Avaya Agile Communication Environment™ Administration — Microsoft Office Communications Server Integration

Release 2.3.2
NN10850-012, 07.02
March 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 AVAYAAFFILIATE 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 types

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

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

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

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

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

Avaya ACE is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

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: New in this Release

The following details what's new in *Avaya Agile Communication Environment™ Administration — Microsoft Office Communications Server Integration* (NN10850-012) for release 2.3.1 and 2.3.2.

Microsoft Communicator Add-in

Avaya Agile Communication Environment™ (ACE) Release 2.3.1 introduces Microsoft Communicator Add-in. The Communicator Add-in is a new method of integration to Office Communications Sever (OCS). In this release, the Communicator Add-in can be deployed with the service provider Avaya Aura Communication Server release 5.2.1 and higher. Subsequent release will expand support for other service providers.

Avaya Agile Communication Environment™ (ACE) Release 2.3.2 contains the following Avaya ACE Microsoft Communicator Add-in enhancements:

- Microsoft Communicator Add-in supports "click-to-call" from Microsoft Office (2007 and 2010) and Internet Explorer (R6 to 8). When a call is initiated from these desktop applications, the Avaya ACE Communicator Add-in Conversation Window opens for mid call control. The call is set up using desk phone or computer mode options in the Communicator Add-in toolbar.
- Computer mode has been enhanced with the addition of Dial pad for DTMF, call forwarding, mute and volume controls.
- Phone Mode has been enhanced with support for CS 1000 Release 5.5 to 7.0.
- Microsoft Communicator Add-in is now localized in the following languages:
    - Simplified Chinese
    - Japanese
    - Korean
    - English
    - French
    - German
    - Italian
    - Russian
    - Lat-Spanish
    - Brazilian-Portuguese

Deprecated support

Support for Avaya Aura Communication Manager, Avaya CS 1000 and Cisco Unfied Communication Manager utilizing Remote Call Control capabilities through the Microsoft UCMA API has been deprecated for this release. The CS 2000 continues to utilize this method.

Chapter 2: Introduction

Avaya ACE™ provides two independent OCS Integration solutions:

- A client side integration of the Avaya ACE Microsoft Communicator Add-in which is applicable to the Avaya Aura® Communication Manager, the Avaya Communication Server 1000, and the Cisco Unified Communication Server.
- A server side integration applicable to the Genband Communication Server 2000 solution.

Both of these solutions provide the end user with the ability to have their telephony presence published to OCS and allow OCS to control their communication device. Features and functionality will differ with the solutions and the communication infrastructure utilized. These features are expanded upon within this document.

- Information on the Avaya ACE Communicator Add-in solution starts with Avaya ACE Microsoft Communicator Add-in on page 13.
- Information on the Communication Server 2000 solution starts with Remote Call Control capabilities utilizing Microsoft UCMA API on page 49.

Avaya ACE™ documentation

Before using Avaya ACE, familiarize yourself with the following documentation resources.

Avaya ACE documentation

These documents provide information on Avaya ACE fundamentals, planning, software ordering, installation, Avaya and third-party system solution integration, web service application programming interfaces (APIs), administration, security, fault and performance management, troubleshooting, and core applications/APIs delivered with the base software (Personal Assistant, Message Drop and Blast API).

Avaya ACE application documentation

The application documentation includes information on the planning, installing, administration, and use of the Application Integration Engine (AIE) platform and the applications it hosts, Microsoft and IBM desktop integration solutions, and all other prepackaged Avaya ACE applications.

Avaya ACE Release Notes

The Avaya ACE release notes describe operational considerations for a specific release of Avaya ACE. You can download this document from avaya.com/support. It is important to carefully review the release notes for the Avaya ACE release you support prior to a software

install or upgrade. In addition, this document is a helpful reference for the ongoing support and use of Avaya ACE.

Obtaining documents

- All Avaya ACE documentation is available from the Avaya support web site at https://support.avaya.com.
- Avaya ACE documentation is available
  - on the **Avaya ACE Server** disk
  - from the Avaya ACE GUI **Help** menu
  - on the Avaya ACE server under the Linux folder `/opt/avaya/ace/doc/NTP` or under the Windows folder `\Program Files\Avaya\Avaya ACE\ace\doc\NTP`.
- Avaya ACE application documentation is available
  - on the **Avaya ACE Applications** disk
  - from the AIE GUI **Help** menu (for applications hosted through the AIE)

Avaya ACE™ professional services and support

Avaya ACE combines industry-leading consulting and design services with the right mix of custom development and communications integration capabilities, providing communications solutions that meet business needs now and in the future.

- Consulting and solution design: Help customers understand and design communications solutions holistically, ensuring all elements of the solution are addressed and aligned.
- Solution development and customization: Ensure the enterprise's unique requirements are met.
- Solution integration and implementation: Ensure the solution is deployed and integrated within the network and communications infrastructure and applications effectively, to achieve organizational and business goals.
- Project management and ongoing solution maintenance: Help enterprises manage and maintain their network and communications infrastructure.
- Business optimization: Ensure the deployed solution delivers maximum performance.

Avaya Global Services

Avaya Global Services delivers world-class support in three areas: Avaya Professional Services, Avaya Support Services, and Avaya Operations Services.

Avaya Professional Services

Avaya Professional Services consultants are technically proficient, possess strong business acumen and have developed vertical industry specialization to help you address the challenges of today’s converged voice, video and data communications environments. At the same time,

we actively help you look for ways to optimize your communications environment to better enable your people, increase your business agility, and drive costs out of your operations.

Avaya Support Services

Avaya Support Services are backed by global resources, including more than 5,800 industry-certified service desk and backbone engineers and 34 regional network operations centers delivering 24x7 monitoring, diagnostics and problem resolution, as well as support in 14 languages.

Avaya Operations Services

Avaya Operations Services are available for customers that want to out-task the proactive management and monitoring of their communications infrastructure. These services can be delivered by Avaya directly or may be private-labeled and co-delivered by Avaya authorized partners.

Navigation

Chapter 3: Avaya ACE™ Microsoft Communicator Add-in

Network administrators can integrate the Avaya Agile Communication Environment™ (ACE) into their Microsoft Office Communications Server 2007 (OCS) network infrastructure to enhance existing communication services. Avaya ACE™ supports unified communication (UC) desktop integration with OCS 2007 R2 Microsoft Office Communicator Clients. Leveraging Avaya ACE web services and user profile management, OCS administrators can provide unified communication services to Office Communicator clients utilizing their Avaya Aura® Communication Manager, Avaya Communication Server 1000, or Cisco Unified Communication Service provider. Note that supported features may differ by service provider and where differences occur, they are indicated in this document.

Avaya ACE OCS Integration is client side. The Avaya ACE Communicator Add-in is an add-in application that extends Microsoft Office Communicator functionality using Microsoft Office Communicator supported APIs. The Communicator Add-in extends Microsoft Office Communicator by providing two telephony modes, Phone and Computer mode.

- Phone mode allows Communicator to control the desk phone. The Communicator Add-in uses Restful HTTP to integrate with ACE Application Integration Engine to control media anchored on the phone.
- Computer mode allows Communicator to use the Computer as a phone. The Communicator Add-in uses Avaya UC Desktop Engine capabilities to use media capabilities of the computer.

The Avaya ACE solution integrates telephony capabilities into OCS, but requires only an OCS 2007 R2 Standard CAL.

The Avaya ACE OCS Integration solution supports controlling the user's primary line using the Communicator Add-in. Phone mode allows the user to control the desktop phone, with media going over existing PBX telephony equipment. Computer mode allows the user to use the computer as a phone, using the media capabilities of the computer.

The solution supports the following functionality:

- Support Microsoft Office Communicator 2007 R2 user interface to provide voice services utilizing Avaya Aura Communication Manager, Avaya Communications Server 1000, or Cisco Unified Communication Manager voice infrastructure (See topology diagrams below).
- Support for Computer (soft client) and Phone (CTI control of Desk phone) modes.
- Make Calls from OC Contact list, or search dialog box utilizing contacts OC published numbers.
- In conjunction with the Office Add-in and Web Browser Add-in applications, Make Calls from Microsoft Office applications ad Internet Explorer (see *Avaya Agile Communication Environment™ Web Browser and Office Add-ins Application Fundamentals* (NN10850-031).

- Translate E164 numbers to customer dial plan including insertion or deletion of appropriate digits.
- Publish Telephony Presences on behalf of the user when their client is signed in and on a call.
- Display a conversation window with the following mid-call functionality:
  - Release/End call
  - Place call on Hold and Retrieve call
  - Insert DTMF digit in to an established call.
  - Speaker volume control and speaker mute function (Computer mode).
  - Microphone mute function (Computer mode).
- Display an incoming call window with the following functionality:
  - Indicate the Incoming Caller line ID or Caller name
  - Allows the user to Answer the call or Divert (Phone mode) to one of their specified devices
  - Graphically indicate which device (Computer or Phone mode) the call will be answered on
- Select Computer or Phone Modes
- Set Call Forward options

Microsoft Office Communication System 2007 R2 can be deployed within an Enterprise or as a hosted service, Business Productivity Online Suite (BPOS). In both of these deployment the Avaya ACE Microsoft Communicator Add-in will inter operate with Communicator client deployed on the users PC. The following diagram represents Avaya ACE deployed within an Enterprise. For Avaya ACE deployed in a hosted service configuration, see Communicator Add-in support for Microsoft BPOS on page 23.

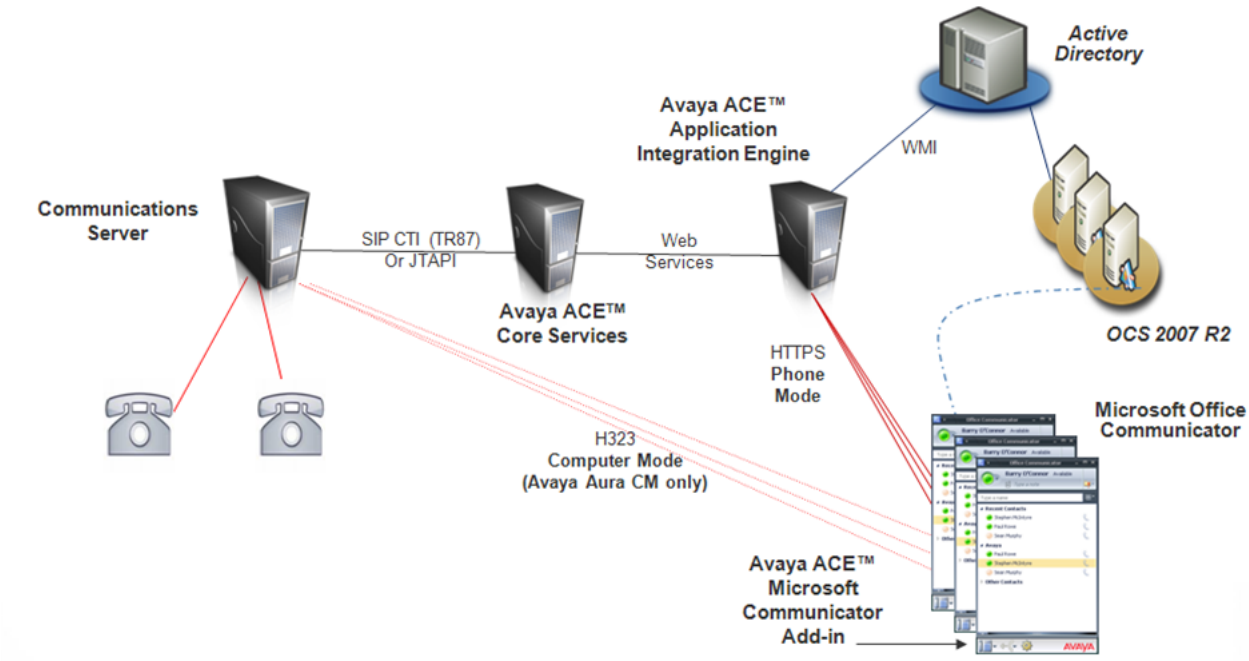


Figure 1: Avaya ACE deployed in an Enterprise with the Communicator Add-in

The following section describes the key components of the Avaya ACE Microsoft Communicator Add-in with Microsoft Office Communication Server 2007 R2 deployed within an Enterprise.

- Microsoft Office Communicator 2007 R2 release 3.5.6907.196 or above
- Avaya ACE Microsoft Communicator (MC) Add-in
- Microsoft Office Communicator Server 2007 R2
- Avaya ACE core services
- Avaya ACE Integration Engine (AIE)
- Service provider
- Desk phone which can be CTI controlled

Communicator Add-in Key Components

The Communicator Add-in features the following key components.

Microsoft Office Communicator

Microsoft's Office Communicator is the unified communication desktop client providing IM and presence capabilities to the overall solution. Microsoft's Office Communications Server delivers IM and presence aggregation services to the end user.

Avaya ACE Microsoft Communicator Add-in

This is a client side add-in to Microsoft Office Communicator 2007 R2. It utilizes the Office Communicator User interface to drive Avaya Voice capabilities to the end user. The Communicator Add-in operates in two modes. In Computer mode, it utilizes the Avaya Unified Communication (UC) desktop engine to deliver soft client functionality. In Phone mode it utilizes the AIE Restful Session Control Services to provide CTI control over the end user's desk phone.

The AIE must be available for the Communicator Add-in to operate in either Phone or Computer mode.

Microsoft Office Communicator Server 2007 R2

Microsoft Office Communicator Server (OCS) 2007 R2 provides the end user with the IM and Presence aggregation functionality. The Avaya ACE Microsoft Communicator Add-in builds on this OCS functionality and its Communicator client user interface to deliver an Avaya voice experience.

Active Directory

AIE accesses Active Directory to determine which OCS user it will service. If the OCS user has an Avaya ACE profile, then AIE will deliver voice and telephony presence services to the user's Office Communicator client and allow this user to control the end devices registered in their profile.

Avaya ACE™

Provides the integration point to the customer’s multivendor Communication system environment through vendor specific protocol adaptors. ACE core Service interacts with these Communication system on a signaling bases only it relies on the underlining communication infrastructure to control the media. This allows ACE to monitor and control end user devices. It maintains a profile of the end user’s services and devices. One of ACE Cores Services, ACE Address Manager, converts E164 Numbers used by OCS to the number formats which can be used by the Communication System.

Avaya ACE Application Integration Engine (AIE)

This Server Role hosts the Restful Session Controls Services utilized by the Avaya ACE Microsoft Communicator Add-in to deliver call control functionality over the end user's Avaya Communication system device. These Restful Session Controls Services are delivered over a secure HTTP session. AIE also provides the authentication services used by the Communicator Add-in to ensure the user is a valid OCS, Avaya ACE and Communication Manager user.

Service provider

The following service providers are supported:

- Avaya Aura® Communication Manager (Computer and Phone Mode)
- Communications Server 1000 (Phone Mode)
- Cisco Unified Communication Manager (Phone Mode (Beta))

Network diagrams

The following figures illustrate the network connectivity with the supported service providers.

