

Avaya Solution & Interoperability Test Lab

Application Notes for Microsoft Office Communicator Clients with Avaya Communication Manager Phones - Issue 1.1

Abstract

These Application Notes describe the configuration procedures for enabling Microsoft Office Communicator (MOC) clients to operate Avaya Communication Manager phones. The MOC client and Microsoft Office Communications Server (OCS) provide the user with multiple modes of communications, such as Instant Messaging (IM), voice, and video. The configuration steps described herein focus on the TR/87 integration between Avaya Application Enablement Services and Microsoft OCS. The TR/87 integration allows MOC clients to make and answer calls on Avaya Communication Manager phones, as well as perform basic call control operations such as hold/retrieve, transfer, and disconnect.

1. Introduction

These Application Notes describe the procedures for configuring TR/87 integration between Avaya Communication Manager and Microsoft Office Communications Server (OCS). The TR/87 integration allows a Microsoft Office Communicator (MOC) client running on a Microsoft Windows computer to operate an Avaya Communication Manager phone using CSTA CTI call control constructs.

Microsoft OCS is comprised of several component servers that may run on the same physical Microsoft Windows server or on separate physical servers, depending on the desired capacity, topology, and security. Consult [4] and [5] for further details on the Microsoft OCS architecture and deployment options. The MOC client is a Microsoft Windows application that allows the user to communicate with other MOC users using any combination of Instant Messaging (IM), audio, and video, in both point-to-point and conferencing scenarios. For voice communications, each MOC client may be configured as an Enterprise Voice (EV) or a Remote Call Control (RCC) client. EV mode is configured when the user wants voice calls to be established on the computer on which the MOC client runs, whereas RCC mode is configured when the user has an existing PBX phone and wants voice calls to be established on the PBX phone. More specifically, in EV mode, Microsoft OCS handles the user's voice calls, whereas in RCC mode, the PBX handles the user's voice calls and the MOC client only provides a user interface for operating the PBX phone. These Application Notes focus on the RCC clients, particularly the configuration required to allow RCC clients to place, answer, hold/retrieve, transfer, and disconnect calls on Avaya Communication Manager phones. The configuration for EV clients, as well as for routing calls between EV clients and Avaya Communication Manager phones, is covered in [1]. It should be noted that these Application Notes also assume that the call routing configuration described in [1] has already been implemented since calls between RCC clients and EV clients are functionally equivalent to calls between Avaya Communication Manager phones and EV clients¹.

2. Configuration

The sample configuration described throughout these Application Notes is shown in **Figure 1**. The Avaya 4600 Series H.323 and SIP Telephones are registered with Avaya Communication Manager (running on the Avaya S8300 Server) and Avaya SIP Enablement Services (SES), respectively. The Avaya Application Enablement (AE) Services server provides interfaces for CTI applications, e.g., Microsoft OCS, to control Avaya Communication Manager elements. For voice communications, the MOC clients in RCC mode are able to operate² Avaya telephones, whereas the MOC clients in EV mode are standalone voice endpoints served by Microsoft OCS.

² Although depicted in **Figure 1** as operating Avaya H.323 telephones, RCC mode MOC clients can also operate Avaya digital and analog telephones (however, operation of Avaya SIP telephones is currently not supported).

RL; Reviewed:
SPOC 11/5/2007

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

¹ Users with RCC clients still have the option of placing voice calls to other MOC users directly from their MOC clients, i.e., instead of using the MOC client to place the calls from their PBX phones. These voice calls always arrive on the called user's MOC client, even if the called MOC client is a RCC client. This is because such calls are internal to Microsoft OCS and are thus not impacted by the call routing between Microsoft OCS and Avaya Communication Manager.

Both RCC and EV clients are registered with Microsoft OCS, which is comprised of one or more of each of the following: Front-End Servers, IM Conferencing Servers, Telephony Conferencing Servers, A/V Conferencing Servers, Web Conferencing servers, and IIS Servers. In the sample configuration of **Figure 1**, the aforementioned component servers reside on a single physical server in an Microsoft OCS Enterprise Edition (EE) Consolidated configuration. The Microsoft OCS server and Mediation Server are supported by a Microsoft SQL 2005 database server, as well as another Microsoft Windows Server running Active Directory (AD), DNS, and Certificate Authority (CA) servers. The Microsoft Exchange 2007 Server is enabled with Unified Messaging and provides e-mail, voicemail, and Auto Attendant services.



operating Avaya 4600 Series H.323 Telephones

Figure 1: Network Configuration

3. Equipment and Software Validated

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

Equipment & Software	Version
Avaya S8300 Server	Avaya Communication Manager
	4.0.1 (R014x.00.1.731.2)
Avaya G350 Media Gateway	-
Media Gateway Processor	26.33.0
Avaya Application Enablement Services Server	4.0.1 (Build 57-0)
Avaya SIP Enablement Services Server	SES-4.0.0.0-033.6
Avaya 4600 Series H.323 IP Telephones	2.8 (4621SW)
	2.8 (4625SW)
Avaya 4600 Series SIP Telephones	2.2.2 (4621SW)
Microsoft Active Directory, DNS Server, and	5.2.3790.1830
Certification Authority on Microsoft Windows Server	
2003 R2 Enterprise Edition Service Pack 2	
Microsoft Exchange 2007 Server on Microsoft Windows	08.01.0085.004
Server 2003 R2 Enterprise x64 Edition Service Pack 2	
Microsoft Office Communications Server 2007 on	3.0.6362.0
Server 2003 R2 Enterprise Edition Service Pack 2	
Microsoft SQL 2005 Server on Microsoft Windows	2005.90.3042.0
Server 2003 R2 Enterprise Edition Service Pack 2	
Microsoft Mediation Server on Microsoft Windows	3.0.6362.0
Server 2003 R2 Enterprise Edition Service Pack 2	
Microsoft Office Communicator on Microsoft Windows	2.0.6362.0
XP Professional Version 2002 Service Pack 2	

 Table 1: Equipment/Software List

4. Avaya Communication Manager and Avaya Application Enablement Services Integration

These Application Notes assume that basic Avaya Communication Manager and Avaya Application Enablement (AE) Services administration has already been performed. These Application Notes further assume that an AE Services connection and TSAPI CTI link has already been configured and established between Avaya Communication Manager and Avaya AE Services.

4.1. Extensions

In the sample configuration, assume that Avaya Communication Manager phones that are associated with RCC clients are assigned 5-digit extensions that begin with "23", Avaya Communication Manager phones that are not associated with RCC clients are assigned 5-digit extensions that begin with "21" and "22", and Microsoft EV clients are assigned 5-digit "extensions" that begin with "3".

