and verify if the system has make necessary changes for the selected group correctly.

Deleting groups

1. On the Central Management navigation menu, click **Manage Groups**.

The **Manage Groups** page appears with list of all groups.

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 the users or roles from the Central Management server.
   - The system does not remove the roles assigned to users after deleting the group.

Filtering groups

You can filter groups by entering a group name, by selecting a user role, selecting a template, or by using a combination of group name, user role, and template name.

1. On the Central Management navigation menu, click **Manage Groups**.

   The **Manage Groups** page appears.

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

   The keyword matching the group name appears in the list.

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

   The keyword matching the group role appears in the list.

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

   The keyword matching the template appears 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 keyword matching both the criteria group appears in the list.

Chapter 4: Administering templates and settings

Location data in Central Management

Location data enables agents to hot-desk. When hot-desking, agents can log on to the Avaya one-X Agent client from any desk or location and retrieve their profiles with their customized settings and user data. Using 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 and saved data. At log out, the central server stores all user data.

Related topics:

Importing the location data on page 39
Editing location data on page 40
Filtering location data on page 41

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 example sample excel file to the local directory as a `.csv` file, open the `locationexample.csv` file, and assign the location data, as appropriate.

Note:

Avaya recommends that you rename the `locationexample.csv` file. You can use this file for future use.

The `locationexample.csv` file contains the following columns:

Column	Description
Host Name	The host name is the name of an agent's computer.
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`.

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

1. On the Central Management navigation menu, click **Import Location Data** .
2. In the **File** field, click **Browse** to locate the CSV file that contains the location data.
3. Click **Import**.
   The system imports the location data in the database. You can check the new location data in the **Manage Location Data** page. If the data is not correctly imported or if an error message appears, verify the CSV file.

Editing location data

Prerequisites

The location list must be available on Central Management.

1. On the Central Management navigation menu, click **Manage Location Data**.

The **Manage Location Data** page appears with the list of administered locations.

2. Locate the location data, and make necessary changes.
3. Click **Save**.

Filtering location data

1. On the navigation menu, click **Manage Location Data**.
   The **Manage Location Data** page appears with the list of administered locations.
2. Enter the location keywords in the **Filter** field.
   The keywords matching the location data list appears in the location data list.

Central Management templates

A template is a collection of user settings. Using templates saves your time and effort spent in user configuration. You, as an administrator, can create a template and assign it 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, for the user. 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. Any change you make to a parent template, the child template will inherit the changes automatically. However, if an agent changes the fields in the profile generated by a template, these changes will 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 it in the agent profile by editing that value on the desktop. The system changes the modified value back to Central Management in the respective agent's profile. This allows the agent to edit fields that are not set as read-only, but takes advantage of all the other settings that you have configured. The fields, set as read-only, appears 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. For some configurations, only an **All on this page** check box is available, which sets all the fields for the corresponding page as read-only. The administrators must mark the fields as read-only in order to avoid inconvenience to the Avaya one-X Agent client users as the users require various features of the Avaya one-X Agent client for daily use.

You can edit the template that are 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:

A **Reset** button also appears on all the configuration panels. The **Reset** button clears all the entries you apply to the data fields.

Related topics:

Creating templates on page 43
Finding templates on page 43
Configuring the Telephony Login settings on page 44
Configuring the Alternate Server addresses on page 44
Configuring the Agent Login settings on page 45
Configuring the IM Login settings on page 46
Viewing Phone Numbers on page 46
Configuring the Work Handling settings on page 47
Configuring the Audio Greetings settings on page 47
Configuring the Screen Pop settings on page 48
Configuring the Launch Applications settings on page 50
Configuring the Directory settings on page 50
Configuring the Work Log settings on page 51
Configuring the Voice Mail Integration settings on page 52
Configuring the Reason Code settings on page 52
Configuring the Event Logging settings on page 54
Configuring the Outlook Contacts settings on page 55
Configuring the Dialing Rules settings on page 56
Configuring the Touch Tone Shortcuts settings on page 58
Configuring the Video - Basic settings on page 58
Configuring the Video - Advanced settings on page 59
Configuring the IM settings on page 60
Configuring the IM Responses settings on page 61
Configuring the TTY - General settings on page 62
Configuring the TTY- Abbreviations settings on page 63
Configuring the Call Handling settings on page 63
Configuring the User Interface settings on page 64

Creating templates

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

Use the following procedure to create parent and child templates. Ensure that you click the **Add** button against the existing parent template from which you want to derive a new child template.