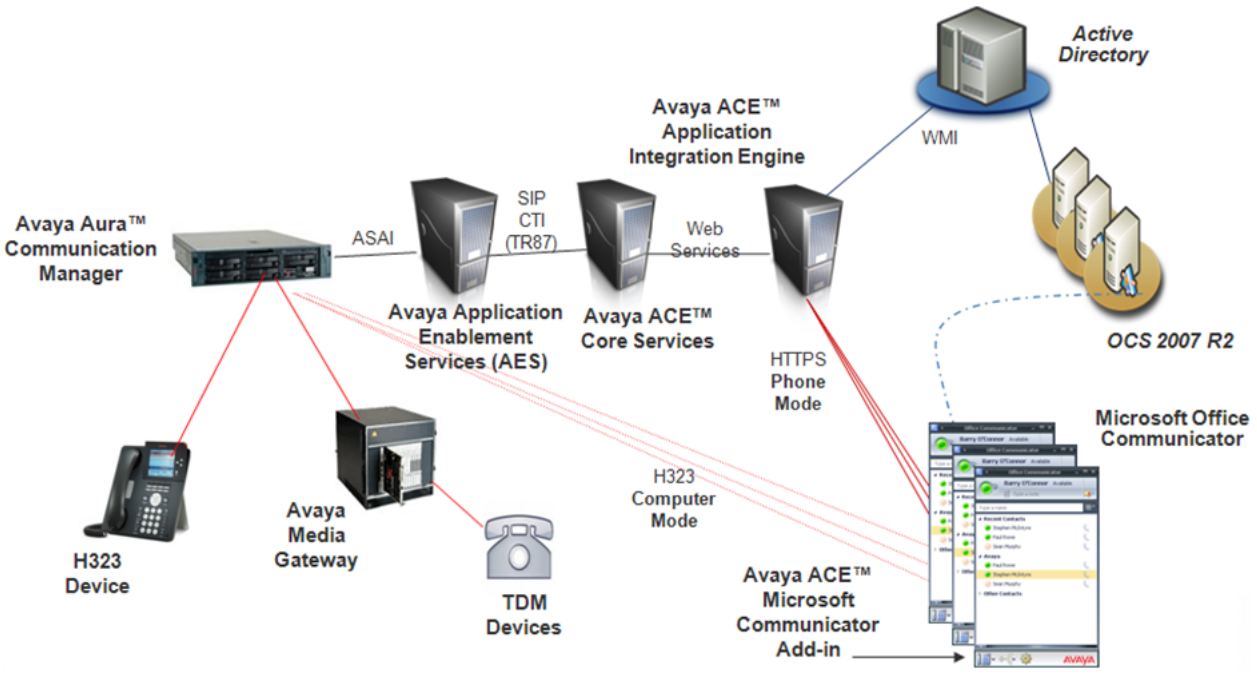


Figure 2: Avaya ACE Communicator Add-in deployed with Avaya Aura™ Communication Manager

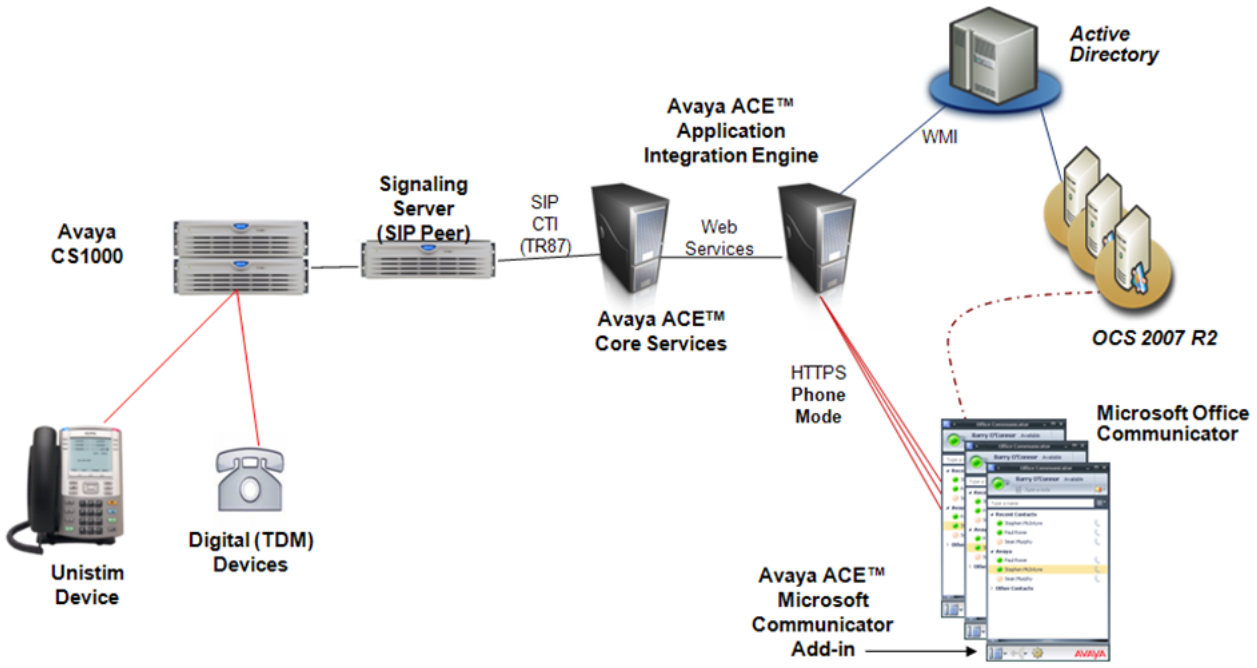


Figure 3: Avaya ACE Communicator Add-in deployed with Avaya Communications Server 1000

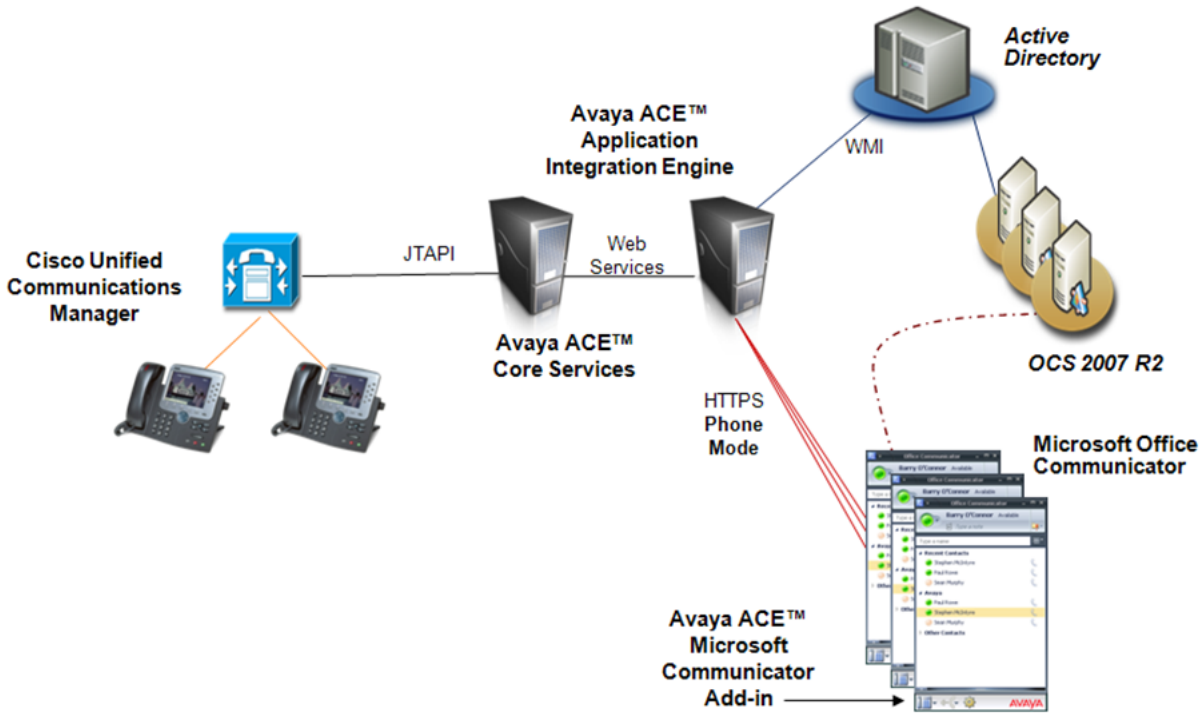


Figure 4: Avaya ACE Communicator Add-in deployed with Cisco Unified Communication Server

Avaya ACE™ telephony services with Communicator Add-in

Avaya ACE OCS Integration is client side. The Avaya ACE Communicator Add-in is an add-in application that extends Microsoft Office Communicator functionality using Communicator supported APIs. The Communicator Add-in extends Communicator by providing two telephony modes: Phone mode and Computer mode.

- Phone mode allows Communicator to control the desk phone. The Communicator Add-in uses Restful Session Control over HTTP to integrate with Avaya ACE Application Integration Engine (AIE) to control media anchored on the phone. Phone mode allows the user to control the desktop phone, with media going over existing communication infrastructure.

  Phone mode is supported on the following service providers:

  - Avaya Aura® Communication Manager
  - Communications Server 1000

- Cisco Unified Communication Manager (Beta)

- In Computer mode, the user can utilize their Communicator client as a soft client (use the Computer as a phone). In this mode, the Communicator Add-in uses the Avaya UC Desktop Engine capabilities to control the computer media interfaces.

  Computer mode is supported on the Avaya Aura® Communication Manager service provider.

Note:

When the Communicator Add-in is in phone mode, you cannot use the Communicator Add-in to control a soft client (Avaya IP Softphone, or One-X Communicator). If the Communicator Add-in detects that One-X Communicator is running, it will attempt to stop the One-X Communicator application.

The Communicator Add-in interacts with the Microsoft Communicator directly using Microsoft Supported APIs. All telephony capabilities are integrated directly between the Communicator Add-in, the Avaya AIE, and Microsoft Communicator. The Avaya ACE solution integrates telephony capabilities into OCS, but requires only an OCS 2007 R2 Standard CAL (license), therefore eliminating the need for a Microsoft voice infrastructure and the Microsoft OCS Enterprise CAL.

Integrating the Communicator Add-in with Microsoft Office Communicator enables telephony services in Communicator. Avaya ACE does not alter the existing functional operation of Communicator. However, the Communicator Add-in does customize and configure Communicator as part of it's installation. For information on using Communicator, see the Microsoft document *Microsoft Office Communicator 2007 R2 Getting Started Guide*.

Note:

If you are using Office Communicator over a Microsoft Remote Desktop session, it is recommended that you use Remote Desktop client version 7.0 or higher. Remote Desktop client software is available from Microsoft.

The Communicator Add-in controls a single line, based on the user's primary line. If the user's desk phone supports multiple lines, non-primary lines will not be represented by the Communicator Add-in.

Table 1: Telephony service matrix

Capability	Description	Phone mode	Computer mode
Make Call	User can make a call on their phone by clicking on a contact in their contact list or entering a number on their Communicator.	Y	Y
Release Call	User can Release a phone call by clicking on the End Call icon in Communicator Add-in Conversation Bar.	Y	Y

Capability	Description	Phone mode	Computer mode
Answer Call	User can accept an incoming call that is presented to them via a pop-up window (toast).	Y	Y
Deflect Call (deflect)	User can redirect an incoming call that is presented to them via a pop-up window (toast).	Y*	N
Caller ID	User receives Calling Party Name in pop-up window.	N	Y
Forward Line	User can activate Call Forward on their PBX line for incoming calls by selecting the CallForward Icon from the Communicator Add-in Communicator Bar.	Y	Y
Call Hold and Retrieve	User can place call on hold using the hold button within the Communicator Add-in Conversation Bar. The Call may be retrieved by selecting anywhere within the conversation bar when the call is in a held state.	Y	Y
Generate Digits (DTMF)	User can inititate sending of DTMF digits through the PBX system by selecting the dialpad icon on the Add-in Conversation bar.	Y	Y
Speaker Control	User can control the speaker volume of an active call by selecting the grey arrow to the right of the Speaker icon on the Add-in Conversation bar. User can mute and un-mute the speaker volume of an active call, by selecting the Speaker icon on the Add-in Conversation bar.	not applicable	Y
Microphone Control	User can mute and un-mute the microphone volume of an active call, by selecting the Microphone icon on the Add-in Conversation bar.	not applicable	Y
Codecs supported	G711, G722 and G729	not applicable	Y
* Not supported with Cisco Unified Communication Manager			

Communicator Add-in telephony service limitations

The Communicator Add-in telephone service has the following limitations.

Avaya component restarts

Avaya Communicator Add-in telephony services are disrupted after an AIE or Avaya ACE application restart. Services may be reduced for 5 to 10 minutes.

OCS restarts

Communicator Add-in will not function during an OCS outage. Within Phone mode, mid-call control may return when OCS becomes available. Users retain the ability to use their Desk phone to make calls until full functionality is restored.

Multiple sessions

While Microsoft Office Communicator allows multiple sessions, the Communicator Add-in does not. The Communicator Add-in cannot be deployed to a shared computer. A single instance of the Communicator Add-in may operate on a workstation at any time. The Communicator Add-in must be deployed for a single OCS user on each workstation to avoid contention for telephony resources.

Having multiple Avaya Soft Phone Clients (Avaya IP Softphone or Avaya One-X Communicator) logged in simultaneously on the same work station is also not supported.

Call Hold and Call Retrieve

- Setting Call Hold or Call Retrieve on a user device is not reflected in Communicator Add-in Call Control Bar.
- After a network connectivity outage between AIE and Avaya ACE, the held state of the call is unknown and should be managed on the device.

Call Forwarding

- Changes in Call Forwarding settings on a line may take five minutes to be reflected within the Communicator Add-in.
- When configuring call forwarding to voice mail, you must configure a corresponding reverse translation rule that is compatible with the network dial plan. The voice mail number must use the E.164 format. If the translation rule is not configured, the Forward to Voice Mail icon does not display in the Communicator Add-in.
- In Computer mode, the Call Forwarding service cannot determine the “forwarded to” number. In Computer mode, Call forwarding appears as on or off.

Dial plan support

The Communicator Add-in telephony services can only support dial plans where the telephony extension is a subset of the public number published in Active Directory and OCS.

Supported Dial Plan example: Extension: 53456, Public Number: +14038753456

Uunsupported Dial Plan example: Extension: 53456, Public Number: +14038713456

Audio controls

- Changes to audio settings on a device may impact other applications using the same audio device.
- When a conversation is initiated, if the audio device setting is already at the lowest setting, the Communicator Add-in will not present the conversation as muted.
- Audio Device settings may appear unsynchronized with the PC settings.
- It is not possible to change audio devices (for example, local sound card to headset) when a call is in progress.
- Audio Settings cannot also be adjusted from the MC Add-in Settings panel, when a call is in progress.

DTMF in Computer Mode

When entering DTMF digits into a conversation, the DTMF tone played back on the speaker may be picked up by the microphone. In this case the digit sequence may be corrupted. There are two workarounds:

- Use a headset when inserting DTMF digits into a conversation
- mute the microphone while DTMF digits are being inserted.

EC500 Integration

- **Phone mode**: When a line has EC500 enabled, and the call is answered on the EC500 forwarded device, the Communicator Add-in is aware of the call and Telephony Presence is published into the Office Communication Server. A Communicator Add-in conversation window appears, including mid-call operation options. In this case, the operations will not control the call.
- **Computer mode**: When a line has EC500 enabled, and a call is answered on the EC500 forwarded device, the Communicator Add-in is aware of the remote call and Telephony Presence is published into the Office Communication Server for the duration of the call. The Communicator Add-in Conversation bar is not presented to the user.

Communicator Add-in presence service limitations

The Communicator Add-in presence service has the following limitations.

Busy in a Call

- If the Communicator is signed-out while the user is on a call (while in Phone mode), the user cannot Sign-in directly as Busy. The user must set the status to busy upon successful sign-in.
- If the user selects **Reset status** while a call is in progress, the presence status changes from Orange/In a Call to Green/Available. If desired, the user must manually set the status to In a Call.

Do Not Disturb

- If the presence status is “Do Not Disturb”, incoming calls are not presented to the user, regardless of the “Level of Access” of the calling contact.
- The exception to the above statement is that if a call is entered ahead of entering the Do Not Disturb state, and the Communicator client is signed out and signed-in again with the same call in progress, a call control window will be presented.

Redundancy limitations

The ACE Communicator Add-in is only supported with AIE in a non-redundant configuration. AIE restarts will result in a temporary loss of functionality.

Communicator Add-in support for Microsoft BPOS

This section describes how Avaya ACE™ integrates with OCS when OCS is deployed within a Microsoft Business Productivity Online Suite (BPOS) environment.

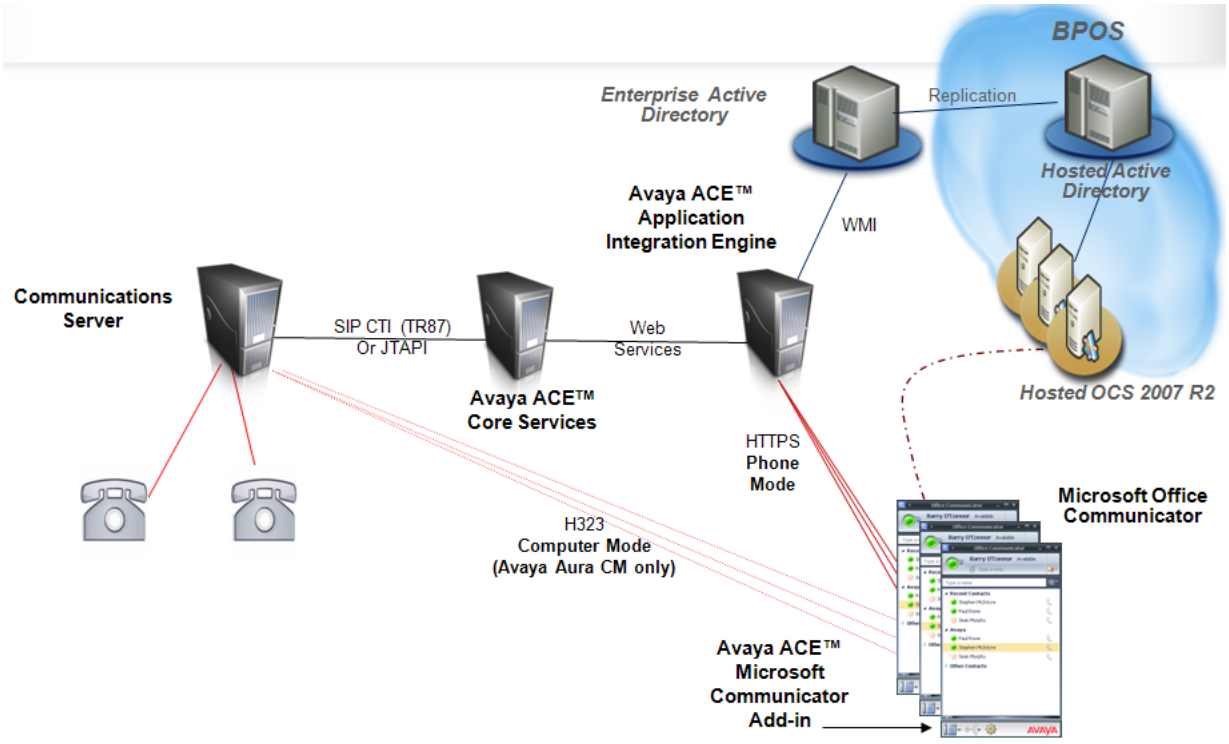


Figure 5: Avaya ACE Communicator Add-in deployed in a Microsoft Business Productivity Online Suite (BPOS) environment

Authentication within a BPOS deployment

Authentication is unchanged within a BPOS deployment. BPOS deployments do not require that Active Directory user data be replicated with a premise Active Directory. The Avaya ACE OCS integration solution does require a premise based Active Directory. When the Communicator Add-in is in phone mode, user authentication occurs within each restful web request to AIE, based on the user credentials of the work station hosting MOC. The AIE must be installed in Active Directory mode and both the AIE and the client PC where the Communicator Add-in is installed must be connected to the same domain. When the Communicator Add-in is in Computer mode, authentication occurs between the Avaya UC engine and the Avaya Communication Manager.