4.2. Avaya AE Services License

Launch a web browser, enter the URL https://<IP address of AE Services server>/WebLM/, and log into the Avaya AE Services Web License Manager interface. In the left pane under Licensed Products, click on "Application_Enablement". In the right pane, verify that there are sufficient Unified CC API Desktop Edition licenses; if not, contact an authorized Avaya account representative to obtain any required licenses.

Change Password	License installed on: Jul 30, 2007 4:10:3	32 PM EDT		-
Server Properties > Manage Users	<u>View Peak Usage</u>			
Logout	License Acquisition Status License acquisition Currently fai Licensed Features	enabled: Yes led over: No		
	Feature (Keyword)	Expiration Date	Licensed	Acquired
	Application Enablement Connections (VALUE_AEC_CONNECTIONS)	2008/01/26	16	1
	CVLAN Proprietary Links (VALUE_PROPRIETARY_LINKS)	2008/01/26	8	0
	TSAPI Version (VALUE_TSAPI_VERSION)	2008/01/26	3.1	Not counted
	Applications Enablement Connections Version (VALUE_AEC_VERSION)	2008/01/26	4.0	Not counted
	CVLAN Switch Connections (VALUE_SWITCH_CONNECTIONS)	2008/01/26	8	0
	DLG (VALUE_DLG)	2008/01/26	1	0
	Product Notes (VALUE_NOTES)	2008/01/26	SmallOfferTypes: s8400;chawk;chawk-lsp;csi MediumOfferTypes: s8500;s8500_blade;vm_blade LargeOfferTypes: sray;seagull	Not counted
	TSAPI Simultaneous Users (VALUE_TSAPI_USERS)	2008/01/26	1000	0
	Unified CC API Desktop Edition (VALUE_AEC_UNIFIED_CC_DESKTOP)	2008/01/26	1000	0

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

4.3. TR/87 Port

Launch a web browser, enter the URL https://<IP address of AE Services

server>:8443/MVAP, and log into the Avaya AE Services OAM Web Interface. In the left pane, select **CTI OAM Admin**. In the left pane of the CTI OAM Home Web Interface, select **Administration** \rightarrow **Network Configuration** \rightarrow **Ports**. In the right pane, enable **TR/87 Port** and click on "Apply Changes" (not shown below).

Αναγα			Арг	Dication Operations	Enablement Servio
CTI OAM Home	You are here: >	<u>Administration</u> >	Network Configuration	> <u>Ports</u>	OAM Home OHelp OLo
Administration Network Configuration	Ports				
Local IP NIC Configuration	CVLAN Port	TCP Port	9999		
<u>Ports</u> Switch Connections	DLG Port	TCP Port	5678		
<u>CTI Link Admin</u> <u>DMCC Configuration</u>	TSAPI Port	TCP Port	450		
TSAPI Configuration Security Database 	CSTA Tlinks Port	TCP Port Min	1050]	
<u>Certificate Management</u> <u>TR87 Configuration</u> Status and Control		TCP Port Max	1065]	
<u>Maintenance</u> <u>Alarms</u>	DMCC Server Ports			Enabled Dis	sabled
Logs Utilities		Unencrypted Port	4721] • •	
Help		Encrypted Port	4722	. 0	
		TR/87 Port	4723	. • •	
	H.323 Port				
		TCP Port Min	3000		

5. Certificates

The Avaya AE Services and Microsoft OCS servers must exchange signed server certificates each time a Transport Layer Security (TLS) enabled TCP connection is initiated between the two servers. The certificates must be obtained from the same Certificate Authority (CA) or from CAs in the same certificate chain. In the sample configuration, a Microsoft Enterprise CA (running on Microsoft Windows Server 2003) serves as the CA for both.

5.1. Install Certificate Chain (Trusted Certificate) on Microsoft OCS Server

This section describes the steps for downloading the certificate chain (trusted certificate) from the Microsoft Enterprise CA and installing the certificate chain on a Microsoft OCS server. The certificate chain should actually have already been installed during Microsoft OCS installation; this section is provided for reference and completeness.

Step	Description
1.	On the Microsoft OCS server, launch a web browser and enter the URL http:// <name ip<="" or="" th=""></name>
	address of Certificate Authority server>/certsrv. If prompted for a user name and password,
	enter the credentials of a domain administrator account.
2.	In the Microsoft Certificate Services Welcome page, click on "Download a CA certificate, certificate chain, or CRL".
	Microsoft Certificate Services SITLCA
	Welcome
	Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
	You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
	For more information about Certificate Services, see Certificate Services Documentation.
	Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Step	Description
3.	In the Microsoft Certificate Services Download a CA Certificate, Certificate Chain, or CRL page, select the " Current " CA certificate of the Microsoft Enterprise CA, set Encoding method to " Base 64 ", and click on " Download CA certificate chain ".
	Microsoft Certificate Services SITLCA Home Download a CA Certificate, Certificate Chain, or CRL To trust certificates issued from this certification authority, install this CA certificate chain. To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. CA certificate: Current [SITLCA]
4.	Encoding method: C DER © Base 64 Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL When prompted, save the CA certificate chain file to a local directory on the Microsoft OCS server. After saving, navigate to that directory in Windows Explorer, right-click on the CA
	certificate chain file, and select "Install Certificate".

Step	Description
5.	In the Certificate Import Wizard dialog box, click on "Next".
	Certificate Import Wizard Import Wizard Welcome to the Certificate Import Wizard Use of the certificate trust with the second of th
6.	In the Certificate Import Wizard dialog box, select " Place all certificates in the following store" and click on " Browse ".
	Certificate Import Wizard
	Certificate Store
	Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for
	C Automatically select the certificate store based on the type of certificate
	Place all certificates in the following store
	Certificate store:
	< <u>Back</u> <u>N</u> ext > Cancel

Step	Description			
7.	In the Select Certificate Store dialog box, select "Trusted Root Certification Authorities" and			
	click on " OK ".			
	Calact Cavificate Store			
	Select the certificate store you want to use.			
	Personal			
	Intermediate Certification Authorities Active Directory User Object			
	Trusted Publishers			
	Show physical stores			
	OK Cancel			
8.	In the Certificate Import Wizard dialog box_click on " Next "			
	Certificate Import Wizard			
	Certificate Store			
	Windows can automatically select a certificate store, or you can specify a location for			
	C Automatically select the certificate store based on the type of certificate			
	Place all certificates in the following store			
	Certificate store:			
	Trusted Root Certification Authorities Browse			
	< Back Dext > Cancel			

Step	Description
9.	In the Certificate Import Wizard dialog box, click on "Finish".
	Certificate Import Wizard Image: Completing the Certificate Import Wizard You have successfully completed the Certificate Import wizard. You have specified the following settings: Certificate Store Selected by User Trusted Root Certific Content PKCS #7 Certificates File Name C:\Cert\certnew.p7b
	< <u>Back</u> Cancel
10.	Repeat Steps 1 – 9 on each Microsoft OCS server in the enterprise pool.