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

   The **Manage Templates** page appears with the list of templates.

   Note:

   If you have logged on to the Central Management Web interface for the first time, only the default template appears.

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

   The system adds a *<new template>* file and displays it as a child template under default or new parent template. The **Template Details** pop-up window appears.

   Note:

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

3. In the **Template name** field, enter an 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 this new template file and displays it as a child template under default or new parent template.

Finding templates

Use the following procedure to find a template.

1. In the **Central Management** navigation page, click **Manage Templates**.
   The **Manage Templates** page appears 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.
   Templates matching the search key appears on the page.
3. To find the filtered templates, click the **Previous Result** or **Next Result** link.

Configuring the Telephony Login settings

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Login - Telephony**.

   The Login - Telephony window appears.
2. Make necessary changes to the fields. For field descriptions, refer to Telephony Login panel field descriptions on page 75.
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**.

Related topics:

Telephony Login panel field descriptions on page 75

Configuring the Alternate Server addresses

The Alternate Server address feature allows you to specify alternate registration servers, if the main registration server defined on the telephony login screen is not available.

Note:

This 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, allows a successful RAS session to be set up to begin with.

Prerequisites

Obtain all alternate server addresses.

1. Under **Template Details**, click **Alternate Servers**.
   The Alternate Servers window appears.
2. Click **Add Server**.
3. In the **Server Address** field, enter the IP Address or FQDN of the alternate server.
   The IP address appears in the **Alternate Servers** fields.

   To add more servers to the list, repeat the above steps.
4. 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.
5. Use the **Up** and **Down** buttons to arrange the order of the servers the system must try in a sequence.
6. To mark the **Server Address** field as read-only in the Avaya one-X Agent user interface, select the **Select read only values** option.
7. Click **Save**.

Related topics:

Alternate Server List panel field descriptions on page 77

Configuring the Agent Login settings

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Detail**, click **Login - Agent**.

   The Login - Agent window appears.
2. Makes necessary changes to the fields. For field descriptions, refer to Agent Login panel field descriptions on page 77.
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**.

Related topics:
Agent Login panel field descriptions on page 77

Configuring the IM Login settings

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Login - IM**.
   The Login - IM window appears.
2. Make necessary changes to the fields. For field descriptions, refer to IM login field descriptions on page 78.
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**.

Related topics:
IM login field descriptions on page 78

Viewing Phone Numbers

Prerequisites

Agent must have added additional phone numbers to view the numbers on this page.

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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, then edit the user profile to add the **Other Phone** configuration that the user can use.

1. Under **Template Details**, click **Phone Numbers**.
   The Phone numbers window appears with phone numbers if an agent has added the phone number as **Other Phone**.
2. Select a number from the **Phone numbers** list.

The name and number appears 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.

   You, as an administrator, can add phone numbers by editing a user's profile on the Manage Users page.
4. Click **Save**.

Related topics:
Phone Numbers panel field descriptions on page 79

Configuring the Work Handling settings

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

1. Under **Template Details**, click **Work Handling**.

   The Work Handling page appears.
2. Select the appropriate options to set the required work handling behavior. Refer to the Work Handling panel field descriptions on page 80 to select the correct options.
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**.

Related topics:
Work Handling panel field descriptions on page 80

Configuring the Audio Greetings settings

Agents can play pre-recorded audio greeting for incoming calls. Agents can record these greetings as standard responses for specific clients, or skills for which this template is developed. An agent or you, can configure greeting triggers to play a specific audio greeting on receiving calls from specific numbers, VDNs, or Prompted Digits.

Prerequisites

Agent must have added at least one greeting to configure greetings.

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Audio Greetings**.

   The Audio Greetings window appears.
2. Click **Add Audio Greeting** to define a new audio greeting.

   A <new entry> file appears in list.
3. In the **Name** field, enter the audio greetings.
4. In the **Description** field, describe the audio greetings.
5. Makes 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**.

Related topics:

Audio Greetings panel field descriptions on page 82

Configuring the Screen Pop settings

Screen Pops are applications, Web pages, or information that appear 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. Under **Template Details**, click **Screen Pop**.

   The Screen Pop window appears.
2. Click **Add Screen Pop**.