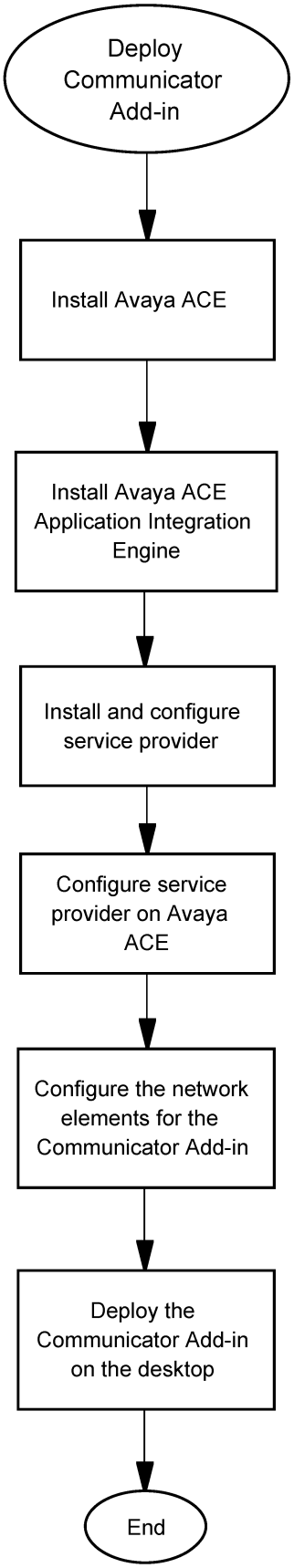
Chapter 4: Deploying Communicator Add-in

This section illustrates the high level work flow required to deploy the Communicator Add-in and lists the requirements for the network components.

Deploying Communicator Add-in work flow

The work flow shows the tasks you perform to deploy the Communicator Add-in.

Note that for the first three tasks, you must refer to information and procedures in the documentation for that network component. The specific documents are referenced in the list of requirements for the component.


Deploy Communicator Add-in
Install Avaya ACE
Install Avaya ACE Application Integration Engine
Install and configure service provider
Configure service provider on Avaya ACE
Configure the network elements for the Communicator Add-in
Deploy the Communicator Add-in on the desktop
End

Navigation

The following procedures are located in this document:

- Configure the network elements for the Communicator Add-in on page 29
- Deploy the Communicator Add-in on the desktop on page 35

Microsoft OCS requirements

- You must have administrator privileges on the OCS server.
- You must be familiar with OCS server administration and OCS server policies.

Avaya ACE requirements

- The Avaya ACE server must be installed and functional. See *Avaya Agile Communication Environment™ Planning and Installation* (NN10850-004).
- You must have administrator privileges on the Avaya ACE server.
- The service provider must be configured. For information about service provider configuration, see *Avaya Agile Communication Environment™ Administration* (NN10850-005).
- You must be familiar with Avaya ACE user management. For more information, see *Avaya Agile Communication Environment™ Administration* (NN10850-005).
- For each instance of the Avaya ACE AIE, a corresponding Avaya ACE user profile must be created and associated with the AIE system user. The AIE system user profile must belong to an Avaya ACE user group of type **System Administrator** or **Group Administrator** and have at minimum, write privileges for the following services:

  - CallForwardingService
  - CallNotificationService
  - ThirdPartyCallService

  For more information on the AIE system user, see *Avaya Agile Communication Environment™ Application Integration Engine Fundamentals* (NN10850–021).
- You must create the Avaya ACE user group **RESTful_Session_Control**. The **RESTful_Session_Control** group must be a child of the group that the AIE system user is a member of.

Avaya ACE Application Integration Engine requirements

- The Avaya ACE Application Integration Engine (AIE) must be installed and configured to communicate with Avaya ACE. See *Avaya Agile Communication Environment™ Application Integration Engine Fundamentals* (NN10850–021).
- The AIE must be deployed as a standalone AIE and installed in Active Directory mode.
- The AIE must be in the same domain as the PC where the Communicator Add-in will be installed.
- The **Enforce HTTPS** setting must be disabled. In the AIE configuration window, the check box for **Enforce HTTPS** must be cleared.

  If you want to disable access to the AIE over HTTP, you must set up firewall rules to block access to the port.

Caution:

Do not block the connection to Avaya ACE. Ensure that communication between AIE and Avaya ACE is allowed on the port.

Avaya Aura requirements

- The Avaya Aura service provider must be configured to use the TR/87 protocol. See the information on TR/87 solutions in *Avaya Agile Communication Environment™ Avaya Aura™ Integration* (NN10850–050).
- Avaya Aura™ Application Enablement (AE) Services 5.2.1 or higher must be installed and configured to communicate with the Avaya Communication Manager service provider and the Avaya Agile Communication Environment™ (ACE). For information on configuring AE Services, see the following documents:
  - *Avaya Agile Communication Environment™ Secure Communication Fundamentals*
  - *Avaya Aura Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007* (Doc ID 02-601893)
  - *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide* (Doc ID 02–300357)

Avaya Communication Server 1000 requirements

The Avaya CS 1000 service provider must be configured to use the TR/87 protocol. See the information on TR/87 solutions in *Avaya Agile Communication Environment™ Communication Server 1000 Integration* (NN10850–023).

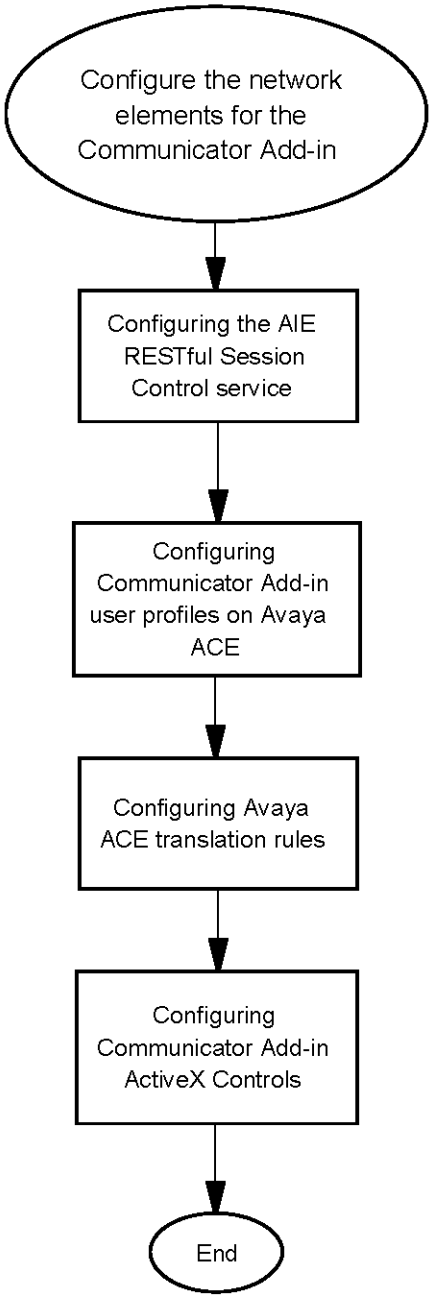
Cisco Unified Communication Manager Requirements

The CUCM service provider must be configured to use the JTAPI protocol. See the information on JTAPI solutions in *Avaya Agile Communication Environment™ Cisco Unified Communication Manager Integration* (NN10850–024).

Chapter 5: Configure the network elements for the Communicator Add-in

Configure the network elements for the Communicator Add-in procedures

This task flow shows the procedures you perform to configure the network elements for the Communicator Add-in.



Navigation

- Configuring the AIE RESTful Session Control service on page 31
- Configuring Communicator Add-in user profiles on Avaya ACE on page 32
- Configuring Avaya ACE translation rules on page 33
- Communicator Add-in ActiveX Controls on page 33

Configuring the AIE RESTful Session Control service

You must configure the RESTful Session Control service on the Avaya ACE™ Application Integration Engine (AIE).

Prerequisites

- You must be able to log in to the AIE GUI (Active Directory mode).
- During the procedure you must provide the following configuration values.

Variable	Description
ACE user group	Members of the Avaya ACE Group **RESTful_Session_Control** are permitted to use the Restful Session Control service. Only a single Avaya ACE Group is supported and the group name must be **RESTful_Session_Control**.
Client access address	The IP Address of the AIE that clients will use to access Restful Session Control services. This is only required in the case when the AIE server is configured with multiple IP Addresses. If only a single IP Address is available on the AIE server, this field should be left blank.
Secure client communications	Check this box if AIE is configured with https certificates. This configuration item causes AIE to present all subsequent URIs as secure HTTPS URIs.
Core access address	The IP Address of the AIE that Avaya ACE will use to send notifications to Restful Session Control. This is only required in the case when the AIE server is configured with multiple IP Addresses. If only a single IP Address is available on the AIE server, this field should be left blank.
Secure core communications	This check box must remain unchecked.

Note:

The HTTP port is publicly open. If you want to disable access to the AIE over HTTP, you must set up firewall rules to block access to the port. HTTP Communication between Avaya ACE and AIE must remain permitted.

- You must be able to restart the AIE. For the procedure to restart the AIE, see *Avaya Agile Communication Environment™ Application Integration Engine Fundamentals* (NN10850–021).

1. Log in to the AIE GUI.
2. On the menu bar, click **Applications**, then **Resource**, and then **Resource Configuration**.
3. Complete the configuration details.
4. Click **Save**.
5. Restart the AIE.

Configuring Communicator Add-in user profiles on Avaya ACE™

Avaya ACE maintains a user profile database to manage user information and to authenticate any entity requesting a web service. For information on creating and managing Avaya ACE user profiles, see *Avaya Agile Communication Environment™ Administration* (NN10850–005).

All Communicator Add-in users must have an Avaya ACE user profile.

Note:
All Communicator Add-in users must be a member of the Avaya ACE “User” group **RESTful_Session_Control**. When you configure the Restful Session Control service on the AIE, you specify **RESTful_Session_Control** as the **ACE user group**.

Table 2: MC Add-in user profile requirements on Avaya ACE

OCS users must be configured with the following contact types in the Avaya ACE user profile settings. The **Contact Name** can be any value. The **Contact Identifier** string `<user_name>@<OCS_domain>` must match the "Sign-In name" for this user in Active Directory. The Sign-In name can be determined by viewing the user properties in Active Directory under the **Communications** tab. Note that the Sign-In name is not necessarily the same as the Active Directory user account name (SAM Account Name or User Principal Name). Also note that for the ACE Contact Identifier, the `sip:` prefix must be replaced with the `ocs:` prefix. You must also add a telephone type contact with the contact identifier matching the e.164 representation of the work number provisioned against the OCS user. The Contact Name can be any value.

Contact Type	Contact Name	Contact Identifier	Priority	Default CLI

Chat	<user_name>	ocs:<user_name>@<OCS_domain>	0.5	No
Telephone	work phone	tel:<e.164_work_number>	0.5	No

Configuring Avaya ACE translation rules

The OCS Environment encourages the use of E.164 telephone numbers to be published by Active Directory and Office Communication Server. In Phone Mode the service provider manages extensions only, and is aware of local numbers. ACE must be configured to translate between these numbering formats between the OCS and Communication Manager domains. For more information on address translation, see *Avaya Agile Communication Environment™ Administration* (NN10850-005).

Communicator Add-in ActiveX Controls

The Avaya ACE™ Communicator Add-in utilizes the ActiveX framework to extend the capabilities of the Office Communicator client by enabling Avaya ACE features. To utilize the ActiveX framework, Internet Explorer 6 or higher must be present on any computer where the Communicator Add-in is deployed.

Internet Explorer secutiry settings for ActiveX

Internet Explorer security settings must explicitly allow ActiveX controls and plug-ins in order for the Communicator Add-In to function properly. At a minimum, the following allowances must be made for any user or computer running the Communicator Add-In:

- The Avaya ACE ™ Application Integration Engine (AIE) server must be a member of the Internet Explorer Trusted Sites Zone. For more information about Internet Explorer security zones, please refer to http://support.microsoft.com/kb/174360 .
- The Internet Explorer security settings for the Trusted Sites Zone must be configured to allow the following:
  - Run ActiveX Controls and plug-ins is enabled.
  - Automatic Prompting for ActiveX Controls is enabled.
  - Initialize and Script ActiveX Controls not marked as safe is enabled.

Note:

Alternatively, you may choose to configure this setting as “prompt”, however this configuration will prevent the Communicator Add-In from automatically starting as

soon as the user logs into the Communicator client. Instead, the user will be presented with an ActiveX prompt which they must accept in order to enable the Communicator Add-In features. Therefore, Avaya recommends that this setting be enabled for the Trusted Sites Zone only.

Avaya recognizes that it may not be practical to individually configure the necessary Internet Explorer security settings for users or computers in large deployments, therefore in such cases we suggest configuring a Group Security Policy for all Communicator Add-In users. Such a policy can be applied to all users in the domain, or if the system administrator wishes, a separate organizational unit (or units) may be created in Active Directory for Communicator Add-In users and the policy applied only where required. For more information on Active Directory Organizational Units, please refer to http://technet.microsoft.com/en-us/library/cc758565(WS.10).aspx .

Configuring a group security policy for Communicator Add-in users within Active Directory

For details and step-by-step procedures, the following resources may be helpful when configuring a group security policy to allow the necessary ActiveX controls to run.

Internet Explorer Policy Settings: http://technet.microsoft.com/en-us/library/bb457144.aspx.

The policy settings are available in the User Configuration nodes of Group Policy Object Editor, in Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel \Security Page.

Group Security Policy Requirements:

- The Site To Zone Assignment List must be enabled and the IP address or fully qualified domain name of the Avaya ACE ™ Application Integration Engine (AIE) must be added to the Trusted Sites Zone (value=2).
- The Trusted Sites Zones Template must be enabled and subsequently configured to any value other than “high” security.
- Within the Trusted Sites Zone, the “Initialize and Script ActiveX Controls not marked as safe” setting must be enabled and subsequently configured to “enable”. **Note: Alternatively, you may choose to configure this setting as “prompt”, however this configuration will prevent the Communicator Add-In from automatically starting as soon as the user logs into the Communicator client. Instead, the user will be presented with an ActiveX prompt which they must accept in order to enable the Communicator Add-In features. Therefore, Avaya recommends that this setting be enabled for the Trusted Sites Zone only.

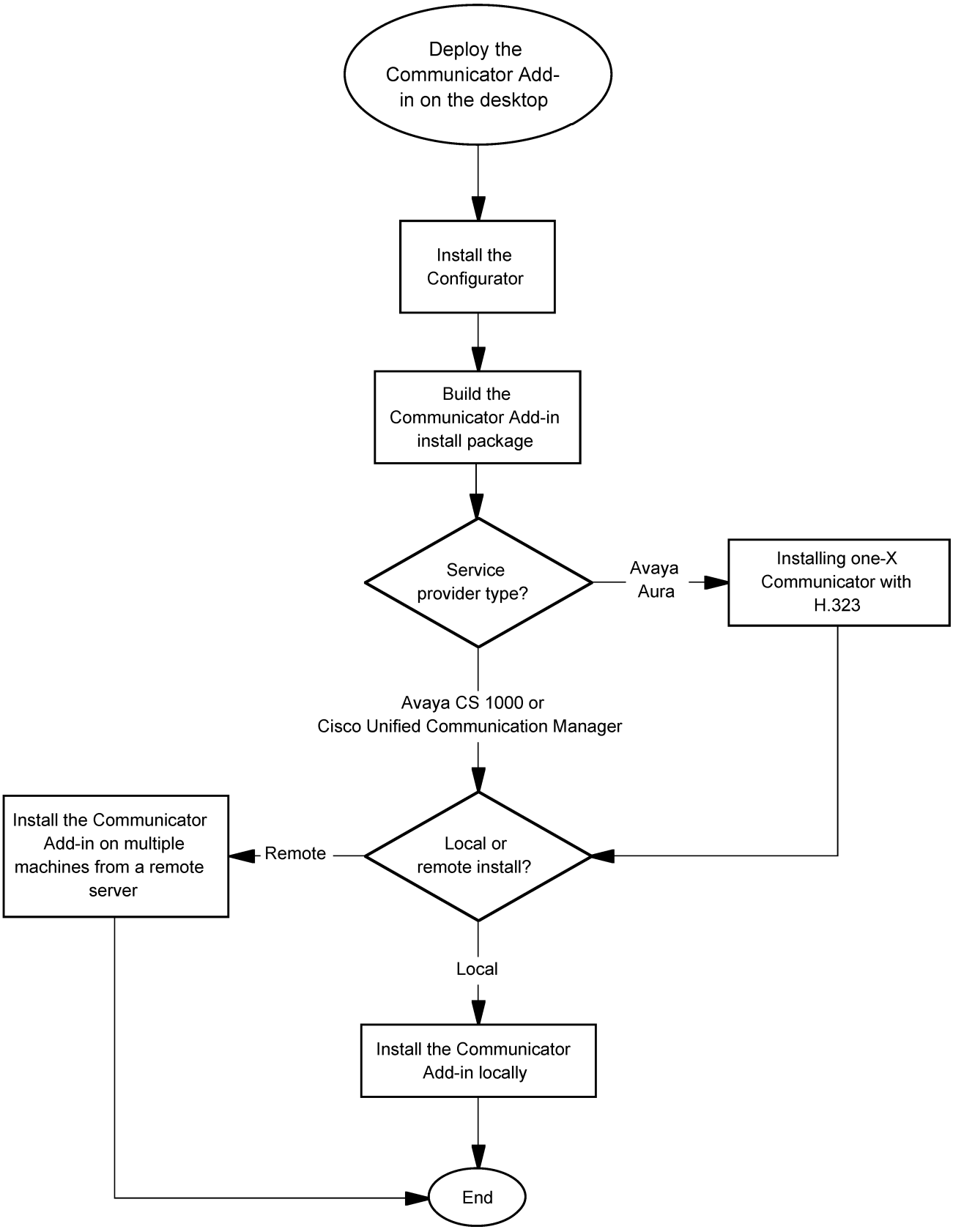
Chapter 6: Deploy the Communicator Add-in on the desktop

Prerequisites

- The machine where the MC Add-in is installed must meet the following hardware requirements:
  - CPU: 1.8 GHz or better
  - Memory: 1 GB
  - Disk space: 100 MB
  - Network Connectivity Download Bandwidth: 80 kbps
  - Network Connectivity Upload Bandwidth: 80 kbps
  - An audio device must be available on the computer to use the Communicator Add-in in Computer mode
- The machine where the MC Add-in is installed must meet the following software requirements:
  - One of the following operating systems:
    - Microsoft Windows XP Service Pack 2, or higher
    - Microsoft Windows 7
  - The latest operating system patches
  - Microsoft .Net 3.5 Service Pack 1, or higher
  - Microsoft Internet Explorer 6.0 or higher
  - Microsoft Office Communicator 2007 R2, version 3.5.6907.196 or higher
  - Avaya One-X Communicator 6.0 SP1 or higher service packs
  - Microsoft Windows Media Player version 10 or higher
  -

Deploy the Communicator Add-in on the desktop procedures

This task flow shows the procedures you perform to deploy the Communicator Add-in on the desktop.