5.2. Create Certificate Template for Server Certificates

The server certificates exchanged between Avaya AE Services and Microsoft OCS must support both Server Authentication and Client Authentication. This section describes the steps for creating a certificate template for such server certificates on the Microsoft Enterprise CA.

Step	Description	
1.	On the Microsoft Enterprise CA server, launch the Certification Authority Microsoft Management Console (MMC) snap-in.	
2.	In the left pane of the Certification Authority MMC snap-in, expand the Certification Author node, right-click on Certificate Templates , and select " Manage " to launch the Certificate Templates MMC snap-in.	rity
3.	In the right pane of the Certificate Templates MMC snap-in, right-click on the Web Server template, and select "Duplicate Template".	

Step	Description					
4.	In the Properties of New Template dialog box, select the General tab, and enter a descriptive					
	Template display name and Template name.					
	Proposition of Now Toppelato					
	General Request Handling Subject Name					
	Template display name:					
	Web Server plus Client Authentication					
	Minimum Supported CAs: Windows Server 2003, Enterprise Edition					
	After you apply changes to this tab, you can no longer change the template					
	I emplate name:					
	WebServerClientAuthent					
	Validity period: <u>B</u> enewal period:					
	2 years ▲ 6 weeks ▲					
	Dunot automatically reenroll if a duplicate certificate exists in Active					
	Directory					
5	In the Properties of New Template dialog box select the Request Handling tab, and ensure					
2.	that Purpose is set to " Signature and encryption ". Click on " CSPs ".					
	Properties of New Template					
	Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name					
	Purpose: Signature and encryption					
	Archive subject's encryption private key					
	□ Include symmetric algorithms allowed by the subject					
	Letere revoked or expired certificates (do not archive)					
	Minimum key size: 1024					
	Do the following when the subject is enrolled and when the private key associated with this certificate is used:					
	Enroll subject without requiring any user input					
	Prompt the user during enrollment					
	 Prompt the user during enrollment and require user input when the private key is used 					
	To choose which cryptographic service providers					
	(CSPs) should be used, click CSPs.					
	OK Cancel Apply					

Step	Description
6.	In the CSP Selection dialog box, select "Requests must use one of the following CSPs:" and
	check the "Microsoft Enhanced Cryptographic Provider v1.0" checkbox. Click on "OK".
	CSP Selection
	Choose which cryptographic service providers (CSPs) can be used in requests:
	○ <u>B</u> equests can use any CSP available on the subject's computer
	Requests must use one of the following CSPs:
	<u>C</u> SPs:
	□ Gemplus GemSAFE Card CSP v1.0 ▲
	Microsoft Base Cryptographic Provider v1.0
	Microsoft Base DSS and Dirite-Heilman Cryptographic Provider ✓Microsoft DH SChannel Cryptographic Provider
	✓ Microsoft Enhanced Cryptographic Provider v1.0
	Microsoft Enhanced RSA and AES Cryptographic Provider
	I✓ Microsoft BSA, SUbappel Livotographic Provider
	Cancel
7.	In the Properties of New Template dialog box, select the Subject Name tab and ensure that
	"Supply in the request" is selected.
	Properties of New Template
	Issuance Requirements Superseded Templates Extensions Security
	 Select this option to allow a variety of subject name formats or if you do
	not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.
	C Build from this Active Directory information
	Select this option to enforce consistency among subject names and to
	Subject name format:
	None
	Include e-mail name in subject name
	Include this information in alternate subject name:
	Liser prinicipal name (UPN)
	Service principal name (SPN)
	OK Cancel Apply

Step	Description	
8.	In the Properties of New Template dialog box, select the Extensions tab. In the Extensions	
	included in this template section, select "Application Policies" and click on "Edit".	
	Properties of New Template	
	General Bequest Handling Subject Name	
	Issuance Requirements Superseded Templates Extensions Security	
	To modify an extension, select it, and then click Edit.	
	Extensions included in this template:	
	Certificate Template Information	
	E Key Usage	
	<u>[</u>]	
	Description of Application Policies:	
	Server Authentication	
	OK Cancel Apply	
9.	In the Edit Application Policies Extension dialog box, click on "Add".	
	Edit Application Policies Extension	
	An application policy defines how a certificate can be	
	used.	
	Application policies:	
	Server Authentication	
	Add Edit Remove	

Step	Description	
12.	In the Properties of New Template dialog box, click on " OK ".	
12.	In the Properties of New Template ? General Request Handling Subject Name Issuance Requirements Superseded Templates Extensions To modify an extension, select it, and then click Edit. Egtensions included in this template: Application Policies Certificate Template Information Issuance Policies Edit Escription of Key Usage: Signature Signature Digital signature Allow key exchange only with key encryption Image:	
13.	In the Certification Authority MMC snap-in, expand the Certification Authority node, right- click on Certificate Templates, and select "New → Certificate Template to Issue".	

Step]	Description	
14.	In the Enable Cer	rtificate Templates dialo	g box, select the Certificate Ten	nplate created in Steps
	3 -12 and click on	" OK ".	-	
		Enable Certificate Templates		? ×
l		Select one or more Certificate Templates to ena	ble on this Certification Authority	
		<u> </u>		
		Name	Intended Purpose	▲
		IPSec (Offline request)	IP security IKE intermediate	
		Key Recovery Agent	Key Recovery Agent	
		RAS and IAS Server	Client Authentication, Server Authentication	
		Router (Offline request)	Client Authentication	
		Smartcard Logon	Client Authentication, Smart Card Logon	
		Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
		Trust List Signing	Microsoft Trust List Signing	
		😨 User Signature Only	Secure Email, Client Authentication	
		Web Server plus Client Authentication	Server Authentication, Client Authentication	
		Workstation Authentication	Client Authentication	
				–
			OK Car	ncel

5.3. Request and Install Server Certificate on Microsoft OCS Server

This section describes the steps for requesting the server certificate (based on the certificate template created in Section 5.2) from the Microsoft Enterprise CA and installing the server certificate on a Microsoft OCS server.