   A <new entry> Screen Pop appears in the list box below.
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 from those mentioned above. 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 choices from **Inbound call is**:
   - **Ringing**
   - **Answered**
   - **Missed**
   - **Released**
8. To see a screen pop trigger for outbound calls, select one of the following choices from **Outbound call is**:
   - **Connected**
   - **Released**
9. If you want the screen pop to start when an incoming calls appears on a specific VDN, select **Trigger only when VDN is** and enter a VDN in the text box.

   Caution:
   Avaya recommends that you create VDNs, which are not more than 15 characters long on Communication Manager. This can cause a VDN to 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**.

Related topics:
Screen Pops panel field descriptions

Configuring the Launch Applications 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 this 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. Under **Template Details**, click **Launch Applications**.
   The **Launch Applications** window appears.
2. Click **Add Application**.
   An untitled application item appears.
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. Optionally, 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**.

Related topics:
Launch Applications panel field descriptions on page 85

Configuring the Directory settings

Public Directory provides access to corporate or public directory services. It 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).

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Directory**.

   The Directory window appears.
2. Click the **Add Directory**.

   An untitled item appears in the directory list.
3. Makes necessary changes to the fields. For field descriptions, refer to Directory panel field descriptions on page 87.
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**.

Related topics:
Directory panel field descriptions on page 87

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. Under **Template Details**, click **Work Log**.

   The **Work Log** window appears.
2. Makes necessary changes to the fields. For field descriptions, refer to Work Log panel field descriptions on page 88.
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**.

Related topics:
Work Log panel field descriptions on page 88

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.

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Voice Mail Integration**.
   The **Voice Mail Integration** window appears.
2. In the **Voice Mail Integration** panel, make necessary changes to the fields.
   For more information, refer to the **Voice Mail Integration** panel field description.
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**.

Related topics:
Voice Mail Integration panel field descriptions on page 89

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 this set of codes to specify the reason they are entering the Auxiliary Agent state. For example, agents may be

Code	Description
	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 this set of codes to provide reasons for logging out of Communication Manager ACD. The user can stay connected, but not logged on to ACD as an agent. For example, agent may 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** code and create the logout codes accordingly.
Call Work Codes	Agents select from this set of codes to add to ACD work that describe details about the call in a such a way (through the codes) that an enterprise can track the calls. For example, bad audio, customer very unhappy, customer has called three times about the same problem, or an agent needed expert assistance to resolve customer problem are reported as digit strings to Communication Manager, similar to all the other types of codes.
Supervisor	Supervisors select codes from this 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 this 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 ones. The system sends only the numeric code assigned to each text string to Communication Manager and the reporting systems.

In 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 ones.

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

Related topics:

Importing Codes on page 54
Reason Codes panel field descriptions on page 90

Importing Codes

You can import codes into a template from a properly formatted CSV file. This is a sample CSV file that an administrator can use. These codes are made available to users who have profiles generated from this 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. Under Template Detail, click **Codes**.

   The **Codes** windows appear. To import codes, follow the instructions in the Codes panel and proceed to the next step.
2. 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.
3. 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 this template** shows the number of inherited codes.
4. 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 relates 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. Under **Template Details**, click **Event Logging**.

   The **Event Logging** window appears.
2. Select the appropriate **Logging level** and **Appender** from the lists. Refer to 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 this field only if Remote syslog. logging is set up. If this 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**.

Related topics:

Event Logging panel field descriptions on page 91

Configuring the Outlook Contacts settings

Configuring Outlook Contacts allows an agent to import Outlook Contacts into the agent's Avaya one-X Agent Contact List. You can configure this to a template assigned to an agent or a group of agents, or by directly editing a user's profile.

Prerequisites

Obtain all the required credentials and location addresses.

1. Under **Template Details**, click **Outlook Contacts**.

   The **Outlook Contacts** window appears.
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 time-out in seconds.

   The system sets the time interval after which a search for contact expires.
6. Click **Save**.

Related topics:
Outlook Contacts panel field descriptions on page 92

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. It ensures 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. It 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 this authorization. The Avaya one-X Agent client automatically appends the authorization code as required so the user does not have to enter it each time a call is made.

Use the following steps to configure the dialing rules for the selected template.