Deploy the Communicator Add-in on the desktop
Install the Configurator
Build the Communicator Add-in install package
Service provider type?
Avaya Aura
Installing one-X Communicator with H.323
Avaya CS 1000 or Cisco Unified Communication Manager
Local or remote install?
Remote
Install the Communicator Add-in on multiple machines from a remote server
Local
Install the Communicator Add-in locally
End

Navigation

Installing the Configurator

Prerequisites

- You are running one of the following operating systems:
  - Microsoft Windows XP (patched to a minimum of SP2)
  - Microsoft Windows Vista
  - Microsoft Windows 7
- You have Microsoft .NET Framework 3.5 SP1.
- The machine where you are installing the Configurator must be able to communicate with the AIE.
- You have the DCE.configurator.msi file on your desktop. The Configurator installation package is available on the Avaya ACE Applications disk in the Desktop Communications Enablement (DCE) folder.

Install the Avaya ACE ™ Configurator. The Configurator is an administrative tool used to configure and build the install packages for the Communicator Add-in application with the needed Avaya ACE AIE configuration details and any specific application configuration prior to distribution of the add-ins to end users.

1. Double-click the DCE.Configurator.msi file to launch the Windows installer for the Avaya ACE Configurator.
2. When the Avaya ACE Configurator installer opens, click **Next**.
3. When the Avaya ACE Configurator setup wizard opens, click **Next**.
4. In the License Agreement window, click **I Agree** to accept the license agreement.
5. In the Select Installation Folder window, specify a path to the installation folder for the Avaya ACE Configurator and click **Next**.
6. In the Confirm Installation window, click **Next** to start the installation.
7. In the Installation Complete window, click **Close** to exit the setup wizard.

A dialog prompts you to view the documentation associated with the Avaya ACE Configurator.

8. To view the Avaya ACE Configurator documentation, click **Yes**.

   Otherwise, click **No**.

   The Avaya ACE Configurator icon appears on your desktop.

Building the Communicator Add-in install package

Prerequisites

- You have installed the Avaya ACE ™ Configurator.
- You know the host URL for the Avaya ACE AIE server that is hosting the Web Browser Add-in application.
- You must be able to define the following configuration variables:

Variable	Description
Supported Providers	The service provider or service providers available for use in the Communicator Add-in. Options available are **Phone**, **Computer**, or **Phone and Computer**. For the Avaya CS 1000 and CUCM service providers, select **Phone**. For the Avaya Aura service provider, both **Phone** and **Phone and Computer** are supported.
Default Provider	The service provider that starts at the initial start up of the Communicator Add-in.
Station Number Length	A number to indicate that when the Communicator Add-in is in Computer mode, dialed digits smaller than this number do not have dial plan rules applied.
Prefixes	If the environment includes extensions distributed across multiple prefixes, configure the Communicator Add-in to recognize them. For example, if the environment uses 5-digit extensions distributed across two prefixes, such as 1905123 for extensions 3xxxx and 1905456 for extensions 6xxxx, enter: `1905123;1905456` Do not include this parameter if all extensions share the same prefix.

Build the install package for the Avaya ACE Communicator Add-in to allow users to install the Communicator Add-in application.

The Avaya ACE Communicator Add-in can integrate with the Avaya ACE Web Browser Add-in and the Avaya ACE Office Add-in applications to provide a unified user experience across all Avaya ACE desktop applications. For more information, see *Avaya Agile Communication Environment™ Web Browser and Office Add-ins Application Fundamentals* (NN10850–031).

The Configurator builds the following files:

- MCAdd-in-<release#>.msi — The Communicator Add-in software.
- onexc_setup-6.0.1.16.msi — The one-X Communicator software.
- vcredist-x86.exe — The one-X Communicator prerequisite software Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update Version 8.0.59193.

These files must be transferred to the machine where the Communicator Add-in is installed.

---

1. Double-click the Avaya ACE Configurator icon to open the Avaya ACE Configurator tool.
2. On the **AIE** tab, enter the Host URL of the Avaya AIE server that is hosting the add-in application.
3. In the **Destination Folder**, enter the folder where the installation package will be built or click the folder icon to browse for a destination folder.
4. Select the **Integration** tab.
5. On the **Application** tab, enable the **None** radio button

   Note:

   Integration between Hot Desking and Communicator Add-in is not supported.
6. Select the **MC Add-in** tab.
7. On the Communicator Add-in window, enable the **Build** check box to build an install package for the Web Browser Add-in.
8. Define the following configuration variables.
   - **Supported Providers**
   - **Default Provider**
   - **Station Number Length**
   - **Prefixes**
9. Click the arrow button at the bottom of the Configurator interface to build the install package for the Communicator Add-in.

   The Configurator validates the information that you entered. If the information is valid, the Configurator creates the add-in installation files that contain all of the validated AIE configuration and application custom configuration.

If the build is successful, the Avaya ACE Applications folder opens displaying the Communicator Add-in folder.

Installing one-X Communicator with H.323

Prerequisites

- You must have administrative privileges on the local desktop
- You must have a dn configured on Communication Manager.
- You must install the Microsoft Visual C++ 2005 SP1 Redistributable Package ATL Security Update Version 8.0.59193. This installation file (`vcredist-x86.exe`) for this software is included with the Communicator Add-in software.
- You must have the one-X Communicator installation file.
- The Avaya ACE ™ Communicator Add-in employs several aspects of the Avaya one-X® Communicator. The one-X Communicator must be installed with the following settings prior to installing the Communicator Add-in:
  - Dial Plan Rules to be configured with Avaya one-X® Communicator, based on the appropriate line and location settings. Communicator Add-in will use these settings when in Computer Mode.
  - one-X Communicator can be used to make calls with the computer.

1. Double click on the one-X communicator `onexc_setup-<version>.msi` install file.
2. If an Open File — Security Warning window opens, click **Run**.
3. In the Welcome window, click **Next**.
4. Accept the license agreement and click **Next**.
5. Configure shortcut preferences and click **Next**.
6. Enter a user name and an organization name and click **Next**.
7. Click on the radio button to indicate that the install will apply to anyone who uses the computer and click Next.
8. Accept the default destination folder and click **Next**.
9. Select the radio button for the **H.323 Protocol** and click **Next**.
10. Click **Next** to start the installation.

11. If the Administrative user performing the installation is the same user who will be using the deployed software, select the check box to start the one-X Communicator, click **Finish**, and continue at step 15. Otherwise, go to step 12.
12. Uncheck the check box to start the one-X Communicator and click **Finish**.
13. Log off the Administrative user and log back in to the machine as the user who will use the deployed software.
14. Start the one-X Communicator: From the Start menu, select **Programs**, **Avaya one-X Communicator**, and then **Avaya one-X Communicator**.
15. The one-X Communicator client will attempt to perform an auto-configuration. If the one-X Communicator has not previously been installed, the auto-configuration will fail and you will be prompted to open the General Settings window. Click **OK** to configure the one-X Communicator if prompted. Otherwise, open the General Settings window by clicking on the menu icon and selecting **Settings** and then **General Settings**.
16. In the navigation list on the left, select **Phone**.
17. In the **Server** box, enter the IP address of the Communication Manager by clicking **Add**.
18. Enter your **Extension** and the associated **Password**.
19. In the navigation list on the left, select **Dialing Rules**.
20. Complete the Dialing Rule information for your network.
21. The remaining settings can be left at the default values. Click **OK** to close the General Settings window.
22. On the one-X Communicator Welcome screen, verify the one-X Communicator is configured to **Place and Receive Calls using My Computer**. This value can be changed by selecting the **My Computer** option from the pull down menu.
23. Click **Log on and save settings** to log on to the one-X client and verify the configuration. Follow any prompts to configure audio settings using the Audio Tuning Wizard.
24. Click the menu icon and select **Exit** to exit the client.

Installing the Communicator Add-in locally

Use this procedure to install the Avaya ACE™ Communicator Add-in where the installation software is local to the machine where it is being installed.

The Communicator Add-in is installed on end user machines coresident with Communicator. Communicator can be running during the Communicator Add-in installation. The Communicator Add-in application will launch during the next Communicator startup.

As part of the Communicator Add-in installation process, Communicator must be made aware of the Communicator Add-in application. The association is made through the following Communicator registry settings:

- `Key: \My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\POLICIES\Microsoft \Communicator\TabURL Description: Microsoft Web Extension that informs Office Communicator of the Avaya ACE™ MC Add-in.`
- `Key: \My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\POLICIES\Microsoft \Communicator\CustomStateURL Description: Custom Busy "In A Call" Presence. This setting enables the MC Add-in publish Telephony Presence to OCS.`

When using this procedure to install the Communicator Add-in, no installation log file is created. If you experience problems with installation, perform the installation from the command line and view the log file. See Installing the Communicator Add-in on multiple machines from a remote server on page 43.

Prerequisites

- You must have administrative privileges on the local desktop.
- You must have the `MCAdd-in-<release#>.msi` file.

The Communicator Add-in install directory is `\Program Files\Avaya\Avaya ACE(TM) MC Add-in`.

---

1. If open, exit Microsoft Office Communicator.
2. If open, exit Internet Explorer.
3. Open a Windows Explorer tool and navigate to the location of the `MCAdd-in-<release#>.msi` file.
4. Double click the file to start the installation.
5. Start Microsoft Office Communicator.

Installing the Communicator Add-in on multiple machines from a remote server

To facilitate the integration of the Avaya ACE™ Communicator Add-in software into bulk software distribution and installation infrastructure, the Communicator Add-in software can be installed without end-user intervention, using the following command:

```
msiexec /i MCAddin-<release#>.msi /lv MCAddin.install.log /q
```

If Microsoft Communicator and Microsoft Internet Explorer are running at the time of Communicator Add-in installation, the Communicator Add-in will launch when the Microsoft Communicator is restarted.

To validate the Communicator Add-in installation, view the file `MCAddin.install.log`. The `MCAddin.install.log` file contains text readable output of the installation process and indicates failures or missing prerequisites. For example:

- The following log entry indicates successful install of Communicator Add-in.

  ```
  Product: Avaya ACE(TM) MC Add-in -- Installation completed
  successfully.
  ```

- The following log entry indicates the one-X Communicator is not available.

  ```
  Skipping action: SetCOMPUTERMODESUPPORTED (condition is false)
  ```

- The following log entry indicates the one-X Communicator is available.

  ```
  Doing action: SetCOMPUTERMODESUPPORTED
  ```

Chapter 7: Uninstall Communicator Add-in

This section contains the procedures for uninstalling the Communicator Add-in software deployed on the desktop.

Navigation

Uninstalling the Communicator Add-in from the local desktop

Prerequisites

- You must have administrator privileges to uninstall the application.
- Close Communicator before performing the uninstall.

1. From the Windows **Start** menu, select **Settings**, **Control Panel**, then **Add or Remove Programs**.
2. In the Add or Remove Programs window, select **Avaya ACE MC Add-in** and then click **Remove**.
3. You are prompted to confirm the uninstall. Click **Yes**.

Uninstalling the Communicator Add-in from multiple machines

To facilitate the integration of the Avaya ACE™ Communicator Add-in software into bulk software distribution and installation infrastructure, the Communicator Add-in software can be uninstalled without end-user intervention, using the following command:

```
msiexec /x MCAddin-<release#>.msi /lv MCAddin.uninstall.log /q
```

Uninstalling one-X Communicator

Use this procedure to uninstall the Avaya one-X Communicator.

1. From the Windows **Start** menu, select **Settings**, **Control Panel**, then **Add or Remove Programs**.
2. In the Add or Remove Programs window, select **Avaya one-X Communicator** and then click **Remove**.
3. You are prompted to confirm the uninstall. Click **Yes**.

Chapter 8: Upgrading Communicator Add-in

To upgrade the Communicator Add-in, you must perform the procedure to uninstall the old version and then install the new version. Before you can install the new version, you must build the .msi file using the Configurator tool.

Prerequisites

Before upgrading the Communicator Add-in, review the chapters listed under Deploying Communicator Add-in on page 25 to ensure that all prerequisites have been met.

1. Uninstall the old version of Communicator Add-in. Perform the procedure Uninstalling the Communicator Add-in from multiple machines on page 45.
2. Install the Configurator. Perform the procedure Installing the Configurator on page 37.
3. Build the .msi file. Perform the procedure Building the Communicator Add-in install package on page 38.
4. Install the Communicator Add-in. Perform the procedure Installing the Communicator Add-in locally on page 41.

Chapter 9: Remote Call Control capabilities utilizing Microsoft UCMA API

Network administrators can integrate the Avaya Agile Communication Environment™ (ACE) into their Microsoft Office Communications Server (OCS) network infrastructure to enhance existing communication services. Avaya ACE™ supports unified communication (UC) desktop integration with OCS 2007 SP1 or OCS 2007 R2. By leveraging Avaya ACE web services and user profile management, OCS administrators can provide unified communication services to Office Communicator clients.

An OCS network with Avaya ACE and the Communication Server (CS) 2000 contains the following core components:

- Communicator clients
- OCS Forest
- Avaya ACE Service Agent (ASA)
- Avaya ACE
- CS 2000 service provider

Avaya ACE™ services with ASA and CS 2000

ASA is an integration element between Microsoft's Office Communication Server and Avaya's Agile Communication Environment. From an OCS perspective, Avaya ACE and ASA appears as a Computer Supported Telecommunications Applications (CSTA) gateway and as an OCS application server.

From the Avaya ACE perspective, ASA appears as Parlay-X Web services application. Primarily, ASA does protocol translation between CSTA/UCMA and Web Services. Where required, ASA also provides key service integration service logic between OCS and Avaya ACE applications, such as Hotdesking.

The CS 2000 service provider is the network communication layer. The network communication layer is responsible for providing the communication services to support web service requests. The following services are provided:

- Remote Call Control (RCC) capabilities:
  - Make call
  - Release call

- Conversation history

• Extended presence

Remote Call Control

Avaya ACE and ASA enable Remote Call Control (RCC) capabilities. RCC provides the capability to control PBX features on your desk phone from within the Office Communicator (OC). The following table lists the supported features. The services are integrated into the Office Communicator by virtue of ASA and Avaya ACE acting as the Computer Supported Telecommunications Applications (CSTA) gateway on behalf of the OCS Front End. ASA and Avaya ACE support the following RCC capabilities.

Table 3: Supported RCC capabilities

OC RCC capability through OC user interface	
Cabability	**Description**
Make Call	User can make a call on their phone by clicking on a contact in their Contact list or entering a number on their OC client
Release Call	User can Release a phone call by clicking on the Phone X Icon in Office Communicator
Conversation History	User can see in the Conversation History folder in Outlook all of incoming and outgoing calls (while their OC client is logged in)

Microsoft Office Communicator RCC limitations

The Microsoft Office Communicator has the following RCC limitations.

Call Forward limitations

- If you configure Call Forwarding settings on a user device, this configuration will not be set in Microsoft Office Communicator. After you log out of Communicator, on the next login, Communicator will re-establish the current settings, irrespective of the Call Forward settings on the device. For the best Communicator experience when setting Call Forwarding via Communicator, the configuration should be done in Communicator.
- If Call Forwarding is disabled on the ASA, a logged in Office Communicator does not reflect the service downgrade. The Call Forwarding feature appears to be available until after Office Communicator is restarted.