Step	Description
1.	On a Microsoft OCS server, launch a web browser and enter the URL http:// <name ip<="" or="" th=""></name>
	address of Certificate Authority server>/certsrv. If prompted for a user name and password,
	enter the credentials of a domain administrator account.
2.	In the Microsoft Certificate Services Welcome page, click on "Request a certificate".
	Microsoft Certificate Services SITLCA Home
	Welcome.
	Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
	You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
	For more information about Certificate Services, see <u>Certificate Services Documentation</u> .
	Select a task:
	Request a certificate View the status of a pending certificate request
	Download a CA certificate, certificate chain, or CRL

Step	Description
3.	In the Microsoft Certificate Services Request a Certificate page, click on "advanced
	certificate request".
	Microsoft Cartificate Services - SITLCA Home
	Request a Certificate
	Select the certificate type:
	User Certificate
	Or, submit an advanced certificate request.
4.	In the Microsoft Certificate Services Advanced Certificate Request page, click on "Create
	and submit a request to this CA".
	Microsoft Certificate Services SITLCA Home
	Advanced Certificate Demust
	The policy of the CA determines the types of certificates you can request. Click one of the following options to:
	Create and submit a request to this CA
	Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base 64 encoded PKCS #7 file.
	A base-on-encoded Fixed and an behalf of another user by using the smart card certificate enrollment station
	Note: You must have an enrollment agent certificate to submit a request on behalf of another user.
5.	In the Microsoft Certificate Services Advanced Certificate Request page, select the
	Certificate Template created in Section 5.2, and configure the fields in the Identifying
	Information For Offline Template section. For Name, enter the FQDN of the Microsoft OCS
	enterprise pool.
	Microsoft Certificate Services SITLCA Home
	Advanced Certificate Request
	Certificate Template:
	Web Server plus Client Authentication
	Identifying Information For Offline Template:
	Name: Entpool.sitIms.net
	E-Mail:
	Company: Avaya
	Department: SITL
	City: Lincroft
	State: New Jersey
	Country/Region: US

Step	Description
6.	Scroll down in the Microsoft Certificate Services Advanced Certificate Request page. In the Key Options section, select "Microsoft Enhanced Cryptographic Provider v1.0" for CSP, and check the Store certificate in the local computer certificate store checkbox. In the Additional Options section, enter a descriptive Friendly Name for the certificate and enter the following (without the quotes) in the Attributes text box:
	"san:dns= <name1>&dns=<name2>&dns=<name3>"</name3></name2></name1>
	where <name1> is the SIP domain of Microsoft OCS, <name2> is the FQDN of a physical server on which Microsoft OCS is running, and <name3> is the FQDN of the Microsoft OCS enterprise pool. If there are multiple SIP domains supported on Microsoft OCS or if Microsoft OCS runs on multiple physical servers, then append the SIP domains and FQDNs in the manner illustrated above. In the example below,</name3></name2></name1>
	san:dns=sip.sitims.net&dns=msocsent1.sitims.net&dns=Entpool.sitims.net [*] is entered.
	Key Options: Create new key set Use existing key set CSP: [Microsoft Enhanced Cryptographic Provider v1 0] Key Usage: Impact Common key sizes: 1024 2048 4006 8192 16384) Key Size: [1024] Mix: 1024 (common key sizes: 1024 2048 4006 8192 16384) Automatic key container name User specified key container name Mark keys as exportable Store certificate in the local computer store Instead of in the user's certificate store. Does not Instead of in the user's certificate store. Does not Instead of in the user's certificate store. Does not Instead of CA's certificate: You must be an administrator to generate or use a key in the local machine store. Additional Options: Request Format: CMC C PKCS10 Hash Algorithm: SHA1 Only used to sign request. Save request to a file san: cdns=sip.sitlms.net 6dns=mso Attributes: Friendly Name: ServerClientAuthent
	Submit >
7.	In the Microsoft Certificate Services Certificate Issued page, click on "Install this certificate".
	Microsoft Certificate Services SITLCA Home Certificate Issued Install this certificate The certificate you requested was issued to you. Install this certificate

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

20 of 48 OCS-ACM-RCC

Step	Description
8.	Repeat Steps 1 – 7 on each Microsoft OCS server in the enterprise pool.

5.4. Assign Server Certificate to Microsoft OCS Enterprise Pool Server Connections

This section describes the steps for assigning the server certificate installed in Section 5.3 to inbound and outbound connections on a Microsoft OCS enterprise pool server.

Step	Description
1.	On a Microsoft OCS server, launch the Microsoft Office Communications Server 2007 MMC snap-in. In the left pane, expand the Forest node down to the Front Ends level (Forest \rightarrow Enterprise pools \rightarrow <name of="" pool=""> \rightarrow Front Ends), right-click on the FQDN of a physical server on which Microsoft OCS runs, and select "Properties".</name>
	Microsoft Office Communications Server 2007
	Ele Window Help
	Office Communications Server 2007 Forest - sittms.net Image: Propol Image: Propol

Step	Description
2.	In the Properties dialog box, click on "Select Certificate".
	msocsent1 sitims net Pronerties
	Specify the certificate to be used for inbound and outbound
	connections on this server.
	Issued to: Entpool.sitims.net Issued by: SITLCA
	Valid from 8/16/2007 11:45 AM to 8/15/2009 11:45 AM.
	Select Cettificate
	Delete Cerțificate
	Warning: This certificate is used by all Office Communications Server roles running on this computer with the exception of the Web Components
	Server. Unanging the certificate will have no effect on existing connections.
3.	In the Select Certificate dialog box, select the certificate installed in Section 5.3 and click on
	"OK".
	N-4- This new serificate wells as the serificate series of hering Misses & OCS installation
	Note: This new certificate replaces the certificate assigned during Microsoft OCS instantation.
	Select Certificate
	Select the certificate you want to use.
	Issued to Issued by Intended P Friendly name Expiration Entpool SITLCA Server Aut ServerClien 8/30/2009
	Entpool SITLCA Server Aut MSOCSENT1 8/15/2009
	OK Cancel <u>V</u> iew Certificate

Step	Description	
4.	In the Properties dialog box, click on " OK ".	
	msocsent1.sitIms.net Properties Image: Conferencing Certificate General IM Conferencing Telephony Conferencing Certificate Server Certificate Specify the certificate to be used for inbound and outbound Certificate	
	Issued to: Entpool.sitims.net Issued by: SITLCA Valid from 8/31/2007 2:29 PM to 8/30/2009 2:29 PM.	
	Select Certificate Delete Certificate	
	Warning: This certificate is used by all Office Communications Server roles running on this computer with the exception of the Web Components Server. Changing the certificate will have no effect on existing connections.	
	Cancel Apply Help	
5.	Repeat Steps $1 - 4$ on each Microsoft OCS server in the enterprise pool.	