1. Under **Template Details**, click **Dialing Rules**.
   The **Dialing Rules** window appears.
2. In the **Number to dial to access outside line** field, specify the number to access an outside line. In North America, this is set to `9`. In Europe, it 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, where multiple local calling area codes are supported, enter them as a comma-separated list. For example, 305,720 if agents 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 the 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, enter `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 `3,5,7`. 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 national long distance number. This 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, this field is set to 2 seconds. You can specify the 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 the authorization code.
    b. In the **Authorization code** field, type the authorization code for the corresponding profile. The 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**.

Related topics:
Dialing Rules field descriptions on page 92

Configuring the Touch Tone Shortcuts settings

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

1. Under **Template Details**, click **Touch Tone Shortcuts** .
   The **Touch Tone Shortcuts** window appears.
2. Click **Add Shortcut**.
   An untitled shortcut appears 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 steps 2 through 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**.

Related topics:
Touch Tone Shortcuts panel field descriptions on page 95

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

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

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Video - Basic**.
   The **Video-Basic** window appears.
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. This option is only enabled for users of the profile/ template where this is administered.
Broadcast video automatically	Starts the video broadcasting immediately after the agent accepts a call on the Avaya one-X Agent client.
Close video window automatically	Closes the video window immediately after the agent ends a video call on the Avaya one-X Agent client.
Open video window automatically on login	Opens the video window in the preview mode on agent login on the Avaya one-X Agent client.
Allow playing video file	Allows an agent to share a video file on the video 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**.

Related topics:
Video Basic field descriptions on page 95

Configuring the Video - Advanced settings

The configuration set for this template is available to all agents assigned with this template.

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Video - Advanced**.

   The Video - Advanced window appears.
2. Configure the video settings. To configure the appropriate settings, refer to the **Video Advanced** panel field descriptions
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**.

Related topics:

Video Advanced tab field descriptions on page 96

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

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

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **IM - Settings**.

   The Instant Messaging - Settings window appears.
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.

Options	Description
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 initiates, 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 this 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 responses that the agents can use. You can customize the responses for specific skills or clients the template is created. Conversely, you can also view the responses that agents have set if you all the agents to modify the field.

Prerequisites

Presence Services is required for an agent to use Instant Messaging and these settings.

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **IM - Responses**.

   The Instant Messaging - Responses window appears.
2. Click **Add Response**.

   A <new entry> text appears.
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**.

Related topics:
[Responses tab field descriptions](#) on page 98

Configuring the TTY - General settings

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **TTY-General**.
   The TTY - General window appears.
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 invoke the TTY only for calls originating from the specified numbers in the panel, and perform the following steps:
   a. Click **Add Phone Number**.
      A new entry appears 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 add 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**.

Related topics:
[TTY General tab field descriptions](#) on page 99

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.

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **TTY - Abbreviations**.

   The TTY - Abbreviations window appears.
2. Click **Add TTY abbreviation** to add a new abbreviation.

   A new entry appears 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 abbreviation.
   c. In the **Literal Meaning** field, enter the expansion of the abbreviation.

      The Literal Meaning can be a literal text the abbreviation is derived, for instance, 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**.

Related topics:

Abbreviations tab field descriptions on page 100

Configuring the Call Handling settings

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

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **Call Handling**.

   The Call Handling window appears.
2. Configure the call handling settings. To configure the appropriate settings, refer to Call Handling panel field descriptions on page 100.
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**.

Related topics:

Call Handling panel field descriptions on page 100

Configuring the User Interface settings

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

Use the following steps after selecting the template to configure. The **Template Detail** page appears. 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. Under **Template Details**, click **User Interface**.

   The User Interface window appears.
2. Configure the User Interface settings. To configure the appropriate settings, refer to User Interface panel field descriptions on page 101.
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**.

Related topics:

User Interface panel field descriptions on page 101

Contact lists

Contact lists are used for adding a group of related contacts to one or more agents' 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 with 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. The bulk import feature saves the effort and time required for adding individual contact to the contact list.

Related topics:

Importing multiple contacts on page 65
Adding a contact list on page 69
Attaching contact list to templates on page 71
Filtering and sorting the contact list table on page 72
Detaching contact list from a template on page 73

Importing multiple contacts

You can import multiple contacts into 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 new contact appears 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 Central Management and save it as *Unicode Text* file. If you have an old CSV file with data, you can save it as a *Unicode Text* file and import.