  If Call Forwarding is disabled on the ASA and Call Forwarding is set in Office Communicator, it cannot be turned off. You must restart Office Communicator. You can continue to manage Call Forwarding manually on the user device.

Call Hold and Call Retrieve limitation

Setting Call Hold or Call Retrieve on a user device is not reflected in Microsoft Office Communicator.

Extended presence

Extended presence enhances telephony presence by allowing a watcher to see the telephony presence of a contact even when that contact is logged out of their Office Communicator. If a user is logged off of the Office Communicator and another device listed in the Avaya Agile Communication Environment user profile goes off-hook, Avaya Agile Communication Environment sends the presence status change through the ASA to the OCS server. The OCS server then broadcasts the presence change to all interested clients.

If your deployment is providing extended presence, you can enable custom offline presence display during installation. When this feature is enabled, if a user is logged off of the Office Communicator, contacts watching this user see the offline presence status for the user, but also see an additional message. For example, if your OCS network environment includes a short message service (SMS), you could configure the presence status to display "IM available", indicating that the user can still receive an instant message (IM) on a mobile device.

Network configuration requirements

This section describes the following CS 2000 network configuration requirements:

- CS 2000 configuration requirements for Click-to-Call
- CS 2000 configuration requirements for Presence, Call Notification, and Call History
- ISSG configuration requirements

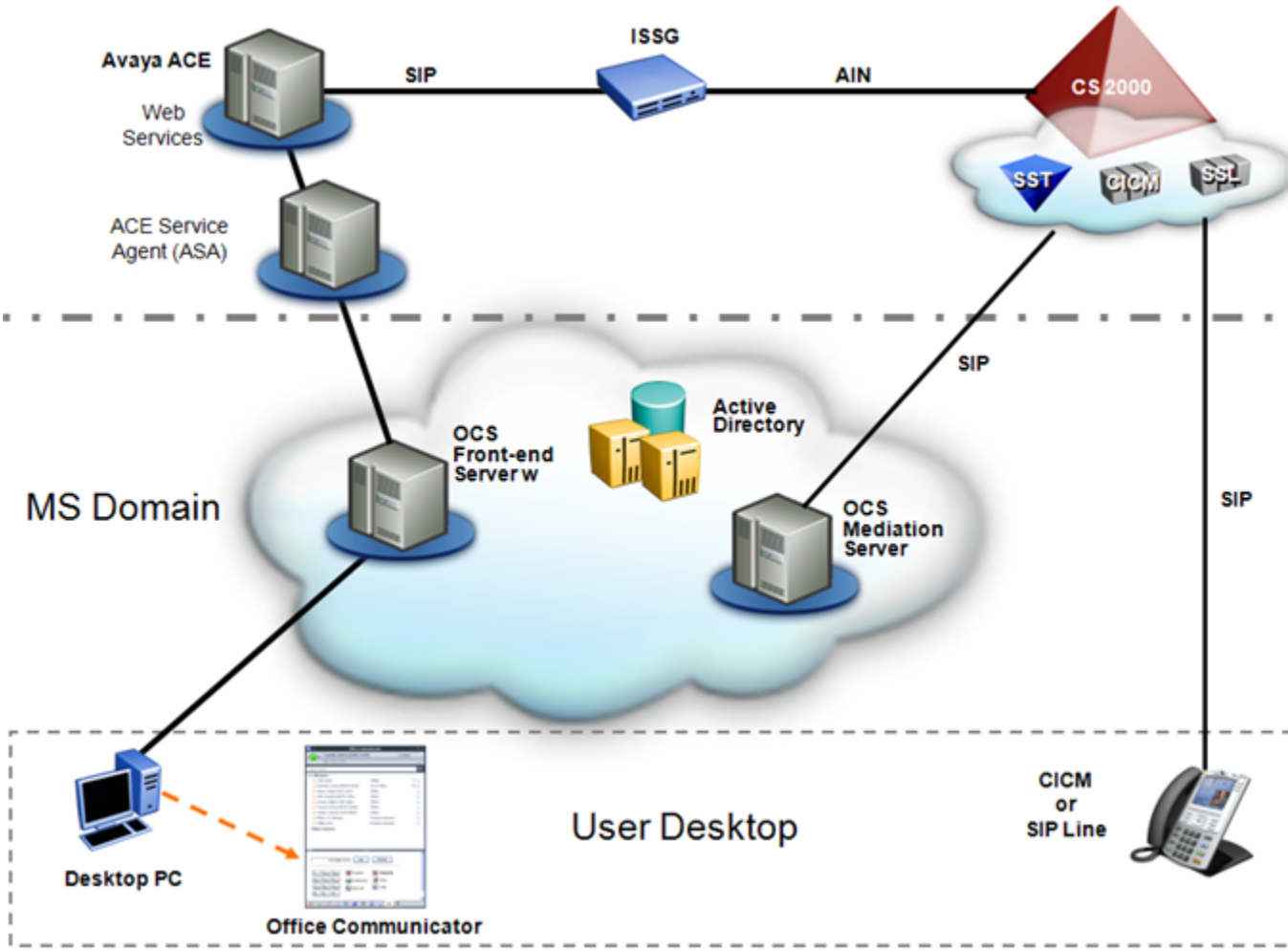


Figure 6: Avaya ACE services with ASA and CS 2000

CS 2000 configuration requirements for Click-to-Call

Avaya ACE supports Click-to-Call control of CS 2000 agents by utilizing the CS 2000 Session Server for SIP Trunks (SST) gateway. Once the SIPT is provisioned on the CS 2000, the associated Avaya ACE Remote SIP Server and Access Link can be provisioned on the SST. SIPT is also known as Dynamic Packet Trunking (DPT) on the CS 2000.

Avaya ACE makes use of the SIP Trunk on the CS 2000 for the setup of calls to the Calling and Called parties in Click-to-Call. Avaya ACE first initiates a SIP Trunking interface to the Calling Party. When the Calling Party answers, Avaya ACE initiates a SIP call across the SIP Trunking interface to the Called Party. When the Called Party answers, the Avaya ACE server sends the answer indication from the Called Party's SIPT trunk to the Calling Party's SIP Trunk in order to establish speech path. During provisioning, the CS 2000 must be properly commissioned and in service including the installation and provisioning of the SST. Both the Avaya ACE service provider IP address and the CS 2000 translation information that associates the SIPT trunk to the network translations system configuration information must be provided during provisioning.

To support communications with Avaya ACE for Click-to-Call, the CS 2000 network element must meet the following configuration requirements:

Session Server for SIP Trunks (SST)

and one of:

- CS 2000 system running software release Carrier Voice Multimedia Release 11 (CVM11) or greater
- CS 2000 Hybrid system running software release Carrier Voice Multimedia Release 11 (CVM11) or greater

CS 2000 configuration requirements for Presence, Call Notification, and Call History

Advanced Intelligent Network (AIN) Triggers are used to provide CS 2000 line presence information to the Avaya ACE server. In this setup the Avaya ACE server acts as a AIN Adjunct server and responds to AIN requests initiated when the AIN Triggers are hit during call processing on the CS 2000. In order to effect the exchange of presence information from the CS 2000 to the Avaya ACE server the AIN Termination Attempt (TERMATT) and Offhook Delay (OFFHKDEL) must be provisioned on the associated CS 2000 lines. When the associated lines make or receive calls, the triggers result in AIN message exchange with the ACE server and cause the presence information on the Avaya ACE server to be updated accordingly. Additional message exchange between the CS 2000 and ACE Server occurs on call take down to update the presence information on the Avaya ACE server.

The interworking point between Avaya ACE and the CS 2000 for AIN Message exchange is the Intelligent Network SIP Signalling Gateway (ISSG). The ISSG converts the AIN messages sent by the CS 2000 into SIP messages and forwards the messages to the associated Avaya ACE server. When the Avaya ACE server responds to the request the ISSG converts the SIP message response into an AIN response and forwards it to the associated CS 2000. The Avaya ACE server is provisioned as an Application server on the ISSG.

To support communications with Avaya ACE for Presence, the CS 2000 network element must meet the following configuration requirements:

- SS7 Links between the CS 2000 and ISSG
- AIN Software Optionality Control (SOC) Options for AIN 0.1
- AIN Subsystem and Triggers associated with the Avaya ACE server
- CS 2000 lines with TERMATT and OFFHKDEL AIN Triggers
- IDP voice must be enabled on the CS 2000

Use the Personal Assistant for Call History. For details about Personal Assistant, see *Avaya Agile Communication Environment Personal Assistant Application, NN10850-032*.

For more information related to the deployment of the CS 2000, refer to the following:

- *DMS-100 Family Advanced Intelligent Network Essentials Service Implementation Guide* (297-5161-021)
- *Avaya CS 2000 Session Server Lines Converged Desktop Fundamentals* (NN10437-115)

- *Carrier VoIP Avaya Universal Signaling Point Administration and Security* (NN10159-611)
- *Carrier VoIP Avaya Universal Signaling Point Configuration* (NN10093-511)

ISSG configuration requirements

To support communications with Avaya ACE, the ISSG must meet the following configuration requirements:

- Avaya ACE System ID and Application Server
- SS7 Links between the ISSG and CS 2000
- Signaling Connection Control Part (SCCP)

Requirements for Avaya ACE™ unified communication for Microsoft OCS using CS 2000 service providers

When using the CS 2000 service provider in an OCS environment, Avaya ACE enables CS 2000 presence information to be displayed in the Office Communicator. To enable Avaya ACE services from CS 2000 the following is required:

- CS 2000 telephony presence will only be published via OCS for users having a corresponding Avaya ACE profile. See Configuring OCS users on the Avaya ACE server on page 81.
- For 3rd-party calls via CS 2000 devices the calling party must have an Avaya ACE user profile. See Configuring OCS users on the Avaya ACE server on page 81. The called party does not require an Avaya ACE user profile, but if this is the case, no presence information for the called party will be available.
- For 3rd-party call control via CS 2000 devices an OCS user must have their Line-URI configured with a public E.164 number that matches the number provisioned in the corresponding Avaya ACE user profile for the device being used to make 3rd-party calls.
- For Call Notification service for calling party via CS 2000 SIP_IN service provider, both the calling and called parties must be OCS users in order to enable the multi-media capability between the two parties. All the dial plans used by the calling party to reach called party must be provisioned in the called party's Avaya ACE user profile.

  For example: sip:<dialplanA_phone_number>@<ss7_domain>
  sip:<dialplanB_phone_number>@<ss7_domain>

This configuration will also support simultaneous ringing of both Office Communicator and the CS 2000 client if the following conditions are met:

- OCS Enterprise Voice must be deployed in conjunction with a media gateway that connects to the CS 2000.
- The CS 2000 must include Integrated Desktop Phone (IDP) configuration to ring both the CS 2000 telephone and the Office Communicator via the media gateway.
- OCS users must be enabled for Enterprise Voice with PBX Integration in Active Directory such that the Line-URI matches the configured IDP number that is sent out to their Office Communicator whenever a call is received for the associated CS 2000 subscriber.

If simultaneous ringing is not required or the OCS is configured for RCC, the following condition must be met:

OCS users must be enabled for remote call control (RCC) in Active Directory.

Avaya ACE™ Service Agent deployment

Avaya Agile Communication Environment™ (ACE) services are provided in an OCS environment by enabling communication between Avaya ACE and the OCS server through the Avaya ACE Service Agent (ASA). The ASA acts as a protocol converter between Avaya ACE and the OCS server.

ASA administrative user

An administrative user is required to deploy and run the ASAservice. This user must be created in Active Directory and enabled for the Office Communications Server Front End or Pool being monitored by ASA.

The ASA administrative user must be a member of the RTCUniversalServerAdmins Group in the Windows domain hosting Office Communications Server. See Adding the ASA administrative user to the OCS RTCUniversalServerAdmins group on page 64.

The ASA administrative user must be a member of the Performance Monitor Users Group on the local computer where the ASA service is deployed. See Adding the ASA administrative user to the local Performance Monitor Users Group on page 65.

The ASA administrative user must have permission to access the private key of the certificate configured for ASA in the local computer personal certificate store where ASA is installed. For a Windows 2008 server, you must perform the procedure Granting private-key certificate access to the ASA administrative user on a Windows 2008 server on page 77. For a Windows 2003 server, the permission is configured by default. If permission is not configured, see the troubleshooting procedure Configuring certificate private key access to the ASA administrative user on Windows Server 2003 on page 88.

The ASA administrative user must also have a corresponding profile on Avaya ACE™. Refer to the next section for details on the Avaya ACE user profile requirements for the ASA administrative user.

Avaya ACE™ user profiles

Avaya ACE maintains a user profile database to manage user information and to authenticate any entity requesting a web service. For information on creating and managing Avaya ACE user profiles, see *Avaya Agile Communication Environment™ Administration, NN10850-005*.

Note that when an Avaya ACE user profile is added, it may take up to 60 minutes for Avaya ACE services to be available in the Office Communicator. User initiated services are available after the next login session. "Proxy services", such as extended presence, are available within 60 minutes.

The following Avaya ACE user profiles are required for Avaya ACE integration with OCS:

- Avaya ACE user profile for the ASA administrative user on page 56
- Avaya ACE user profiles for OCS usersAvaya ACE user profiles for OCS users

Avaya ACE user profile for the ASA administrative user

For each instance of ASA, a corresponding Avaya ACE user profile must be created and associated with the ASA administrative user. This user profile must belong to an Avaya ACE user group with administrative privileges. This is required to allow Office Communications Server to access Avaya ACE web services (via ASA).

To enable Avaya ACE services for ASA users, the access control rules for the user group to which the ASA administrative user belongs must be configured in the ACE GUI. For information on configuring the access control rules for an Avaya ACE user group, see *Avaya Agile Communication Environment Administration™* (NN10850-005). The ASA administrative user must have administrator level privileges for the following services:

- CallForwardingService
- CallNotificationService
- PresenceConsumerService
- PresenceSupplierService
- ThirdPartyCallService

Avaya ACE™ user profiles for OCS users

Each OCS user must have an Avaya ACE user profile in order to use any Remote Call Control features or display telephony presence. The Avaya ACE user profile defines the Avaya ACE user as part of the OCS server domain. Note that when an Avaya ACE user profile is added,

it may take up to 60 minutes for Avaya ACE services to be available in Office Communicator. For an immediate refresh, the user can log out of Office Communicator and then log back in.

Avaya ACE stores information about OCS users and their registered telephones in the user profile. With the device information from the user's profile, Avaya ACE queries each device for the user's presence status and makes the presence status available to the OCS server. The OCS server distributes the presence information to the Office Communicator clients for display in the contact list. Users must have an Avaya ACE user profile that specifies their OCS contact information on the Avaya ACE server and the contact information for every device for which presence information is sought. For devices of the same type, Avaya ACE queries presence for the device with the highest priority.

The Avaya ACE user profile must contain the following information for each configured device.

Table 4: Avaya ACE user profile content

Contact identifier	Contact type	Example
`tel:`*<phone_number>*	Telephone	tel:88501
`sip:`*<number>*@*<IP_domain>*	Telephone	sip:88501@system
`sip:`*<number>*@*<ss7_domain>*	Other	sip:88501@pstn

Important:

For Avaya ACE integration in a network with multiple provider types, Avaya recommends that the same URI type be used for all telephone devices. For information on service provider configuration, see *Avaya Agile Communication Environment Administration* (NN10850-005).

Chapter 10: Installing the Avaya ACE service agent

The Avaya Agile Communication Environment™ (ACE) supports integration with the Microsoft Office Communications Server (OCS) to enhance existing communication capabilities. To enable Avaya ACE services, you must install the Avaya ACE service agent. Follow the procedures in this chapter to enable communication between Avaya ACE and OCS to support Avaya ACE services in an OCS environment.

Integrating Avaya ACE and the Avaya ACE Service Agent (ASA) into an OCS network enables telephony services in the Office Communicator. Avaya ACE does not alter the functional operation of Office Communicator. No Avaya ACE specific configuration of Office Communicator is required.