5.5. Install Certificate Chain (Trusted Certificate) on Avaya Application Enablement Services Server

This section describes the steps for installing the Microsoft Enterprise CA certificate chain (trusted certificate) on an Avaya AE Services server.

Step	Description
1.	On a Microsoft OCS server, make a copy of the CA certificate chain file downloaded in Section
	5.1 Steps 1 - 4. Open the copied file with a text editor, and replace "CERTIFICATE" with
	"PKCS7" in both the header and trailer. Copy the entire contents of the modified file into the
	Windows clipboard.
	Windows clipboard.

Step	Description
2.	On the Microsoft OCS server, launch a web browser and log into the Avaya AE Services OAM Web Interface. In the left pane, select CTI OAM Admin \rightarrow Administration \rightarrow Certificate Management \rightarrow Trusted Certificate . In the Trusted Certificates page, click on "Import".
	AVAYA Application En Operations Adm
	CTI OAM Home Vou are here: > Administration > Certificate Management > Trusted Cert • Administration Network Configuration Switch Connections Trusted Certificates • CTI Link Admin View Import Export Delete • DMCC Configuration Alias Status Issued To Issued By Export • Security Database • avayaprca valid Avaya Product Root CA Avaya Product Root CA Sun Au • TR87 Configuration • TR87 Configuration
3.	In the Trusted Certificate Import page, enter a descriptive name for Certificate Alias , and paste the copied contents from Step 1 into the Certificate PEM textbox. Click on " Apply ".
	CTI OAM Home You are here: > Administration_ > Certificate Management > Trusted Certificate Alangement > Trusted Certificate Import • Network Configuration Switch Connections • CII Link Admin OMCC Configuration • DMCC Configuration Eacurity Database • Certificate Management • Server Certificate • Server Certificate Certificate Management • Server Certificate Trusted Certificate TRS7 Configuration Status and Control • Maintenance Alarms • Logs Utilities • Help Close
	If the import is successful, the message "Certificate imported successfully" is displayed on the Trusted Certificate Import page.

5.6. Request and Install Server Certificate on Avaya Application Enablement Services Server

This section describes the steps for requesting the server certificate (based on the certificate template created in Section 5.2) from the Microsoft Enterprise CA and installing the server certificate on an Avaya AE Services server

Step		Description
1.	On the Microsoft OCS server Web Interface. In the left par Management → Server Cer	a, launch a web browser and log into the Avaya AE Services OAM ne, select CTI OAM Admin → Administration → Certificate tificate . In the Server Certificates page, click on "Add". Application En Operations Adm
	CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database Certificate Management Server Certificate Pending Requests Default Settings Trusted Certificate FR87 Configuration	You are here: > Administration > Certificate Management > Server Cert Server Certificates View Add Import Export Delete Alias Status Issued To Issued By Expiration Date

Step		Description				
2.	In the Add Server Certificate page, configure the following and click on "Apply".					
	• Certificate Alias – enter a descriptive name.					
	• Password and Re-enter Password – enter an arbitrary password.					
	• Distinguished Name – er	nter "CN= <fodn ae="" avava="" of="" services<="" th=""></fodn>				
	server> OU= <departmen< th=""><th>t > O = < Country/Region > "</th></departmen<>	t > O = < Country/Region > "				
	Use the same Department	Company City State and Country/Region values entered in				
	Section 5.3 Step 5 In the	example below				
	"CN-msayaes1 sitlms net	t OU-SITE O-Avava I – I incroft S-New Jersey C-US" is entered				
	Challenge Dessword and	Be onter Challenge Dessword anter an arbitrary password				
	• Chancinge I assword and	he defaults				
	• Leave the other fields at t	ne defaults.				
		Application En				
	AVAYA	Operations Adn				
	CTI OAM Home	You are here: > <u>Administration</u> > <u>Certificate Management</u> > <u>Server Cert</u>				
	<u>Network Configuration</u>	Add Server Certificate				
	Switch Connections					
	<u>CTI Link Admin</u> <u>DMCC Configuration</u>	Certificate Alias aeservercert				
	TSAPI Configuration	Create Self-Signed Certificate				
	Security Database Enrollment Method Manual					
	<u>Certificate Management</u>	Certificate Key Parameters:				
	Server Certificate Dending Requests	Encryption Algorithm 3DES 🗸				
	Default Settings	Password				
	Trusted Certificate	Re-enter Password				
	TR87 Configuration Status and Control	Key Size				
	Maintenance	Certificate Request Parameters:				
	<u>Alarms</u>	Cortificato Validity (Days) 1825				
	Logs	Distinguished Name				
	Help					
		Challenge Password				
		Re-enter Challenge Password				
		Apply				



Step	Description							
6.	In the Submit a Certificate Request or Renewal Request page, paste the copied contents from							
	step 3 into the Saved Kequest textbox, select the Certificate Template created in Section 5.2, and click on " Submit ".							
	Microsoft Certificate Services SITLCA Home							
	Submit a Certificate Request or Renewal Request							
	To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.							
	Saved Request:							
	glnpH0LrSN60sgYtN+/B2/+211CV4rECAwEAAaAb Base-64-encoded bnR1cm9wMTIzMA0GCSqGSIb3DQEBBAUAA4GBABFe TOc0vhxmbdq11A/9dNEYW1jpLcYCOX3Npe5Z0PMV (CMC or K0cmB6tXbrsecw8+VabgT3vimkr8AgpcDj/uVxWu PKCS #10 or PKCS #7): END CERTIFICATE REQUEST Image: State of the st							
	Certificate Template:							
	Web Server plus Client Authentication 💌							
	Additional Attributes:							
	Attributes:							
	Submit >							
7.	In the Certificate Issued page, select "Base 64 encoded" and click on "Download certificate".							
	Microsoft Certificate Services SITLCA Home							
	Certificate Issued							
	C DER encoded or © Base 64 encoded Download certificate Download certificate chain							
0	When anomated source the contificate file to a local dimension on the Microsoft OCS common. After							
δ.	saving, open the certificate file with a text editor and copy the entire contents of the certificate file including the header and trailer into the Windows clipboard							
	The, menualing the neader and traner, into the windows enpotate.							