Tip:

Avaya recommends creating 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 effort of assigning templates post 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 do 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 order of column headings, which is as follows:

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 this column. If the contact list name that you specify does not match with the one in Central Management, the contact will not be added to the contact list.
First Name	Enter the first name of the contact.
Last Name	Enter the last name of the contact.
Favorite	Do one of the following: - 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 favorite.
Speed Dial	Do one of the following: - 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	There are two columns for work. The first column specifies the work number and the second specifies if the work number must appear on

Column names	Column values
	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 appears on speed-dial of the agent's desktop. In 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 e-mail address of the contact.
IM	There are two columns for internet messaging (IM) login name. The first column specifies the IM login name

Column names	Column values
	and the second specifies if the IM login name must appear on speed-dial. In the first column type 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.

Use 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 given above.

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.

Contacts are imported into Central Management.

Next steps

You can view the imported users groups on the Manage Contact Lists page.

Adding a contact list

1. On the Central Management navigation menu, click **Manage Contact Lists**.
   The Manage Contact Lists page appears.
2. Click **Create contact list**.
   The Contact List Details page appears 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 **Contact list name** field and click the **Add contact list member** link.
   This is a mandatory field.
4. Click **Save**.
   The new contact list appears in the **Contact list name** column.

Related topics:

Adding members to contact list on page 69
Editing contact list member details on page 70
Deleting contact list members on page 71

Adding members to contact list

1. On the Central Management navigation menu, click **Manage Contact Lists**.
   The Manage Contact Lists page appears.
2. Click a contact list name to which you want to add members.
   The Contact List Details page appears at the bottom with the following tabs:

- **Contact list details** tab
- **Members** tab
- **Templates** tab

3. Click the **Members** tab.
   The member list appears.
4. Click the **Add contact list member** link.
   The Contact Details window appears.
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 newly added member appears 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 new template appears in the template list.
   b. Click the **Template settings** link to view the template settings corresponding to the assigned template in the view column.
      A new window appears with the template settings.
10. Click **Save**.

Related topics:
Contact Details dialog box field descriptions on page 102

Editing contact list member details

1. On the Central Management navigation menu, click **Manage Contact Lists**.
   The Manage Contact Lists page appears.
2. Click the contact list name to which you want to add members.
   The Contact List Details appears 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 whom you want to make changes.
   The corresponding member details appear in the Contact Details window.
5. In the Contact Details window, make the necessary changes and click **Save**.

Related topics:
Contact Details dialog box field descriptions on page 102

Deleting contact list members

1. On the Central Management navigation menu, click **Manage Contact Lists**.
   The Manage Contact Lists page appears.
2. Click the contact list name to which you want to add members.
   The Contact List Details page appears at the bottom with the following tabs:
   - **Contact list details** tab
   - **Members** tab
   - **Templates** tab
3. Click the **Members** tab.
   The **Members** tab appears 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 creating 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 Manage Contact Lists page appears.
2. Click the contact list name to which you want to add the members.
   The Contact List Details appears 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 the **Add** button.
   The contact list applies to the selected template and the template appears in the **Template name** list.

   Note:
   In the Template tab:
   - The **Template settings** link allows you to view the template settings to which the contact list is attached. The template settings appear in a separate pop-up window; however, you cannot edit them in the pop-up window.
   - The **Manage Templates** link opens the Manage Templates page to check the template hierarchy and the templates to which it inherits the contact list, in addition to the one that you have attached.

   The attached contact list appears in the **Contact lists** column to the corresponding template name in the Manage Templates page. If the contact list names exceed the column width, you can move adjust the **Contact lists** column against 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 Manage Contact Lists page appears.

2. To find a contact list by name, type the keywords in the **Filter** field.
   All names matching the keyword dynamically appear in the contact list.
3. To find a contact list by template, select a template from the **By template** list.
   All templates matching the keyword dynamically appear in the contact list.
4. To sort the list, perform one of the following steps:
   - To sort by contact list name, click **Contact list name** column header.

     The list toggles between alphabetical ascending and descending order.
   - To sort by date, click **Last modified** column header.

     The list toggles between date-wise ascending and descending order.

Detaching 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, click **Manage Contact Lists**.
   The Manage Contact Lists page appears.
2. Click the contact list name to which you want to remove the template:
   The Contact List Details page appears 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.
   The system detaches the template from the associated contact list.

