Module 9: Implementing Public Cloud Instant Messaging with Live Communications Server 2005 with SP1

Contents

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Overview

- Introducing Public Instant Messaging Connectivity
- Identifying Public Instant Messaging Connectivity Deployment Considerations
- Configuring Access Proxy server settings for Public Instant Messaging Connectivity

Introduction

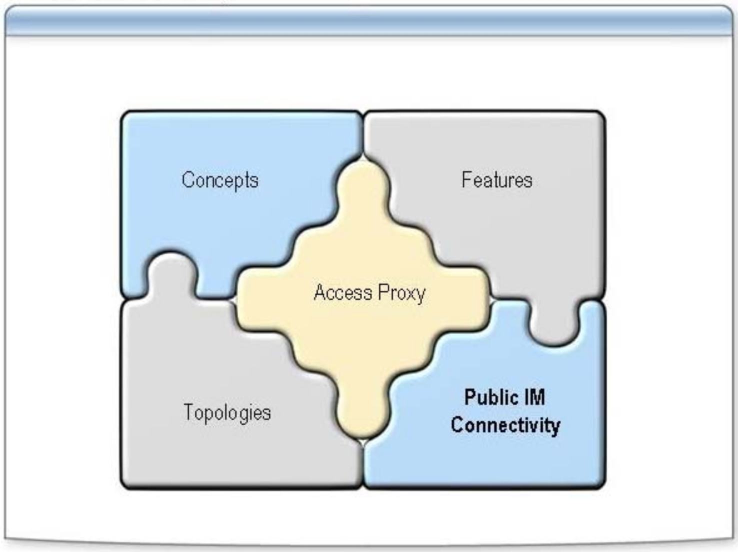
After deploying Microsoft® Live Communications Server 2005 with Service Pack 1 (LCS 2005 with SP1) Standard or Enterprise Edition, you may want to extend your organization's reach by providing secure external connections to your business partners and vendors who have accounts with public instant messaging (IM) service providers.

Objectives

After completing this module, you will be able to:

- Describe concepts, features, and topologies of an Access Proxy server with Public Instant Messaging Connectivity (PIC).
- List the requirements and recommendations for an Access Proxy server with PIC deployment.
- Configure Access Proxy server settings for PIC.

Lesson: Introducing Public Instant Messaging Connectivity



Introduction

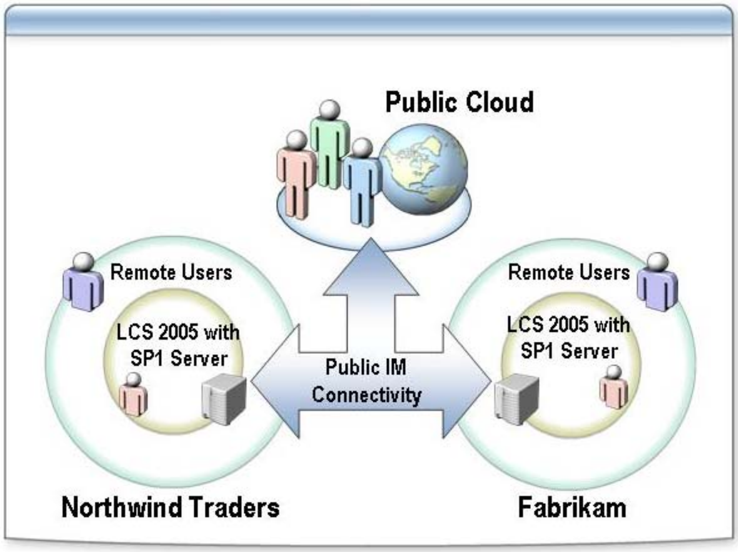
Live Communications Server 2005 with SP1 provides the means for establishing IM connectivity with users of public IM services provided by MSN®, AOL, Yahoo!, and other public service providers. After a connection is established, authorized internal Live Communications Server users can add contacts, share presence information, and communicate in real-time with users of these public IM network services.

Lesson objectives

After completing this lesson, you will be able to:

- Explain the purpose of Public Instant Messaging Connectivity (PIC).
- Describe the features of PIC.
- List public IM service providers.
- Explain the methodology of PIC.

What Is Public Instant Messaging Connectivity?



Introduction

LCS 2005 with SP1 extends the Federation capability of Live Communications Server 2005 by providing the means for communicating with users of instant messaging services provided by MSN, Yahoo!, and AOL. An Access Proxy server role is a prerequisite if you want to enable external communications for your LCS 2005 with SP1 deployment.