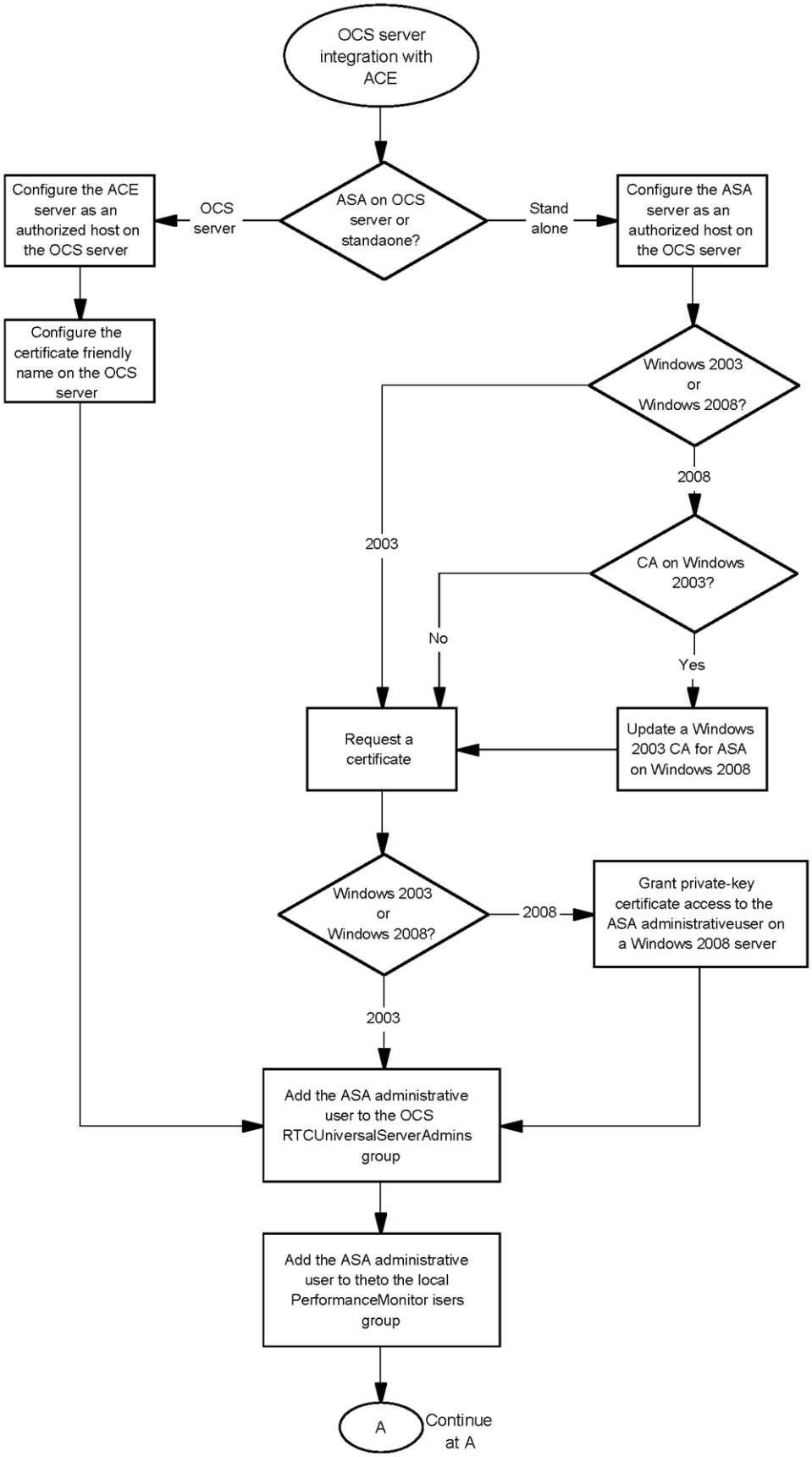
Important:
Deploying the ASA on the OCS server is only supported in a controlled trial environment.

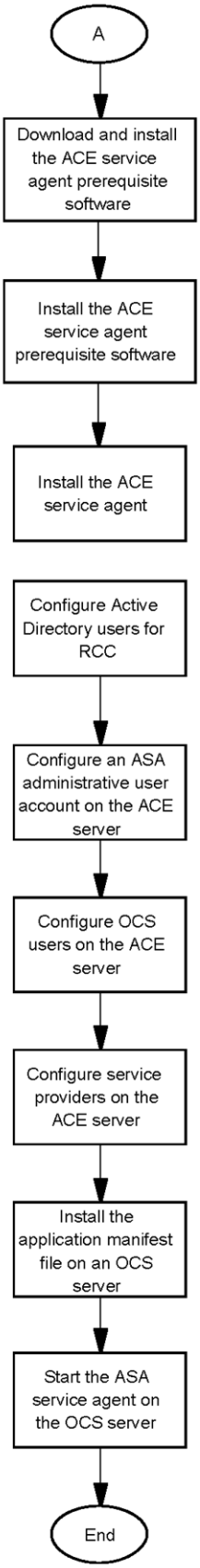
Prerequisites

- For the click-to-call service, ensure that the OCS server is deployed with the necessary client access license (CAL) for call control and management.
- You have administrator privileges on the OCS server.
- You are familiar with OCS server administration and OCS server policies.
- The Avaya ACE server is installed and functional. See *Avaya Agile Communication Environment Planning and Installation* (NN10850-004).
- The required service providers are configured. For information about service provider configuration, see *Avaya Agile Communication Environment Administration* (NN10850-005).
- You must have administrator privileges on the Avaya ACE server.
- Familiarity with Avaya ACE user management. For more information, see *Avaya Agile Communication Environment Administration* (NN10850-005).

Installing the ACE service agent procedures

This task flow shows the procedures you perform to integrate OCS services with Installing the ACE service agent procedures.


OCS server integration with ACE
ASA on OCS server or standaone?
OCS server
Stand alone
Configure the ACE server as an authorized host on the OCS server
Configure the certificate friendly name on the OCS server
Configure the ASA server as an authorized host on the OCS server
Windows 2003 or Windows 2008?
2008
2003
CA on Windows 2003?
No
Yes
Request a certificate
Update a Windows 2003 CA for ASA on Windows 2008
Windows 2003 or Windows 2008?
2008
Grant private-key certificate access to the ASA administrativeuser on a Windows 2008 server
2003
Add the ASA administrative user to the OCS RTCUniversalServerAdmins group
Add the ASA administrative user to theto the local PerformanceMonitor isers group
A
Continue at A


A
Download and install the ACE service agent prerequisite software
Install the ACE service agent prerequisite software
Install the ACE service agent
Configure Active Directory users for RCC
Configure an ASA administrative user account on the ACE server
Configure OCS users on the ACE server
Configure service providers on the ACE server
Install the application manifest file on an OCS server
Start the ASA service agent on the OCS server
End

Navigation

Configuring the ASA server as an authorized host on the OCS server

To enable communication between the ASA server and the OCS server, you must configure the ASA server as an authorized host on the OCS server.

Do not perform this procedure when installing the ASA coresident on the OCS server. For a coresident deployment, perform the procedure Configuring the Avaya ACE server as an authorized host on the OCS server on page 63.

1. Log in to the OCS server.
2. From the Windows **Start** menu, select **Administrative Tools** and then **Office Communications Server 2007**.
3. In the OCS window, in the navigation tree on the left, expand **Forest**. If there is a **Domains** folder under **Forest**, expand the folder.
4. Expand **Standard Edition Servers**.

5. Right-click on the OCS server where you want to add Avaya ACE as an authorized host. Select **Properties** and then **Front End Properties**.
6. In the <server_name> Front End Properties window, click the **Host Authorization** tab.
7. Click **Add**.
8. In the Add Authorized Host window, enter the fully qualified domain name (FQDN) of the ASA server.
9. In the **Settings** box, select **Treat as Authenticated** and **Throttled as Server**.
   The **Outbound only** option remains unselected.
10. Click **Apply**.
11. Click **Add**.
12. In the Add Authorized Host window, enter the IP address of the ASA server.
13. In the **Settings** box, select **Treat as Authenticated** and **Throttled as Server**.
    The **Outbound only** option remains unselected.
14. Click **Apply**.
    The ASA server is added to the authorized host list.
15. Click **OK** to close the <server_name> Front End Properties window.
16. In the navigation tree on the left, expand the OCS server entry and right-click on the fully qualified domain name of the server. Select **Properties** and then **Front End Properties**.
17. In the Front End Server Properties window, click the **General** tab.
18. Click **Add**.
19. In the Add Connection window, in the **IP Address** box, select **All**.
20. In the **Port** box, enter **5060**.
21. In the **Transport** box, select TCP.
22. Click **OK**.
23. Click **OK** to close the Front End Properties window.

Configuring the Avaya ACE ™ server as an authorized host on the OCS server

To enable communication between the Avaya ACE server and the OCS server, you must configure the Avaya ACE server as an authorized host on the OCS server.

Do not perform this procedure when installing the ASA on a standalone server. For a standalone deployment, perform the procedure Configuring the ASA server as an authorized host on the OCS server on page 62.

1. Log in to the OCS server.
2. From the Windows **Start** menu, select **Administrative Tools** and then **Office Communications Server 2007**.
3. In the OCS window, in the navigation tree on the left, expand **Forest**. If there is a **Domains** folder under **Forest**, expand the folder.
4. Expand **Standard Edition Servers**.
5. Right-click on the OCS server where you want to add Avaya ACE as an authorized host. Select **Properties** and then **Front End Properties**.
6. In the <server_name> Front End Properties window, click the **Host Authorization** tab.
7. Click **Add**.
8. In the Add Authorized Host window, enter the fully qualified domain name (FQDN) or the IP address of the Avaya ACE server.
9. In the **Settings** box, select **Treat as Authenticated** and **Throttled as Server**.

   The **Outbound only** option remains unselected.
10. Click **OK**.

    The Avaya ACE server is added to the authorized host list.
11. Click **Add**.
12. In the Add Authorized Host window, enter the fully qualified domain name (FQDN) or the IP address of the OCS server.
13. In the **Settings** box, select **Treat As Authenticated** and **Throttled As Server**.

    The **Outbound Only** option remains unselected.
14. Click **OK** to close the Add Authorized Host window.
15. Click **OK** to close the <server_name> Front End Properties window.

Adding the ASA administrative user to the OCS RTCUniversalServerAdmins group

You must add the ASA administrative user to the OCS RTCUniversalServerAdmins group. Ensure that the user belongs to the domain users group.

Usually, the active directory is on a remote server. However, if the active directory is collocated with an OCS server, you must open the **Users** folder from **Active Directory Users and Computers**.

1. Log into any system where Active Directory Domain Users can be managed. You will need to log in as a user having the appropriate permission to modify the properties of a domain user.
2. Open the Windows **Start** menu.
3. Select **Administrative Tools** and then **Active Directory Users and Computers**.
4. Right-click on the domain where the Office Communications Server users are located and select **Find** to open the Find Users, Contacts & Groups window.
5. Enter all or a portion of the ASA administrative user's user name in the **Name** field and click **Find Now**.
6. Verify that the ASA administrative user appears in the Search Results window. Right-click on the user and select **Properties** to open the Properties window.
7. In the Properties window, click on the **Member of** tab.
8. Click **Add**.
9. Click **Advanced**.
10. In the Select Groups window, click **Find Now**.
11. In the Find Now window, in the **Search Results** list, select the group **RTCUniversalServerAdmins**.
12. Click **OK** to close the Find Now window.
13. Click **OK** to close the Select Groups window.
14. Click **Apply**.
15. Click **OK** to close the window.

Adding the ASA administrative user to the local Performance Monitor Users Group

You must add the ASA administrative user to the local Performance Monitor Users Group on the computer where the ASA service is deployed.

1. Log into the server where ASA is deployed as an administrative user.
2. From the Windows **Start** menu, select **Administrative Tools**, then **Computer Management** to open the Computer Management console.
3. In the Computer Management Console, select **System Tools**, then **Local Users and Groups**, and then **Groups**.
4. In the Groups window, right-click on the **Performance Monitor** users group and select **Properties**.
5. Click **Add** to open the Select Users, Computers or Groups window.
6. Click **Locations** and select the Windows domain containing the ASA administrative user.
7. Click **OK**.
8. Enter a portion or all of the name of the ASA administrative user in the Enter the object names to select window.
9. Click **Check Names** and select the ASA administrative user from the list. If only one matching name is found, it will be automatically populated and underlined in the window.
10. Click **OK** to add the ASA administrative user to the local **Performance Monitor Users Group**.
11. Click **OK** to save the changes and close the Performance Monitor Users Properties window.

Installing ASA prerequisite software packaged with Avaya ACE™

The Avaya ACE Service Agent (ASA) requires the following software:

- Microsoft .Net framework 3.5 SP1
- Microsoft Visual C++ 2008 redistributable
- Microsoft UCMA 2.0 redistributable

The installation files required to install each software item are included on with the Avaya ACE software. There are separate files for 32 and 64 bit operating systems.

Prerequisites

The prerequisite software applications installed during this procedure are common tools. Use the Windows Control Panel Add or Remove Programs tool to determine if the software has already been installed.

You must have the ASA prerequisite installation software. You can obtain the software from the following locations:

- from the Linux **Avaya ACE Software and Installation Tools** disk at: `\ace-<version>\ACEServerAgent`
- on the Linux Avaya ACE server at: `/opt/avaya/ace/ACEServerAgent`
- on the Windows Avaya ACE server at: `\Program Files\Avaya\Avaya ACE\ace\ACEServerAgent`

Download the zip file for your operating system:

- `ace_server_agent_32bit.zip`
- `ace_server_agent_64bit.zip`

In the downloaded zip file, there is a file containing the prerequisite software. You will require one of the following files:

- `Prerequisites32bit.zip`
- `Prerequisites64bit.zip`

---

1. Copy the ASA prerequisite software zip file to the OCS server.
2. Unzip the file.
   The following folders are unzipped. The software items must be installed in the order listed below.
   - dotNet35SP1
   - Visual C++ 2008
   - UCMA 2.0
3. For each software item, open the folder and double-click on the install file.
   Follow the prompts to install the software.

Downloading and installing prerequisite software

Additional Windows software tools must be downloaded and installed. Due to licensing restrictions, these tools cannot be delivered with the Avaya ACE software. There are separate tools for Windows 2003 and Windows 2008 servers.

The ASA installation software is dependent upon these tools to automatically configure the ASA software. If these tools are not present, the ASA application may not function correctly until additional manual configuration procedures are performed.

Windows 2003

winhttpcertcfg

The `winhttpcertcfg` utility is part of the Windows Server 2003 Resource Kit Tools. For information on this software and instructions on how to download and install, go to http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en.

httpcfg

The `httpcfg` utility is part of the Windows Server 2003 Service Pack Support Tools. For information on this software and instructions on how to download and install, go to http://support.microsoft.com/kb/892777.

Windows 2008

netsh

The `netsh` utility is typically included as part of the default installation of Windows Server 2008. Verify that the netsh utility is present prior to installing ASA. The default location is `C:\Windows\System32\netsh .`

Installing the Avaya ACE™ Service Agent

Install the ASA software that enables Avaya ACE integration with OCS. The ASA can be installed on the OCS server or on a separate server.

Important:
Deploying the ASA on the OCS server is only supported in a controlled trial environment.

Once all the required information is gathered, this procedure should result in only 15 minutes of downtime.

Prerequisites

You must have the ASA software. You can obtain the software from the following locations:

- From the Linux **Avaya ACE Software and Installation Tools** disk at: `\ace-<version>\ACEServerAgent`
- on the Linux Avaya ACE server at: `/opt/avaya/ace/ACEServerAgent`
- on the Windows Avaya ACE server at: `\Program Files\Avaya\Avaya ACE\ace\ACEServerAgent`

Download the zip file for your operating system:

- `ace_server_agent_32bit.zip`
- `ace_server_agent_64bit.zip`

In the downloaded zip file, You will require the following files:

- `setup.exe`
- `ASASetup32.msi` OR `ASASetup64.msi`

During the procedure you must provide the following configuration values. For information on setting these values, see the requirements section for the network type being deployed.

Variable	Description	Value
ACE IP Address	IP address of the Avaya ACE server.	
ACE User Name	The ASA administrative user has a user account on the ACE server. See Configuring an ASA administrative user account on the Avaya ACE server on page 80.	
ACE Password	Password for the ACE user name.	
ASA Firewalled From ACE	Select Yes if there is a Network Address Translation (NAT) firewall between ASA and Avaya ACE such that Avaya ACE cannot communicate directly with the IP address configured on the ASA host system. Select No if Network Address Translation is not required in your network.	
ASA Callback IP Address	This is the public IP address used by Avaya ACE to communicate with ASA when there is a Network Address Translation (NAT) firewall between the ASA and the Avaya	

Variable	Description	Value
	ACE. This value is required only if you have selected Yes for "ASA Firewalled from ACE" variable.	
Active Directory Server Name	The fully qualified domain name of the server where the OCS active directory resides. For example, `hostname.avaya.com`	
OCS server name	The fully qualified domain name of the OCS pool or standard edition front end in the domain that the ASA will communicate with.	
Enable Transport Layer Security	Select this option to enable Transport Layer Security (TLS) encryption between the Office Communications Server Front End(s) and the ASA. Deselecting this option will result in unencrypted communication between OCS and ASA.	
Enable OCS Health Monitoring	Select this option to enable the ASA to monitor the health of the Office Communications Server Front End(s). Note that this option requires the ASA Administrative user to have administrative privileges on the OCS front end(s) in the pool or standalone server. Do not select this option unless the ASA administrative user has administrator privileges on the OCS front end(s).	
ASA FQDN / IP Address	The fully qualified domain name or the IP address of the OCS server where the Avaya ACE Server Agent is being installed. If the ASA is being installed on a standalone machine, enter the fully qualified domain name or IP address of the server where the ASA is being installed.	
Certificate Friendly Name	The network naming policy default is UCMA.	

Variable	Description	Value
ASA Administrative User	The user login name for the ASA administrative user as specified in Active Directory. The name can be determined by viewing the user properties in Active Directory under the **Account** tab. The value entered here must take the form <user_name>@<domain>	
ASA Endpoint Listener Port	This is the port defined in the ProxyRequest of ASA application manifest installed on OCS server.	
ASA Application Name	The name as it appears in the front end scripts.	
Custom Offline Presence Service	Can be enabled for extended presence. When a contact is offline, the presence indicator displays a line of text. Default is Disabled.	
Custom Offline Text	The default text is: Offline (IM/ Mobile Call Available)	
Aggregated Presence	Select Yes to enable Aggregated Presence, which publishes the users aggregated presence into ACE.	
Aggregated Presence User	The user name for the Aggregated Presence User as specified in Active Directory. The name can be determined by viewing the user properties in Active Directory under the **Account** tab. The value entered here must take the form <user_name>@<domain>	
Aggregated Presence Endpoint Listener Port	The Aggregated Presence User uses this port to listen for OCS presence changes.	
Enable Call Control	Select Yes to enable remote call control (RCC). If you are deploying the ASA in conjunction with converged office, select No.	
Enable ACE URI Dialing	Select Yes to enable Avaya ACE URI Dialing.	