Chapter 5: Central Management configuration field descriptions

Telephony Login panel field descriptions

The Telephony Login panel provides the following controls:

Name	Description
Enable automatic connection to Communication Manager	Automatically registers the telephone extension with Communication Manager using the previous successful registration. If cleared, prompts to provide settings at each login.
Extension	Use this field to register the extension number in conjunction with Avaya one-X Agent.
Password	Use this field to register the numeric password associated with the specified extension number.
Save password during sign in	Use this option to save the password on signing in with the associated extension number for subsequent logins.
CM Auto Answer Support Required	Use this option to provide auto-answer support if the agent's extension is so administered on Communication Manager.
Warn for Another User Logged in at Extension	Use this option if you want the system to displays a warning message if a user has logged in with the same extension from another location.
Server Address	Use this field to enter the IP address or FQDN of the primary registration server. A connection must be made to allow the registration to proceed. Refer to the Alternate Server List administration for backup registration addresses.
User Type	Sets one of the following user types: • **Agent** (default option): To log in as an agent • **Non-agent**: To log in as an extension • **Supervisor**: To log in as supervisor

Name	Description
	Important: The **Basic** user type (license) is removed and the **License** field is renamed to agent as **User Type** in the Avaya one-X Agent 2.5 release. If older profiles in Avaya one-X Agent 2.0 have **Basic** user type (license), the application uses **Agent** as **User Type** with **Desk Phone** as default modes.
Place and receive calls using	Use this option to set the telephone line to register the telephone settings with Communication Manager. Depending upon the location, telephone set, and access network, select one of the following settings: • **My Computer**: To register agent personal computer as a phone with Communication Manager. • **Desk Phone**: To register the office desk phone with Communication Manager.
Other Phone	Select an existing **Other Phone** number (defined in the **Phone Numbers** settings) or enter a new **Other Phone** number in an individual user's profile (Manage Users) to set the phone to be used to place and receive calls by that user (Telecommuter mode). **Note:** You can enter a valid phone number in the **Other Phone** field and click **Save**. The phone number gets saved as **Other Phone**: `xxxxx` in the **Place and receive calls using** field. It also gets saved in the Phone Numbers settings section of this user profile.
Telephone at	Appears only on the client user interface, if **Other Phone** is selected from **Place and receive call using** list. The telephone can be an analog telephone, a cellular telephone, or an extension on a local or remote switch. **Note:** The **Telephone at** field appears during a log in sequence. The system uses the number as a temporary sign in and does not store the phone number in the Phone Numbers panel in the System Settings.

Related topics:

Configuring the Telephony Login settings on page 44

Alternate Server List panel field descriptions

The Alternate Server List panel contains the following controls:

Name	Description
Alternate Servers	The Alternate Servers list displays all the IP addresses of alternate servers. You must not enter the IP address of primary server in this list.
Server address	Use this field to enter the IP address of the alternate server.
Maximum attempts of each server	Use this field to specify the number of attempts the system must make to establish connection with the server before switching to the next server in the list, if defined. The minimum value for this option is 2.

Button	Description
Add Server	Clicking **Add Server** creates an item in the **Alternate Servers** list.
Delete Server	Clicking **Delete Server** removes the corresponding server from the **Alternate Servers** list.
Up	Clicking **Up** moves the selected alternate item above its current position in the **Alternate Servers** list.
Down	Clicking **Down** moves the selected alternate item below its current position in the **Alternate Servers** list.

Related topics:

Configuring the Alternate Server addresses on page 44

Agent Login panel field descriptions

The Agent Login panel contains the following controls:

Name	Description
Enable ACD Login	Use this option to enable the ACD feature. When you enable this option, you must provide the required user credentials to log in to the ACD Services. By default, the option is enabled.

Name	Description
	Note: The ACD tab will not appear if you have logged in as a Non-Agent or if appropriate buttons are been administered for this extension.
Automatically sign into the ACD server	Use this option if you want Avaya one-X Agent to automatically log the user on to the ACD after successfully registering the extension with Communication Manager.
Agent	Use this field to enter the agent login ID
Password	Use this to enter the agent login password.
Remember password for next login	Saves the password associated with the agent extension number. This saves the effort to enter the password again at the next sign in.
Default Agent State upon ACD connection	Sets the default agent state after successful connection with the ACD service. You can set the default agent state to: • **Ready** — Choose this option for immediate availability after the ACD connection. • **Auxiliary** — Choose this option for setting up work space and to adjust the application preferences immediately after the ACD connection.