6. Avaya Application Enablement Services TR/87 Configuration

This section describes the Active Directory and Dial Plan configuration on Avaya AE Services for TR/87 integration with Microsoft OCS.

Step		Description			
1.	Launch a web browser and log into the Avaya AE Services OAM Web Interface. In the left pane, select CTI OAM Admin \rightarrow Administration \rightarrow TR87 Configuration \rightarrow Active Directory. In the Active Directory Configuration page, configure the following and click on				
	 Apply Changes . User DN for Query Authentication – enter the Distinguished Name (DN) of an Active Directory user object that has sufficient privileges for accessing Active Directory. In the example below, the DN of the domain administrator is entered: "CN=Administrator,CN=Users,DC=sitIms,DC=net" Password and Confirm Password – enter the Active Directory password for the user. Base Search DN – enter a DN that includes all Active Directory users (particularly those that are also configured as Microsoft OCS users). IP Address – enter the IP address of the Active Directory server. 				
	AVAYA		Application En Operations Adm		
	CTI OAM Home	You are here: > <u>Administration</u>	> <u>TR87 Configuration</u> > <u>Active Directory</u>		
	 Administration <u>Network Configuration</u> <u>Switch Connections</u> <u>CTI Link Admin</u> <u>DMCC Configuration</u> <u>TSAPI Configuration</u> <u>Security Database</u> <u>Certificate Management</u> <u>TR87 Configuration</u> <u>Active Directory</u> 	Active Directory Config User DN for Query Authentication Password : Confirm Password : Base Search DN : IP Address : Dort :	uration : CN=Administrator,CN=Users,DC=sit ••••••• ••••••• CN=Users,DC=sitIms,DC=net 135.8.19.100 389		
	<u>Dial Plan</u> <u>Status and Control</u>	Apply Changes Cancel	305		

Step		Description
2.	In the left pane, select Dial P Administration page, select Communication Manager, an	Ian → Switch Administration. In the Switch Dial Plan the switch connection corresponding to the appropriate Avaya d click on "Detail". Application En Operations Adm
	CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database Certificate Management Certificate Management TR87 Configuration Active Directory Dial Plan Switch Administration Default Cottings	You are here: > Administration > TR87 Configuration > Dial Plan > Sw Switch Dial Plan Administration Administered Switches Image: msavcm1 Detail Apply Defaults Use as Default

Step		Description				
3.	In the Dial Plan Settings – C	Conversion Rules page, click on "Add" in the From TelURI				
	 section. Avaya AE Services uses the From TelURI table to convert E.164-formatted number TR/87 requests received from Microsoft OCS into extensions and number strings that Avaya Communication Manager can handle and route. For example, when an RCC client places a car on behalf of an Avaya Communication Manager phone, Microsoft OCS sends a call initiation request to Avaya AE Services. The calling number (device identifier) in the request is the number assigned to the RCC user in Microsoft OCS (see Section 7 Step 3) and may be in E.16 format. An appropriate entry in the From TelURI table would then be required to extract the extension of the associated Avaya Communication Manager phone from the E.164-formatted number. In the sample configuration, Microsoft OCS users were all assigned E.164 11-digit numbers. If the called number in the request is also an E.164-formatted number (which commonly occur when the RCC client places a call using the MOC Contacts list), an appropriate entry in the From TelURI table, however, does not convert numbers that are not E.164-formatted, so Avaya AE Services passes such numbers without modification to Avaya Communication Manager. Therefore, RCC clients can also dial any extension or number string that Avaya Communication Manager. 					
	Αναγα	Operations Adn				
	CTI OAM Home	You are here: > <u>Administration</u> > <u>TR87 Configuration</u> > <u>Dial Plan</u> > <u>Sv</u>				
	 Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database Certificate Management TR87 Configuration Active Directory Dial Plan Switch Administration Default Settings Status and Control Maintenance Alarms Logs Utilities Help 	Dial Plan Settings - Conversion Rules for msavcm1 From TelURI Minimum Length Maximum Length Pattern Minimum Delete Length Replacer				

Step	Description				
4.	In the Add Dial Plan From TelURI page, configure an entry that converts the E.164-formatted numbers assigned to the RCC clients (see Section 7 Step 3) to the corresponding Avaya Communication Manager phone extensions (see Section 4.1), and click on " Apply Changes ". This entry applies to the calling number when a RCC client sends a call initiation request to Avaya AE Services, and allows Avaya Communication Manager to identify the phone for which the RCC client is placing the call. In the example below, the entry matches E.164 11-digit numbers that start with "+17328823" and deletes the leading six digits to obtain extensions of the form 23xxx.				
	Note : This entry also applies to the called number if the called number is the E.164-formatted number assigned to another RCC client.				
	CTI OAM Home You are here: > Administration > TR87 Configuration > Dial Plan > SW • Administration Network Configuration Switch Connections CTI Link Admin • DMCC Configuration Security Database • Certificate Management Minimum Length: • TR87 Configuration Attive Directory • Dial Plan Switch Administration Switch Administration Delete Length: • Delat Settings Cancel Changes				
5.	In the Add Dial Plan page, click on "Apply". Application En Operations Add Operations Add Operations CTI OAM Home Administration Vou are here: > Administration > TR87 Configuration > Dial Plan > Sv Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Warning! Are you sure you want to add this Dial Plan? Add Dial Plan Add D				
6.	Repeat Steps 3 – 5 as necessary for each range of E.164-formatted numbers assigned to RCC clients.				

Step		Description				
7.	numbers assigned to the EV clients (refer to [1] and Section 4.1). This entry applies to the called number when a RCC client sends a call initiation request to Avaya AE Services, where the called number is the E.164-formatted number assigned to an EV client. The extracted "extensions" can then be used by Avaya Communication Manager to route the calls to Microsoft OCS according to the routing configuration described in [1]. In the example below, the entry matches E.164 11- digit numbers that start with "+1732883" and deletes the leading six digits to obtain extensions of the form 3xxxx. The routing configuration described in [1] routes calls placed to 3xxxx to Microsoft OCS. Note that Avaya Communication Manager applies the same routing configuration when RCC clients use extension dialing, i.e., dialing 3xxxx, to call EV clients. Repeat this step as necessary for each range of E.164-formatted numbers assigned to EV clients.					
	CTI OAM Home Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database Certificate Management TR87 Configuration Active Directory Dial Plan Switch Administration Default Settings	You are here: > Administration > TR87 Control Add Dial Plan - msavcm1	Infiguration > Dial Plan > Sw 11 11 11 11 11 11 11 1732883 Note: or 6 1			