Public IM Connectivity

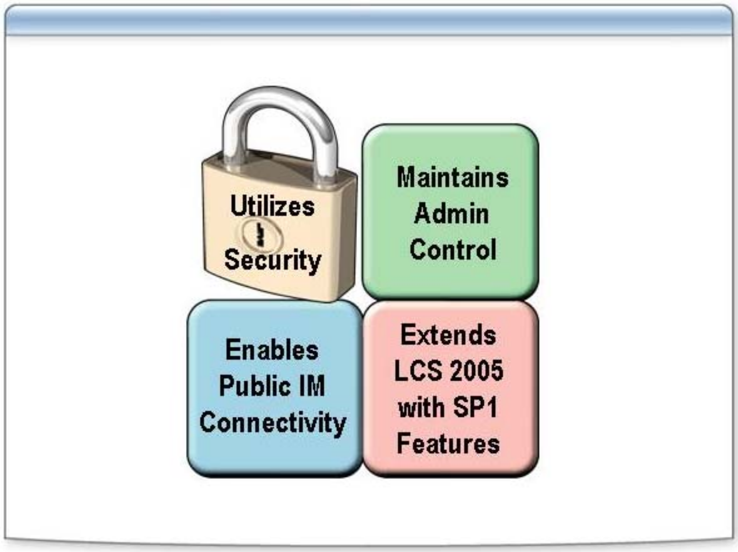
You can set up Public IM Connectivity to connect your internal and remote users to business partners who use public IM service providers.

In addition, users in your organization can employ either Microsoft Office Communicator 2005 or Microsoft Windows® Messenger 5.1 or later to communicate with all their contacts, whether those contacts are internal colleagues, employees of federated partners, or users of public IM services.

PIC Scenarios

A technical recruiting company could enable the Public IM Connectivity on their Access Proxy server. After Public IM Connectivity is configured and their internal users are enabled for Public IM Connectivity, employees can work with contracted recruiters who work in different geographical areas and utilize AOL, Yahoo!, or MSN instant messaging accounts.

Features of Public IM Connectivity


Utilizes Security
Maintains Admin Control
Enables Public IM Connectivity
Extends LCS 2005 with SP1 Features

Introduction

In the information worker age, individuals can work from home, office, car, and plane. Access to up-to-date information is critical. LCS 2005 with SP1 provides encrypted communications with external users and organizations. The LCS 2005 with SP1 Access Proxy server with Public IM Connectivity enabled provides additional security and creates a single connection point between your organization and its affiliates.

Administrative Control

Administrators have full control over who in their organization is authorized for Public IM Connectivity. Once that permission is granted, however, a user can communicate with all of the public IM service providers enabled for the organization. You cannot authorize a user to communicate over one enabled public IM service provider but not over another one.

You can choose which public IM service providers will be enabled in your LCS 2005 with SP1 deployment. You can choose to enable Yahoo! but not enable Public IM Connectivity with AOL.

Administrators can authorize Public IM Connectivity for one or more users and change these authorizations as needed. Additional licensing is required for Public IM Connectivity.

Security

As with other types of Federation, all IM traffic between an organization and a public IM service provider uses an encrypted Mutual Transport Layer Security (MTLS) connection. To connect to MSN, AOL, and Yahoo!, an organization must use a certificate from a public certification authority (CA) from the default list of trusted certificate authorities in Windows Server® 2003.

Features

After a connection is established, users who are authorized for Public IM Connectivity can carry out the following actions:

- Add contacts to their contact list
- Share their presence information
- Communicate in real time with public IM users

Note Features that require multimedia, conferencing, and games will not be enabled between LCS 2005 with SP1 and public IM service providers.

Access Proxy

The key component in public IM connectivity is the Access Proxy. The Access Proxy acts as a gateway between your organization and the public IM provider. A single Access Proxy server can provide multiple connections to remote users, subsidiaries, as well as to outside vendors. An Access Proxy server can also support the following connectivity options:

- Federation (Enhanced and Direct)
- Remote Users

Archiving

The Archiving service supports public IM connectivity to provide the following capabilities:

- Archive all the instant messaging conversations for all or for specific users
- Archive usage data on all or on specific users

For more information about the archiving service, see “Module 12: Archiving Messages with Live Communications Server 2005 SP1.”