Related topics:

Configuring the Agent Login settings on page 45

IM login field descriptions

The IM-Login panel contains the following settings:

Name	Description
Automatically connect to IM Server	Select this option to allow agent to connect to the Presence Services server automatically after registration of the user's telephony extension.
User ID	Enter the user name registered on the IM server.
Password	Enter the IM password.
Domain	Enter the domain name of the IM server.

Name	Description
Remember password for next login	Select this option if you want the system to save the password for the subsequent login.
IM Server Address	Enter the IP address of the IM server.

Related topics:

Configuring the IM Login settings on page 46

Phone Numbers panel field descriptions

Phone numbers relate to a specific user, and can only be set in a User profile. To prevent all agents using this template from adding their own phone numbers in the client, check the read only option. You can still add phone numbers by editing a user's profile on the Manage Users page.

The Phone Number panel contains the following controls:

Name	Description
Phone numbers	This field list displays the phone configuration along with the user-created telephone numbers. **Note:** You can rename the phone number by clicking the corresponding items.
Phone name	Use this field to specify the name of the telephone for the corresponding phone.
Phone number	Use this field to specify the telephone number for the corresponding phone configuration.

Button	Description
Add	Clicking **Add** creates a new item in the Phone Number list.
Remove	Clicking **Remove** deletes the item from the Phone Number list.

Related topics:

Viewing Phone Numbers on page 46

Work Handling panel field descriptions

The Work Handling panel contains the following controls:

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>BASIC CONTROLS</td><td></td></tr>
<tr><td>Work Completion for ACD calls</td><td>Use the following options to configure the Work Completion settings for ACD calls:
Auto-complete: Select this option if you want the agent to perform change the work states to Ready immediately after the ACD completes. The agent can, on a call by call basis, override this option if it is set, and perform Follow Up Work. If the agent does this, the Auto Complete option is restored for the subsequent calls.
Allow Follow-Up: Select this option if you want to the agent to perform Follow Up Work on ACD calls. The agent can, on a call by call basis, override this option to have the work completed automatically when the ACD call ends. On the next and subsequent calls, the Follow Up option will be in force.
Timed Follow-Up: This option is available, if the Allow Follow-Up option is set for work completion for ACD calls. The agent can specify the time in seconds to follow-up tasks in the Time Period field .
Allow extending Follow-Up: Use this option if you want the agent to extend the timed follow-up period that is defined above.</td></tr>
<tr><td>Transitions to Ready State</td><td>Use the following options to configure the transition state:
Auto-Ready: Enable this option, if you want the agent's system to automatically change the agent status to ready after completing the work item.
Manual-Ready: Enable this option if you want the agent to change the agent state to AUX status after completing the work item.

With Aux Code: The AUX state works in conjunction with AUX code. If you have defined a reason code for AUX, the option will be available in the drop-down list.</td></tr>
</table>

Name	Description
ADVANCED CONTROLS	
Work items	Use the following options to configure the Work Item settings: • **Auto-Accept**: Enable this option, if you want the agent's system to answer the call automatically. This feature is not related to **CM Auto Answer Support Required** on the Login window. However, either use the Communication Manager **Auto Answer** feature with Avaya one-X Agent support, or this **Auto Accept** feature. Do not use the features together. • **Manual-Accept**: Use this option if you want the agent to answer each call manually, or if you have administered Auto Answer in Communication Manager.
Communication Manager Ready Mode	Use the following options to configure the Communication Manager Ready Mode settings: • **Auto In**: Use this option only if you want to override Avaya one-X Agent application handling. It must only be used if the user wants to use the Communication Manager timed after call work feature and other Communication Manager **Auto-in** features incompatible with the Avaya one-X Agent application behavior. This feature is not related to **CM Auto Answer Support Required** displayed on the Login window. However, the functionality is the same. • **Manual In**: This is the default option, and must always be in the assigned state to allow the Avaya one-X Agent application to perform its work. You must not get confused with Communication Manager use of the same names. The classic CM In behaviors are controlled in Avaya one-X Agent by Auto Ready and Manual Ready settings on the front tab.

Related topics:

Configuring the Work Handling settings on page 47