Step		Description				
8.	Repeat Steps 3 – 5 to configure an entry that extracts the extensions from E.164-formatted numbers corresponding to Avaya Communication Manager phones that are not associated with RCC clients. This entry applies to the called number when a RCC client sends a call initiation request to Avaya AE Services, where the called number is an E.164-formatted number containing the extension of an Avaya Communication Manager phone that is not associated with an RCC client. In the example below, the entry matches E.164 11-digit numbers that start with "+17328822" and deletes the leading six digits to obtain extensions of the form 22xxx. Repeat this step as necessary for each range of E.164-formatted numbers corresponding to Avaya Communication Manager phones that are not associated with RCC clients.					
	CTI OAM Home • Administration • Network Configuration Switch Connections • CTI Link Admin • DMCC Configuration TSAPI Configuration TSAPI Configuration • Security Database • Certificate Management • TR87 Configuration Active Directory • Dial Plan Switch Administration Default Settings	You are here: > Administration > TR87 Co Add Dial Plan - msavcm1 From TelURI Minimum Length: Maximum Length: Matching Pattern: tel:+ Delete Length: Replacement String: Apply Changes	Application En Operations Add nfiguration > Dial Plan > Sv			



Step	Description						
10.	In the Dial Plan Settings – Conversion Rules page, click on "Add" in the To TelURI section.						
	Avaya AE Services uses the To TelURI table to convert extensions and number strings received						
	from Avaya Communication Manager into formatted numbers that Microsoft OCS recognizes.						
	For example, when an RCC-associated Avaya Communication Manager phone places or receives						
	a call, Avaya Communication Manager sends a call notification to Avaya AE Services, where the						
	calling and called numbers may be extensions or any number strings. An appropriate entry in the						
	To TelURI table can convert the numbers into E.164-formatted numbers or any other formatted						
	numbers that Microsoft OCS recognizes. In the sample configuration, Microsoft OCS users						
	were all assigned E.164 11-digit numbers. If the reformatted calling/called number is that of						
	another Microsoft OCS user (whether configured for RCC or EV mode), then the RCC client can						
	also resolve the number to the calling user's name.						
	No avaligit To TallIDI table entry is passed on the calls where the calling/called number is the						
	averagion of an BCC associated Avera Communication Manager phone. This is because the						
	extension of an RCC-associated Avaya Communication Manager phone. This is because the manning between the extension and essectieted Microsoft QCS number is already known from an						
	mapping between the extension and associated wheresoft OCS number is already known from an appropriate entry in the From TalLIPI table (see Stops $4-6$)						
	appropriate entry in the From FeroKi table (see Steps 4 - 0).						
	To TelURI						
	Minimum Length Maximum Length Pattern Match Delete Length Replacer						
	Add Edit Delete Reorder						



³ The original calling party number sent by Microsoft OCS for such a call may be in fact an E.164-formatted number, but the leading "+" is removed by Avaya Communication Manager.

7. Configure Microsoft Office Communications Server

This section highlights the Microsoft Office Communications Server (OCS) configuration for TR/87 integration with Avaya AE Services. These Application Notes assume that basic Microsoft OCS server installation and configuration have already been performed according to the guidelines provided in [6], [7], and [8]. These Application Notes further assume that user accounts have been created in Microsoft Active Directory and enabled for Microsoft OCS.

Step			Descripti	on			
1.	On the Microsoft OCS server, launch the Microsoft Office Communications Server 2007 (MMC) snap-in. In the left pane, expand the Forest node down to the Users level (Forest \rightarrow Enterprise pools \rightarrow <name of="" pool=""> \rightarrow Users). In the right pane, right-click on a user and</name>						
	select " Properties ".	Server 2007					
	Office Communications Server 2007 Forest - sitins.net Front Ends Front Ends Front Front Ends Front Front Ends Front Ends	Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled	Display name Bryan Katz Chuck Bertsch David Boyer Dilbert Engineer Homer Simpson Michael Scott MSLZDA1 MSLZDP1 Peter Griffin	SIP URI sip:bkatz@si sip:chuck@s sip:djboyert sip:dilbert@: sip:homer@: coldia@idlf Gonfigure users Delete users Move users Properties Help	itlms.net itlms.net gsitlms.net sitlms.net s.net ms.net MSLZDP1.sitlms.net itlms.net@sitlms.net ns.net	Type User User User User User User AutoAttendant AutoAttendant User	
	Opens the properties dialog box for the cu	rrent selection.					

Step	Description
2.	In the selected user's Properties dialog box, click on "Configure".
	User Lois Griffin Properties X Communications Y Enable user for Office Communications Server Sign-in name: sip.lois @ sitims.net Server or pool: Y Entpool.sitims.net Y Malow anonymous participants Y Policy: Default Policy Y Default Policy Y Vew Note: Meeting settings cannot be changed unless the global setting allows per user configuration. Additional options: Configure OK Cancel Apply

Step	Description
3.	In the User Options dialog box, in the Telephony section, select "Enable Remote call control", enter "sip:aes@ <fqdn ae="" of="" server="" services="">" for Server URI, and enter an E.164 Tel URI for Line URI. The trailing five digits of the E.164 Tel URI should contain the user's Avaya Communication Manager phone extension (see Section 4.1). In the sample configuration, users were configured with Line URIs of the form "Tel:+17328823xxx", where 23xxx is the user's Avaya Communication Manager phone extension and +17328823xxx is the corresponding E.164 11-digit number. Click on "OK".</fqdn>
	User Options X
	Telephony Select a telephony option. These settings affect only those calls that are routed through IP-PSTN or remote call control gateways.
	C Enable PC-to-PC communication only
	Enable <u>R</u> emote call control
	C Enable Enterprise Voice
	I Enable PB∑ Integration Note: To enable both remote call control and PBX integration, you must specify a Server URI below.
	Policy: Default Policy View
	Server URI: sip:aes@msavaes1.sitIms.net
	Line URI: tel:+17328823001
	Federation □ Enable federation □ Enable remote user access □ Enable public IM connectivity
	Archiving
	Archive internal IM conversations
	Note: Archiving settings cannot be changed unless the global setting allows per user configuration.
	Enable enhanced presence Note: Enhanced presence cannot be changed once it has been set.
	Cancel Help
4.	Back in the selected user's Properties dialog box, click on " OK ".
5.	Repeat Steps $1 - 4$ for other users with RCC clients.
~•	

Step	Description
6.	In the left pane of the Microsoft Office Communications Server 2007 MMC snap-in, expand
	the Forest node down to the Enterprise Pool level (Forest \rightarrow Enterprise pools \rightarrow <name of<="" th=""></name>
	Pool>), right-click on Front Ends , and select " Properties ".
	Microsoft Office Communications Server 2007
	Eile Window Help
	Office Communications Server 2007
	□···▲> Forest - sitlms.net □···□■ Enterprise pools
	Front Ends
	⊕-
	er in assigned users er in and the servers <u>Help</u>
7	In the Front Ends Properties dialog box select the Routing tab and click on " Add "
	in the Front Ends Froperites during took, select the Routing too and enex on Fruu .
	Front Ends Properties
	Federation Host Authorization Archiving Voice
	Routing
	Specify static routes for outbound connections.
	Matching URI Next Hop Port Transport
	Authorization tab.