Variable	Description	Value
	Avaya ACE URI Dialing can only be enabled if Call Control has also been enabled.	
Enable Calling Direction Call Notification	Select Yes to receive call notifications on the Office Communicator client whenever a user originates a call from a device which is being monitored by Avaya ACE as a telephone-type contact.	
Enable Called Direction Call Notification	Select Yes to receive call notifications on the Office Communicator client whenever a user receives a call on a device which is being monitored by Avaya ACE as a telephone-type contact.	

1. Copy the ASA software files to the OCS server.
2. Double click on `setup.exe` to start the installation.
3. In the Welcome to the Avaya ACE Server Agent Setup Wizard window, click **Next**.
4. In the Select Installation Folder window, specify a location for the software. Ensure that the **Everyone** check box is selected and then click **Next**.
5. In the Confirm Installation window, click **Next**.
6. The installation begins. The Welcome to Avaya ACE Server Agent Configuration window, opens. Click **Next**
7. In the ACE Configuration window, enter the following data:

Variable
ACE IP Address/FQDN
ACE Username
ACE Password

8. Click the **Yes** checkbox if NAT firewall traversal is required for ACE to communicate with ASA.
9. If you clicked the**Yes** checkbox in the step above, enter the public IP address of the ASA server if NAT firewall traversal is enabled. This value is not required if there is no NAT firewall between ASA and Avaya ACE.
10. Click **Next**

11. In the OCS Domain Information window window, select the Active Directory server from the list.
12. Click **Next**
13. In the OCS Configuration window, use the arrow button to move the OCS servers that ASA will communicate with into the **Selected OCS Servers** box.
14. **Transport Layer Security** between ASA and OCS is enabled by default. Deselect this option if you do not want communications between ASA and OCS to be encrypted via TLS.
15. Select **Enable OCS Health Monitoring** for ASA to monitor the health of the OCS Front End(s).

    Note that this option requires the ASA Administrative user to have Administrative privileges on the OCS front end(s) in the pool or standalone server. Do not select this option unless the ASA Administrative user has Administrator privileges on the OCS front end(s).
16. Click **Next**
17. In the Avaya ACE Server Agent Configuration window, enter the IP Address of the ASA.
18. Enter the **Certificate Friendly Name**. The network naming policy default is **UCMA**.
19. In the **ASA Administrative User** box, enter the user login name of the user created in Active Directory for the ASA service. The user login name can be found in the user properties window under the **Account** tab and must be in the form:

    `<user_name>@<domain>`
20. Enter the **ASA Endpoint Listener Port**. The port number has to be the same port defined in the ProxyRequest of ASA application manifest installed on OCS server. Use the default value unless otherwise required.

    Enter the **ASA Application Name**. Use the default value unless otherwise required.

    Click **Next**.
21. In the ASA Service Configuration window, click the **Yes** check box if you want to enable **Custom Offline Presence Service** and enter the text you want displayed in the **Customized Offline Text**.
22. Click the **Yes** check box if you want to enable **Aggregated Presence**.
23. In the **Aggregated Presence User** box, enter the user login name of the user created in Active Directory for the ASA service. The user login name can be found in the user properties window under the **Account** tab and must be in the form:

    `<user_name>@<domain>`
24. Enter the **Aggregated Presence Endpoint Listener Port**. Use the default value unless otherwise required.

25. Click the **Yes** check box if you would like to **Enable Call Control**.
26. Click the **Yes** check box if you would like to **Enable ACE URI Dialing**. Note that ACE URI Dialing will not function unless Call Control has been enabled.
27. Click the **Yes** check box if you would like to enable Calling Direction Call Notification.
28. Click the **Yes** check box if you would like to enable Called Direction Call Notification.
29. Click **Next**.
30. In the Configuration Summary window, review the data and then click **Next**.
31. The second Configuration Summary window informs you that the configuration parameters have been saved. Click **Finish**.
32. The Installation Complete window informs you that ASA has been successfully installed. Click **Close**.
33. Continue with the installation process. See Installing the Avaya ACE service agent on page 59.

Updating a Windows 2003 CA for ASA on Windows 2008

For an ASA installed in a standalone server, a Server Authentication type certificate must be installed on the ASA server. The certificate must be issued by the Enterprise Root certificate authority (CA) node serving the OCS Forest.

If the ASA is installed on a Windows 2008 server and the CA is on a Windows 2003 server, you must perform this procedure to install a Microsoft patch.

1. Open a web browser and go to http://www.microsoft.com from a Windows 2003 server machine where you have certificate authority installed.
2. Hover your mouse over **Downloads and Trials**, and click on **Download Center**.
3. In the search box, enter **KB922706** and hit **Enter**.

   Once the search results return, click on the link **Download details: Update for Windows Server 2003 x64 Edition (KB922706)**.
4. Click Download and save the file to your desktop.
5. Open and Run the executable file which was saved to your desktop.
6. Accept the User Agreement and click **Next** to complete the install.

Requesting a certificate

For an ASA installed in a standalone server, a Server Authentication type certificate must be installed on the ASA server. The certificate must be issued by the same Certificate Authority (CA) issuing certificates for the OCS Forest.

Prerequisites

- In order for the CA to issue a Server Authentication type certificate, the CA must be configured with the Web Server certificate templates.
- You must know the IP address of the CA server.
- In the Certificates Request form, accept the default values except for the following variables:

Variable	Value
Certificate type	Server Authentication
Server / application name	FQDN of the ASA server
Certificate friendly name	Defined during ASA install (the default is UCMA)

1. Launch certificate request web enrollment form from the server where you have installed ASA. Open a web browser and go to http://<Certificate_Authority_Server_IP>/certsrv/certrqma.asp.
2. Under **Identifying Information**, complete the fields.

   If you deployed on an Enterprise Edition lab, in the Name field enter the fully qualified host name of the pool.

   If you deployed on a Standard Edition lab, in the Name field enter the fully qualified host name of the OCS server.
3. Under **Type of certificate**, select the Server Authentication certificate.
4. Under **Key Options**, select "Microsoft Enhanced RSA and AES Cryptographic Provider" in the **CSP** dropdown menu, select an appropriate number for **Key Size** and select the check box beside **Mark Keys as exportable**.
5. Under **Additional Options**, enter the certificate **Friendly Name** value that was defined during the ASA install.
6. Click **Submit**.
7. Log in to the certificate authority server.

8. Open the machine's Certificate Authority.

   Go to **Start**, **Administrative tools** and click on **Certificate Authority**.

9. In the Certificate Authority window, expand the **OCS** folder, then expand the **Pending requests** folder.
10. Right-click on the certificate requested and select **All tasks** > **Issue**.
11. From the ASA server, open a web browser and go to `http://<Certificate_Authority_Server_IP>/certsrv/`

    Click **View the status of a pending certificate request** and on the following page, click **Install this certificate**.

12. On the taskbar, click **Start** and then **Run**.
13. In the Run window, type **`mmc`**.
14. In the Console1 window, select **File** and then **Add/Remove Snap-in...**
15. In the Add/Remove Snap-in... window, select **Add**
16. In the Add Standalone Snap-in window, select **Certificates** and select **Add**.
17. In the Certificates Snap-in window, select **My user account** and then select **Finish**.
18. Click **Close** and **OK** to close the Add Standalone Snap-in and Certificates Snap-in windows.
19. Navigate to the certificate that was just installed.

    In the Console1 window, expand the **Certificates - Current User** folder, the **Personal** folder and the **Certificates** folder.

20. Right-click the certificate that was just installed and select **All Tasks** > **Export...**
21. In the Certificate Export Wizard window, select **Yes, export the private key** and select **Next**.
22. Select **Personal Information Exchange** and ensure **Include all certificates in the certification path if possible** and **Export all extended properties** is selected.

    Click **Next**.

23. Enter a password and select **Next**.
24. Choose a location to save the certificate, save it as `.pfx` file and select **Save**.
25. Navigate to the certificate saved above and double click on it. Select **Next** in the pop up window to export the certificate.
26. In the Certificates snap-in window, select **Computer account** and click **Next**.
27. Navigate to the certificate.

28. In the Console1 window, expand the **Certificates (Local Computer)** folder, and right-click on the **Personal** folder, highlight **All Tasks** and select **Import...**.
29. Enter the password and select **Next**.

Granting private-key certificate access to the ASA administrative user on a Windows 2008 server

The ASA administrative user requires private key access to the certificate configured for ASA within the local computer personal certificate store. For Windows 2003, this permission is automatically granted during the ASA installation procedure. For Windows 2008, perform this procedure on the computer where ASA is installed.

Prerequisites

The certificate for the ASAapplication must already be installed in the Local Computer personal certificate store.

1. From the Windows **Start** menu, select **Run**.
2. In the Run window, enter
   `mmc`
3. In the console window, click **File** and select **Add/Remove Snap-in**.
4. In the Add/Remove Snap-in window, select **Certificates** and then click **Add**.
5. In the Certificates snap-in window, click the **Computer account** option button and then click **Next**.
6. In the Select Computer window, click the **Local computer** option button and then click **Finish**.
7. In the Add or Remove Snap-ins window, click **OK** .
8. In the Console window, expand **Certificates (Local Computer)**, click **Personal** folder, and then click **Certificates** folder.
9. Select the certificate, right click, select **All Tasks**, and select **Manage Private Keys**.
10. In the Permissions for UCMA private keys window, click **Add**.
11. Click **Locations**.
12. The Network Password window opens. Enter the user ID and password to log in to the domain.
13. In the Locations window, expand **Entire Directory** and then select the domain.

14. Click **OK**.
15. In the Select Users, Computers, or Groups window, the **From this location** field is populated with the domain name.
16. Click **Advanced** and then **Find Now**.
17. The Search results field lists all the users in the domain. Select the ASA administrative user.
18. Click **OK** and then click **OK** again.
19. Verify that the user is now displayed in the list of users permitted to access the private key of the certificate. Verify that the check box **Full Control** is checked.
20. Click **Apply** and then click **OK**.

Configuring the web server certificate friendly name on the OCS server

If you are deploying the ASA coresident on the OCS server, you must define the friendly name for the web server certificate on the OCS server. A certificate is issued as part of the OCS installation process.

Do not perform this procedure if the ASA is deployed on a standalone server.

Important:
Do not configure more than one certificate with the same friendly name.

1. From the Windows **Start** menu, select **Run** and then enter `mmc` .
2. Click **OK**.
3. In the Console window, click on the **File** menu and select **Add/Remove Snap-in**.
4. In the Add/Remove Snap-in window, click **Add**.
5. In the Add Standalone Snap-in window, select **Certificates** and then click **Add**.
6. In the Certificates snap-in window, click the **Computer account** option button and then click **Next**.
7. In the Select computer window, click the **Local computer** option button and then click **Finish**.
8. In the Certificates Snap-in window, click **Close**.
9. In the Add Standalone Snap-in window, click **Close**.

10. In the Add/Remove Snap-in window, click **OK**.
11. In the Console window, right click on **Certificates (Local Computer)** and select **Find Certificate**.
12. In the Find Certificates window, select
    - Find in: All certificate stores
    - Contains: <OCS_server_host_name>
    - Look in field: Issued to
13. Click **Find Now**.
14. Look for the certificate with the intended purpose **Server authentication**.
15. Double click on the certificate and in the Certificate window, select the **Details** tab.
16. Look for the field **Certificate Template Name** and verify that the value is **Web Server**.
17. Click **Edit Properties** and define the **Friendly Name** property based on your network naming policy. The network naming policy default is **UCMA**.
18. Click **Apply** and then **OK**.

Configuring active directory users for RCC

To enable Avaya ACE™ services, OCS users in the active directory must be configured for Avaya ACE. Use this procedure when configuring users for RCC. The RCC option is used when deploying Avaya ACE unified communication for Microsoft OCS using the CS 1000 and the Avaya Contact Center (MLS) service providers.

Important:
Users may be enabled for RCC as part of the CS 1000 and the Avaya Contact Center Manager (MLS) Converged Office configuration.

Prerequisites

- Users have been defined as a Windows entity in the active directory.
- Users have been enabled for OCS.

1. Log in as an administrative user on the OCS server where the active directory is installed.
2. Launch the active directory. Click **Start**, then **Administrative Tools**, and then **Active Directory Users and Computers**.
3. In the Active Directory Users and Computers window, expand the domain name of the OCS server, then click **User**.
4. The list of users is displayed in the right-hand pane. Right-click on the user name you want to configure and select **Properties**.
5. In the Properties window, click the **Communications** tab and note the value of the Sign-in name which is in the format **sip:<user_name>@<domain>**.
6. Click **Configure**.
7. In the User Options window, select **Enable RCC**.
8. In the **Server URI** box, enter the Sign-in name noted from the previous screen. The value must be entered in the form **sip:<user_name>@<domain>**.
9. In the **Line URI** box, enter the active directory phone number for this user, prefixed with tel:+. For example: `tel:+11231234567`
10. Click **OK** to close the User Options window.
11. Click **OK** to close the Properties window.

Configuring an ASA administrative user account on the Avaya ACE™ server

You must create an Avaya ACE user account with administrative privileges for the ASA administrative user.

1. Open a web browser and log in to the Avaya ACE GUI as administrator.
   `https://<ACE-server>:9443/oamp`
2. On the menu bar, choose **Security**, **User Management**, and then **Create User**.
3. On the User tab, specify the name of the ASA administrative user in the **User ID** field, and a password for the account in the **User Password** and **Confirm User Password** fields.
4. Click **Submit** to save the changes.

The User Creation Success window appears, displaying the settings for the user you have created.

5. On the menu bar, choose **Security**, **User Group Management**, and then **Create User Group**.

   The Create User Group window appears.

6. Specify a name for the ASA administrative user group (for example, OCSUserGroup).
7. In the **User Group Type** field, select **System Administrator** from the drop-down menu.
8. In the **Parent User Group** field, select **SystemAdminGroup** from the drop-down menu.
9. In the **Membership Information** area, assign the ASA administrative user account you created to the new user group by selecting the ASA administrative user account from the **Available Users** list and moving it to the **User Group Members** list.
10. In the **User Group Policy** area, set the **Access Level** field to Admin (using the drop-down menu) for the web services being deployed.
11. Click **Submit** to save your changes.

    The User Group Details window opens, displaying the settings for the user group you have created.

Configuring OCS users on the Avaya ACE ™ server

In order to complete this procedure, you must understand Avaya ACE user management. For information on Avaya ACE user management, see *Avaya Agile Communication Environment™ Administration* (NN10850-005).

In order to integrate Avaya ACE and OCS, you must create an Avaya ACE user for each corresponding OCS user. The specific requirements for Avaya ACE users in an OCS environment are listed below.

Table 5: OCS user profile requirements for CS 2000 service provider

Each OCS user must be configured with three contacts: one in the OCS domain, one for CS 2000 telephony presence via the SIP_IN service provider (ISSG), and one for 3rd-party call control of a CS 2000 device via the SIP service provider (SST). For each user, the **Contact Name** can be any value. For the contact in the OCS domain, the **Contact Identifier** string `<user_name>@<OCS_domain>` must match the "Sign-In name" for this user in Active Directory. The Sign-In name can be determined by viewing the user properties in Active Directory under the **Communications** tab. Note that the Sign-In name is not necessarily

the same as the Active Directory user account name (SAM Account Name or User Principal Name). Also note that for the ACE Contact Identifier, the `sip:` prefix must be replaced with the `ocs:` prefix. For the contact associated with CS 2000 telephony presence, the **Contact Identifier** string can use the `sip:` or `tel:`. The phone number format depends on the network dialing plan, but the digits configured here must match those that will be sent by the ISSG when forwarding CS 2000 telephony presence for this user. You can also add additional telephone contacts. For the contact associated 3rd-party call control of a CS 2000 device, the Contact Identifier string must use the `tel:` format in conjunction with an E.164 number that matches the corresponding OCS user contact's Line-URI.			
Domain	**Contact Name**	**Contact Type**	**Contact Identifier**
OCS	<user_name>	Chat	ocs:<user_name>@<OCS_domain>
CS 2000 ISSG	<user_name>	Telephone	sip:<phone_number>@<IP_domain> tel:<phone_number>
		Other	sip:<phone_number>@<ss7_domain>
CS 2000 SST	<user_name>	Telephone	tel:<E.164>

Configuring service providers on the Avaya ACE™ server

In order to integrate Avaya ACE and OCS, you must define the network elements that will provide the telephony services to the OCS users. For information on configuring service providers, see *Avaya Agile Communication Environment™ Administration* (NN10850-005).

Installing the application manifest file on an OCS server

Enable the ASA.am script for each OCS server. The ASA.am script is located in the ASA install folder.