SPIM Control

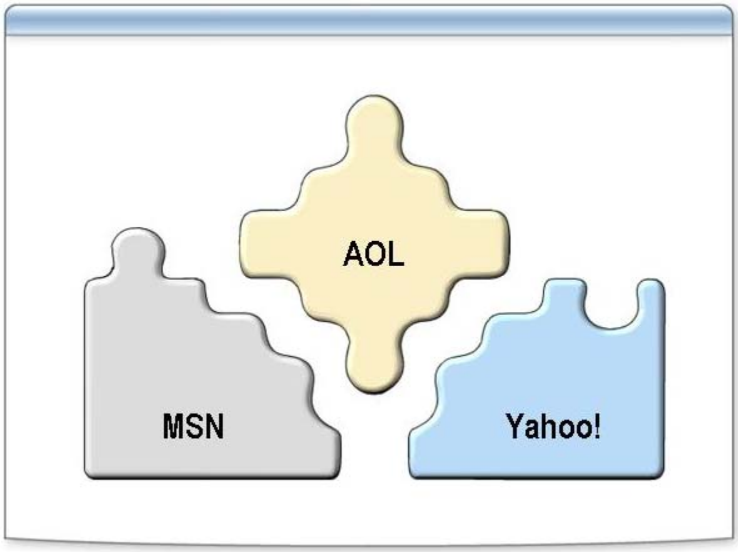
With public IM connectivity, there is a greater possibility that users may receive spam on instant messaging messages. You can control spam over instant messaging (SPIM) by filtering SPIM based on defined rules in a LCS 2005 with SP1 deployment.

The Access Proxy server reviews the message filter settings and then accepts or rejects the incoming messages based on user verification of the sender.

Message Filtering

With Public IM Connectivity, there is also a greater risk of users receiving malicious URLs. LCS 2005 with SP1 includes an application, IMFilter.am, that provides a way to block potentially malicious URLs. IMFilter.am also blocks messages that attempt to initiate a file transfer.

Public Instant Messaging Providers



Introduction

Users inside typical corporations may be able to carry out instant message conversations with customers and partners using one of the three main public IM clients: MSN Messenger, AOL Instant Messenger, and Yahoo! Messenger. However, organizations may want to restrict these communications, for security and compliance reasons.

Public IM Client Issues

Public IM clients do not offer the encryption of data, or the ability for your administrators to log and archive the transactions, which is often required to meet record retention or disclosure requirements. Public IM clients usually do not meet most corporate security standards and often require corporate users to run multiple clients simultaneously to enable connections with multiple public IM service providers. This makes the management of desktop software difficult and decreases productivity by the individual user.

Your company might have chosen to disable public IM connectivity either at the network edge or by locking the desktop software. Completing these tasks would have helped you to increase corporate security or to help reduce the number of employees that use public IM services for personal use.

Encryption and Logging

Live Communications Server 2005 Public IM Connectivity allows corporate users of Live Communications Server to connect with customers and partners utilizing MSN, AOL, and Yahoo! IM services. Unlike with public IM clients, this connection is encrypted and enables logging of IM sessions between users of those services and Live Communications Server internal users.

Office Communicator 2005

Using the new Microsoft Office Communicator 2005 client, Live Communications Server-enabled users will have a single client experience for adding contacts, sending IM, and sharing presence information with users on MSN, AOL, and Yahoo! networks.

With tools delivered in Live Communications Server 2005 with SP1, you can authorize Public IM Connectivity on a per-user basis. These tools allow you to enable Public IM Connectivity for those corporate users that have a legitimate business need to communicate with customers and partners over one of the public IM service provider networks, thus helping to manage the number of employees using public IM services for personal use.