Step	Description
8.	In the Add Static Route dialog box, in the Matching URI section, enter the FQDN of the
	Avaya AE Services server for Domain . In the Next hop section, enter the FQDN of the Avaya
	AE Services server for FQDN, select "TLS" for Transport, and enter the Avaya AE Services
	TR/87 Port (see Section 4.3) for Port. Click on "OK".
	Add Charlie Davids
	Matching URI
	Domain: msavaes1.sitlms.net
	E Phone URI
	C Next hop
	FODN msavaes1.sitIms.net
	Iransport:
	P <u>o</u> rt: 4723
	☐ <u>R</u> eplace host in request URI
	Cancel Help
9.	In the Front Ends Properties dialog box, select the Host Authorization tab and click on " Add ".
	Front Ends Properties
	General Routing Compression Authentication Federation Host Authorization Archiving Voice
	Specify authorized hosts such as gateways, application servers, special clients that need additional bandwidth and so forth.
	Servers Outbound Only Throttle As Se Treat As A
	Add Edit <u>R</u> emove
	OK Cancel Apply Help

Step	Description
10.	In the Add Authorized Host dialog box, in the Server section, select "FQDN" and enter the
	FQDN of the Avaya AE Services server. In the Settings section, ensure that the Outbound
	Only checkbox is unchecked, and check the Throttle As Server and Treat As Authenticated
	checkboxes. Click on " OK ".
	Add Authorized Host
	Server
	• EQDN:
	C IP address:
	✓ Treat As Authenticated
	Cancel Help
11.	In the Front Ends Properties dialog box, click on " OK ".
	Front Ends Properties
	General Routing Compression Authentication
	Federation Host Authorization Archiving Voice
	Specify authorized hosts such as gateways, application servers, special clients that need additional bandwidth and so forth
	Servers Outbound Only Throttle As Se Treat As A
	Imsavaes1.sitIms.net No Yes Yes
	Add <u>E</u> dit <u>B</u> emove
	UK Cancel Apply Help

8. Verification Steps

The following steps may be used to verify the configuration:

- Place outbound calls from a RCC client to Avaya phones (associated and not associated with RCC clients), EV clients, and Microsoft Exchange voicemail access and Auto Attendant using extension dialing. Verify that the calls are established successfully on the associated RCC Avaya phones.
- Place outbound calls from a RCC client to Avaya phones (associated and not associated with RCC clients), EV clients, and Microsoft Exchange voicemail access and Auto Attendant using the MOC Contacts list. Verify that the calls are established successfully on the associated RCC Avaya phones.
- Establish a call between two RCC-associated Avaya phones. Verify that both users' names are displayed on the RCC clients.
- Establish a call from an Avaya phone to an RCC-associated Avaya phone. Verify that the calling extension is displayed on the RCC client.
- Establish a call from an EV client to an RCC-associated Avaya phone. Verify that the name of the calling user is displayed on the RCC client.
- Establish outbound calls from an RCC-associated Avaya phone. Verify that the calls are accurately reflected on the RCC client.
- Place inbound calls to an RCC-associated Avaya phone. Verify that the calls can be answered at the RCC client and the phone.
- Establish multiple inbound and outbound calls on an RCC-associated Avaya phone. Verify that the RCC client displays a conversation window for each call and the user can move easily between the conversation windows.
- Verify that call hold, retrieve, disconnect, and transfer operations performed from a RCC client are accurately reflected on the Avaya phone associated with the RCC client.
- Verify that call hold, retrieve, disconnect, and transfer operations performed from an RCC-associated Avaya phone are accurately reflected on the RCC client.
- Establish multiple inbound and outbound calls on an RCC-associated Avaya phone. Verify that the RCC client displays a conversation window for each call and the user can move easily between the conversation windows.
- Establish an IM conversation between two RCC clients and escalate the conversation to a voice call. Verify that the call is established successfully on the associated RCC phones.
- Configure an RCC client to forward calls to another destination (Avaya phones associated and not associated with RCC clients, and EV clients). Place inbound calls to the Avaya phone associated with the forwarding RCC client. Verify that the calls are forwarded to the correct destinations.
- Verify that the presence status of the RCC client correctly reflects the telephony status (in a call or idle) of the associated Avaya phone.

9. Conclusion

These Application Notes described the configuration procedures for enabling Microsoft Office Communicator (MOC) clients to place, answer, hold/retrieve, transfer, and disconnect calls on Avaya Communication Manager phones. The integration between MOC clients and Avaya Communication Manager phones was achieved through TR/87 integration between Avaya Application Enablement Services and Microsoft OCS.

The following was observed from sanity testing of basic telephony functionality: On a call between two RCC-associated Avaya phones, when the call is transferred to an EV client, the transfer succeeds, but the call is dropped on the RCC client associated with the transferred Avaya phone (the call is still up between the transferred phone and EV client).

10. Additional References

[1] "Application Notes for Call Routing Between Avaya Communication Manager and Microsoft Office Communications Server", Issue 1.0, September 2007

The following document may be obtained from http://support.avaya.com.

[2] "Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide Release 4.0.1", Issue 7, July 2007, Document Number 02-300357.
[3] "Avaya MultiVantage Application Enablement Services Implementation Guide for Microsoft Live Communications Server", Issue 3, July 2007, Document Number 02-601893.

The following documents may be obtained from <u>http://www.microsoft.com</u>.

- [4] "Microsoft Office Communications Server 2007 Technical Overview", July 2007.
- [5] "Microsoft Office Communications Server 2007 Planning Guide", July 2007.
- [6] "Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide", July 2007.
- [7] "Microsoft Office Communications Server 2007 Enterprise Voice Planning and Deployment Guide", July 2007.
- [8] "Microsoft Office Communications Server 2007 Administration Guide", July 2007.
- [9] "Integrating Telephony with Office Communications Server 2007", July 2007.

© 2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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