1. Locate the ASA.am file in the ASA install folder
2. Copy this file to each OCS server machine and record the location.
3. From the Windows **Start** menu, select **Administrative Tools** and then **Office Communications Server 2007**.
4. In the OCS window, in the navigation tree on the left, expand **Forest**. If there is a **Domains** folder under **Forest**, expand the folder.
5. Expand **Standard Edition Servers**.
6. Expand the OCS server where you want to install the application manifest file.
7. Expand the fully qualified domain name of the server.
8. Open the Properties window.
   - For an R1 OCS server, right-click on **Applications** and click **Properties**.
   - For an R2 OCS server, right-click on **Front End Scripts** and click **Properties**.
9. In the Properties window, click **Add** .
10. In the Add windows, browse to the location of the ASA.am file.
11. Enter the name enabled for the ASA application name.
12. Enter the URI that is contained in the manifest file.
13. Click **OK** to close the Add window.
14. In the Properties window, in the **Available Applications** list, select the ASA entry, and then click **Up** to move the entry up the list. It should be the fifth entry, after IMFilter and before UserPINService.
15. Click the check box **Enabled**.
16. Click **OK** to close the Properties window.
17. Check the Windows Event Viewer to see that the script has been started correctly.
18. Repeat this procedure for each OCS server.

Starting the Avaya ACE ™ service agent on the OCS server

You must restart ASA after the configuration file has been edited.

Important:
Office Communicator must be restarted after ASA installation.

Prerequisites

This procedure requires configuration of the ASA service with the ASA administrative user. Prior to performing this task you must first verify the following for the ASA administrative user:.

- The ASA administrative user must be created in Active Directory and enabled for the Office Communications Server Front End or Pool being monitored by ASA.
- The ASA administrative user must be a member of the RTCUniversalServerAdmins group for the domain.
- The ASA administrative user must be a member of the Performance Monitor Users group for the local computer where ASA is installed.
- The ASA administrative user must have permission to access the private key of the certificate configured for ASA in the local computer personal certificate store where ASA is installed.
- The ASA administrative user must have a corresponding Avaya ACE user profile belonging to an Avaya ACE user group with administrative privileges.

See ASA users for more details on the ASA administrative user.

1. From the Windows **Start** menu, select **Control Panel**, then **Administrative Tools**, and then **Services**.
   In the Services window, locate the **Avaya ACE Server Agent**. Right click on the service and select **Properties**.
2. In the service Properties window, click the **Log on** tab.
3. Click the **This account** option button.
4. Click **Browse**.
5. Click **Locations**.
6. The Network Password window opens. Enter the user ID and password to log in to the domain.
7. In the Locations window, expand **Entire Directory** and then select the domain.
8. Click **OK**.
9. In the Select User window, the **From this location** field is populated with the domain name.
10. Click **Advanced** and then **Find Now**.

11. The Search results field lists all the users in the domain. Select the ASA administrative user.
12. Click **OK** and then **OK** again.
13. In the Avaya ASA Properties window, enter the password for the Administrator user ID in the **Password** and **Confirm Password** fields.
14. Click **Apply** and then **OK**.
15. In the Services window, right click on the ASA service and select **Start**.

Chapter 11: Troubleshooting ASA installation

Use the information in this chapter to help troubleshoot issues related to Avaya Agile Communication Environment™ (ACE) Service Agent (ASA) installation and startup.

Navigation

ASA Presence Service fails to initialize

If the ASA Presence service fails to initialize, it may be due to the ASA administrative user having insufficient privileges to access the private key of the certificate used to communicate with OCS. To resolve this issue, there are separate procedures for Windows Server 2003 and Windows Server 2008.

For Windows Server 2003, see the troubleshooting procedure Configuring certificate private key access to the ASA administrative user on Windows Server 2003 on page 88.

For Windows Server 2008, see the installation procedure Granting private-key certificate access to the ASA administrative user on a Windows 2008 server on page 77.

ASA Service fails to create a Logs directory

If the ASA service fails to create a logs directory during initial startup, it may be due to the ASA Administrator user lacking sufficient privileges to write to the installation directory. Since the

installation is performed by an administrative user, depending upon your local security policy, the ASA administrative user may not have been granted sufficient access to the ASA installation directory. This issue may also cause ASA startup to fail.

See the procedure Granting the ASA administrative user access permissions to the ASA installation directory on page 89.

ASA Presence or Call Notification service fails to enable

If the ASA Presence Service fails to enable, it may be due to the ASA administrative user lacking sufficient permissions to start the HTTP controller on the presence service port.

If the ASA Call Notification Service fails to enable, it may be due to the ASA administrative user lacking sufficient permissions to start the HTTP controller on the call notification service port.

There are separate procedures for Windows Server 2003 and Windows Server 2008.

For Windows Server 2003, see Granting the ASA administrative user permission to start the HTTP controllers on Windows Server 2003 on page 90.

For Windows Server 2008, see Granting the ASA administrative user permission to start the HTTP controllers on Windows Server 2008 on page 91.

Configuring certificate private key access to the ASA administrative user on Windows Server 2003

Use this procedure to grant the ASA administrative user access to the private key of the local computer certificate used for communication with the OCS front end(s).

Prerequisites

- The certificate issued for ASA communication with OCS must be installed in the local computer personal certificate store.
- You must be able to log in to the ASA host computer as an administrative user.
- The winhttpcertcfg utility must be installed on the computer hosting ASA as part of the prerequisites for installing ASA. If the winhttpcertcfg utility was not installed, refer to the procedure Installing ASA prerequisite software packaged with Avaya ACE on page 66.
- You must know the full distinguished name (DN) of the ASA administrative user (Active Directory domain + user account name).

1. Log on to the ASA host computer as an administrative user.
2. From the Windows **Start** menu, select **Run**.
3. In the Run window, enter **cmd** and press **Enter**.
4. Navigate to the directory where the `winhttpcertcfg` utility was installed. If you accepted the default installation directory, the program will be installed in:
   - 32 bit version: `C:\Program Files\Windows Resource Kits\Tools\`
   - 64 bin version: `C:\Program Files (x86)\Windows Resource Kits\Tools\`
5. Enter the command `winhttpcertcfg.exe -g -c LOCAL_MACHINE\My -s <fully_qualified_computer_name> -a <Domain\user>`where
   - *<fully_qualified_computer_name>* is the complete hostname of the computer where ASA is installed.
   - *<Domain\user>* is the Windows Domain and user account name of the ASA administrative user.
6. Verify that the output returned from this command includes the confirmation `Granting private key access for account: <Domain\user>.`

Granting the ASA administrative user access permissions to the ASA installation directory

Use this procedure to grant the ASAadministrative user access to the ASAinstallation directory in order to write to the ASA log files.

Prerequisites

You must be able to log in to the ASA host computer as an administrative user.

1. Log on to the ASA host computer as an administrative user.
2. Open a Windows Explorer tool and navigate to the ASA installation directory. By default this directory is `C:\Program Files\Avaya\ACE\:Avaya ACE(TM) Server Agent .`
3. Right click on the installation folder and select **Properties**.
4. In the Properties window:
   - for a Windows 2003 server, click the **Security** tab and then click **Add**

- for a Windows 2008 server, click **Edit** and then click **Add**

5. In the Select Users, Computers or Groups window, click **Advanced** and then **Locations**.
6. In the Locations window, navigate to the parent domain of the ASA administrative user and select this domain.
7. Click **OK**.
8. In the Select Users, Computers or Groups window, enter the user name of the ASA administrative user in the **Name: Starts With** box.
9. Click **Find Now**.
10. Verify that the ASA administrative user appears in the list of names returned.
11. Select the ASA Administrative user and then click **OK**.
12. In the Select Users, Computers or Groups window, click **OK**.
13. In the Properties window, select the ASA administrative user.
14. Check the box to **Allow Full Control** of the folder for the ASA administrative user.

Granting the ASA administrative user permission to start the HTTP controllers on Windows Server 2003

Prerequisites

- You must be able to log in to the ASA host computer as an administrative user.
- You must have the httpcfg utility installed. See Downloading and installing prerequisite software on page 68.

1. Log in to the ASA host computer as an administrative user.
2. From the Windows **Start** menu, select **Run**.
3. In the Run window, enter **cmd** to open a console window.
4. Navigate to the ASA installation directory. The default path is `C:\Program Files\Avaya\ACE\ACE Server Agent\`
5. Enter the following command to generate output for port 8012.
   `UrlAclGenerator2K3.exe 8012 <domain_name>\<user_name>`

where

- <*domain_name*> is the fully qualified domain of the ASA administrative user
- <*user_name*> is the user account name of the ASA administrative user

The output from the command is similar to the following: `httpcfg set urlacl /u http://*:8012/ /a <sddl>` where <*sddl*> is the ASA administrative user represented in security definition descriptor language.

6. Copy the output.
7. From the Windows **Start** menu, select **Programs**, then **Windows Support Tools**, and then **Command Prompt**, to open the Windows Support Tools command prompt.
8. Paste the command generated by the UrlAclGenerator into the command prompt and press `Enter`.

   The command output should be. `HttpSetServiceConfiguration completed with 0`
9. Enter the command to generate output for port 8013.

   `UrlAclGenerator2K3.exe 8013 <domain_name>\<user_name>`
10. Copy and paste the command output into the Windows Support Tools command prompt and verify the command output.
11. Enter the command to generate output for port 8014.

    `UrlAclGenerator2K3.exe 8014 <domain_name>\<user_name>`
12. Copy and paste the command output into the Windows Support Tools command prompt and verify the command output.

Granting the ASA administrative user permission to start the HTTP controllers on Windows Server 2008

Prerequisites

- You must be able to log in to the ASA host computer as an administrative user.
- You must have the netsh utility installed. The netsh utility is typically deployed by default during installation of Windows Server 2008 and is located at `C:\Windows\System32\netsh .`

1. Log in to the ASA host computer as an administrative user.
2. From the Windows **Start** menu, select **Run**.

3. In the Run window, enter **cmd** to open a console window.
4. Enter the following command to check whether the http url reservation exists or not. Enter

   ```
   netsh http show urlacl
   ```

   Check for the following urls:

   - http://*:8012/
   - http://*:8013/
   - http://*:8014/
5. If the above url reservations exist for a specfic user which will not be used to start ASA, then use following commands to remove them. If not, proceed to step 6.

   ```
   netsh http delete urlacl url=http://*:8012/ netsh http delete urlacl url=http://*:8013/ netsh http delete urlacl url=http://*:8014/
   ```
6. Enter the following commands to reserve the urls for the user will be used to start ASA.

   ```
   netsh http add urlacl url=http://*:8012/ user=<domain_name>\<user_name> netsh http add urlacl url=http://*:8013/ user=<domain_name>\<user_name> netsh http add urlacl url=http://*:8014/ user=<domain_name>\<user_name>
   ```

   where

   - <*domain_name*> is the fully qualified domain of the ASA administrative user
   - <*user_name*> is the user account name of the ASA administrative user
7. Verify that after each command is entered, the netsh utility indicates `URL reservation successfully added .`

Chapter 12: ACE service agent logs

This section contains procedures to view Avaya ACE service agent (ASA) logs and change the logging level.

Navigation

Viewing ASA events

View events generated by the ASA.

This procedure describes how to view ASA events in the Windows Event Viewer. Events are also written to the `SystemOut.log` file at `<ASA_install_directory>\logs` . With the default configuration settings, the log file can reach a maximum size of 10 MB before rollover, or it rolls over weekly. Old files are overwritten.

1. From the Windows **Start** menu, select **Control Panel** and then **Administrative Tools**.
2. Double click on **Event Viewer**.
3. In the Event Viewer window navigation tree, click **Application**.

   The window displays a list of events. Events generated by the ACE application agent display **Enterprise Library Log** in the **Source** column.

Configuring the ASA log level

Change the log level by editing the `logging.config` file and the `AvayaASA.config` file.

The log level controls which event messages are available for viewing in the Windows Event Viewer and are saved to the `SystemOut.log` file. The ASA has three log levels, Error, Warning, and Information. The default setting is to save all logs.

1. Log in to the OCS server.
2. The `logging.config` is located at the top level of the ASA install folder. Open the `logging.config` file in a text editor.
3. Search for the string `logFilters` . The log level section of the configuration file is shown below. The example below shows the default setting, where all logs are saved.

```
<logFilters>

    <add categoryFilterMode="DenyAllExceptAllowed"
type="Microsoft.Practices.EnterpriseLibrary.Logging.Filters.CategoryFilte
r,Microsoft.Practices.EnterpriseLibrary.Logging, Version=3.1.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" name="CategoryFilter"
        <categoryFilters>
            <add name="Warning Category" />
            <add name="Information Category" />
            <add name="Error Category" />
        <categoryFilters>
    </add>
<logFilters>
```

4. To change the log level, comment out the level you want to exclude. For example, to exclude Information level logs, change `<add name="Information Category" />` to`<!--<add name="Information Category" />-->`
5. Save and close the file.
6. The `AvayaASA.config` is located at the top level of the ASA install folder. Open the `AvayaAS.config` file in a text editor.
7. Modify the second line in the file from `<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">` to `<configuration>` .
8. Save and close the file.
9. To apply the changes, you must restart ASA. From the Windows **Start** menu, select **Control Panel**, then **Administrative Tools**, and then **Services**.
10. In the Services window, locate the Avaya ACE(TM) Server Agent service. Right click on the service and select **Restart**.

Configuring event message output

Change the event message output by editing the `AvayaASA.config` file.

Event messages can be made available for viewing in the Windows Event Viewer and saved to the `SystemOut.log` file. The ASA has three log levels, Error, Warning, and Information. You can configure the output for each log level.

1. Log in to the OCS server.
2. The `AvayaASA.config` is located at the top level of the ASA install folder. Open the `AvayaASA.config` file in a text editor.
3. Search for the string `categorySources` . The categorySources section of the configuration file is shown below. The example below shows the default setting, where for each log level, event messages are sent to both the Event Viewer and the `SystemOut.log` file.

```
<categorySources>
    <add switchValue="Error" name="Error Category">
        <listeners>
            <add name="Formatted EventLog TraceListener" />
            <add name="Rolling Flat File Trace Listener" />
        </listeners>
    </add>
    <add switchValue="All" name="Information Category">
        <listeners>
            <add name="Formatted EventLog TraceListener" />
            <add name="Rolling Flat File Trace Listener" />
        </listeners>
    </add>
    <add switchValue="Warning" name="Warning Category">
        <listeners>
            <add name="Formatted EventLog TraceListener" />
            <add name="Rolling Flat File Trace Listener" />
    </add>
</categorySources>
```

4. For each log level, the following line sends event messages to the Event Viewer: `<Formatted EventLog TraceListener" />`

   For each log level, the following line sends event messages to the `SystemOut.log` file: `<add name="Rolling Flat File Trace Listener" />`

   To stop sending event messages for a log level to the Event Viewer or `SystemOut.log` file, comment out the appropriate line. For example, to stop sending event messages to the Event Viewer, change `<add name="Formatted EventLog TraceListener" />` to `<!--<add name="Formatted EventLog TraceListener" />-->`
5. Save and close the file.

6. To apply the change, you must restart ASA. From the Windows **Start** menu, select **Control Panel**, then **Administrative Tools**, and then **Services**.
7. In the Services window, locate the Avaya ACE(TM) Server Agent service. Right click on the service and select **Restart**.

Configuring the log file rollover settings

Change the log level by editing the `AvayaASA.config` file. You can configure the maximum size of the file and the rollover interval. With the default configuration settings, the log file can reach a maximum size of 20 MB before rollover, or it rolls over weekly. Old files are overwritten.

1. Log in to the OCS server.
2. The `AvayaASA.config` is located at the top level of the ASA install folder. Open the `AvayaASA.config` file in a text editor.
3. Search for the string `loggingConfiguration` . The log file configuration section of the configuration file is shown below. The example below shows the default settings, where the rollover size is 20000 KB and the rollover interval is weekly.

```
<loggingConfiguration name="Logging Application Block" traci
ngEnabled="true" defaultCategory="Information Category"
logWarningsWhenNoCategoriesMatch="false">
    <listeners>
        ...
        <add fileName="Logs\\SystemOut.log" rollSizeKB="20000" timeStamp
Pattern="yyyy-MM-dd" rollFileExistsBehavior="Overwrite"
rollInterval="Week" formatter="Text Formatter"
```

4. Change the settings for the `rollSizeKB` and `rollInterval` variables as required.

   where

   - *rollSizeKB* is the maximum file size in kiloBytes.
   - *rollInterval* is the rollover interval. Possible values are Minute, Hour, Day, Month or Year.

5. Save and close the file.

Chapter 13: Uninstalling the Avaya ACE™ Server Agent

Use this procedure to uninstall the Avaya Agile Communication Environment™ (ACE) plugin.

1. From the Windows **Start** menu, select **Control Panel**, then **Administrative Tools**.
2. In the Administrative Tools window, double click **Services**.
3. In the Services window, select the **Avaya ACE Server Agent** service.
4. Click **Stop the service**.
5. Close both the Services window and the Administrative Tools window.
6. From the Windows **Start** menu, select **Control Panel**, then **Add or Remove Programs**.
7. In the Add or Remove Programs window, select **Avaya ACE Server Agent** and then click **Remove**.
8. You are prompted to confirm the uninstall. Click **Yes**.
9. Verify that the service has been removed. From the Windows **Start** menu, select **Control Panel**, then **Administrative Tools**, and then **Services**.
   Verify that the Avaya ACE(TM) Server Agent service is not listed.
10. Close both the Services window and the Administrative Tools window.