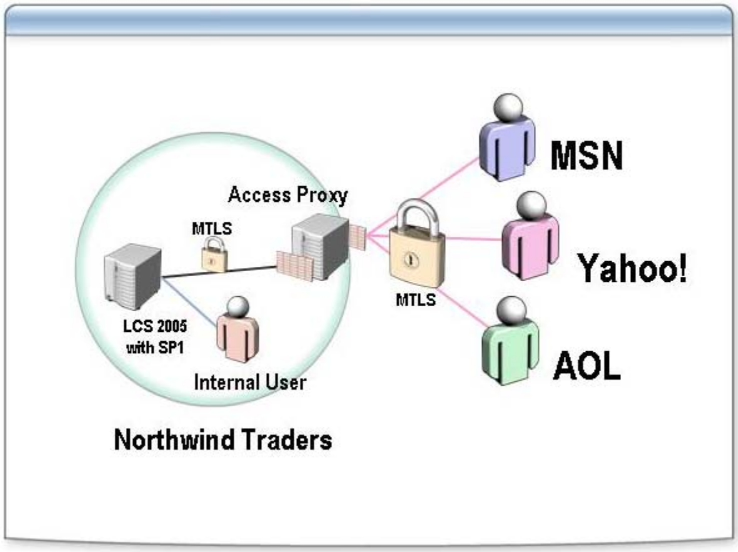
Pricing

Live Communications Server 2005 Public IM Connectivity is offered on a per-user, per-month subscription price. This service is an additional cost to the standard Live Communications Server Client Access License (CAL). The service license price includes access to all three public IM Internet service providers.

Additional Resources

For more information about requesting pricing for Public IM Connectivity, review "How to Buy" on the Microsoft Web site, at: http://www.microsoft.com/office/livecomm/howtobuy/default.mspx.

PIC Methodology



Introduction

Public IM Connectivity licenses cover all three of the supported public IM service providers (MSN, AOL, and Yahoo!). As an administrator, you will be able to retain control over which of the providers you enable for your organization. You can enable one, two, or all three of the public IM service providers if so desired.

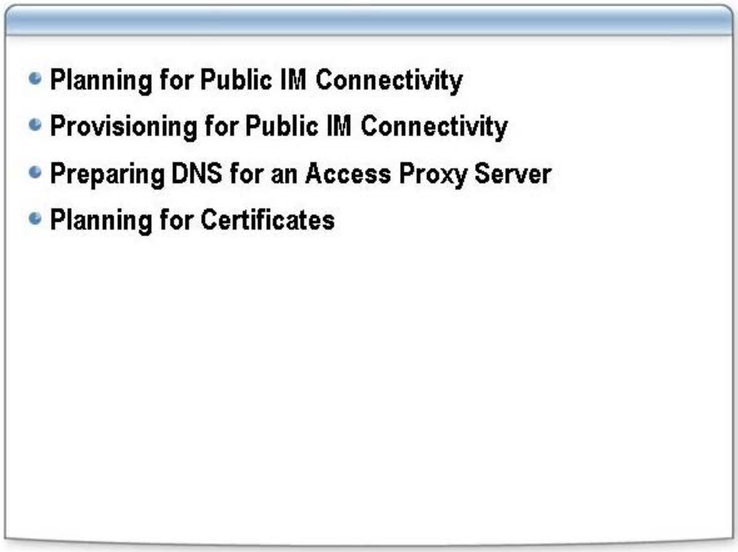
PIC Methodology

After you have enabled Public IM Connectivity on your Access Proxy server, the PIC methodology will establish an encrypted connection if the following requirements are met:

1. Is the domain of the public IM service provider not on the Block list?
2. Can the domain name service (DNS) service record (SRV) entry of the public IM service provider be found, for example, _SIPFederationTLS._TCP.hotmail.com?
3. Does the name of your public IM service providers' Access Proxy server match its domain name?
4. Is the fully qualified domain name of the public IM service providers' Access Proxy server in the list of clouds, for example, Federation.Messenger.MSN.COM?

After the requirements are met, your Access Proxy server establishes a MTLS connection to the remote provider, verifies the certificate, and allows your users to exchange instant messages with other users who have AOL, MSN, or Yahoo! accounts.

Lesson: Identifying Deployment Considerations



- Planning for Public IM Connectivity
- Provisioning for Public IM Connectivity
- Preparing DNS for an Access Proxy Server
- Planning for Certificates

Introduction

An Access Proxy server with Public IM Connectivity implementations requires a dependable underlying network infrastructure. These infrastructure requirements include provisioning, DNS, and certificates.

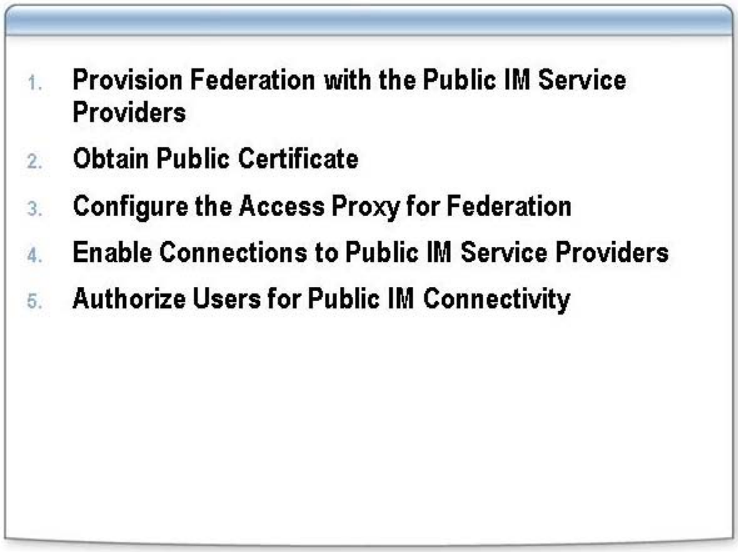
Without these infrastructure requirements, Public IM Connectivity will not function correctly. Hence, it is important for you to review and configure the existing infrastructure before deploying an Access Proxy server with Public IM Connectivity.

Lesson objectives

After completing this lesson, you will be able to:

- Plan for Public IM Connectivity.
- Explain the provisioning process for PIC.
- Configure DNS for a PIC implementation.
- Plan for certificate support

Planning for Public IM Connectivity



1. Provision Federation with the Public IM Service Providers
2. Obtain Public Certificate
3. Configure the Access Proxy for Federation
4. Enable Connections to Public IM Service Providers
5. Authorize Users for Public IM Connectivity

Procedures

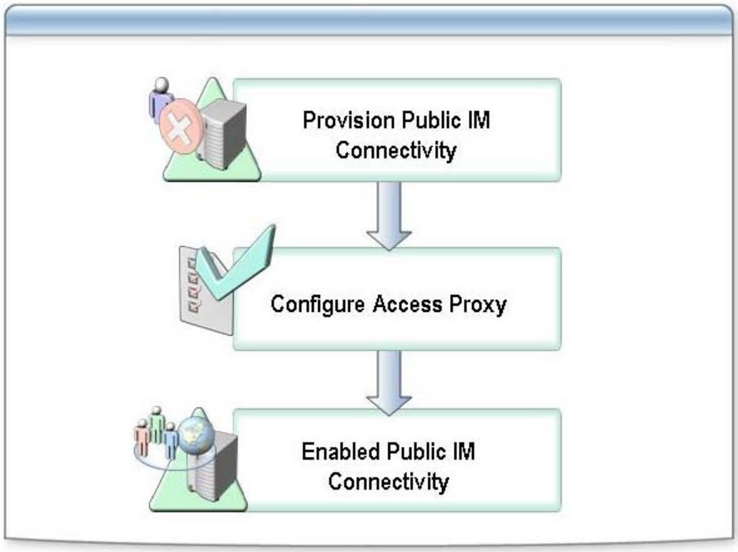
Enabling Federation with the public IM service providers is a four-step process. These steps are explained in detail in later topics in this module:

1. **Provision Federation with the public IM service providers**. Your organization and the public IM service provider must exchange network connectivity information in order to activate Federation. You perform this exchange by connecting to a Microsoft-hosted provisioning site and completing a form that initiates a provisioning request.

Note Before completing the provisioning form and initiating the request to connect with the public IM service providers, you must have first purchased service licenses for Live Communications 2005 Public IM Connectivity and installed Live Communications Server 2005 SP1, pursuant to the terms and conditions of your Microsoft Volume Licensing agreement. If you do not first purchase the necessary licenses, the provisioning process will not be completed

2. **Obtain a public certificate**. Public IM Connectivity requires MTLS, which requires a certificate obtained from a public certification authority. For more information, contact an appropriate public certification authority.
3. **Configure the Access Proxy for Federation**. Public IM connectivity requires that Federation is enabled on the Access Proxy.
4. **Enable connections to public IM service providers**. Each IM service provider with which you want to federate must be enabled and configured on the Access Proxy. The LCS 2005 with SP1 Forest Level must also be configured to enable Federation and Public IM Connectivity.
5. **Authorize users for public IM connectivity**. You can authorize one or more users for public IM connectivity. Users who are not authorized for public IM connectivity can be authorized for other types of Federation and Remote User Access.

Provisioning for Public IM Connectivity


Provision Public IM Connectivity
Configure Access Proxy
Enabled Public IM Connectivity

Introduction

The first step in enabling Public IM Connectivity is to initiate provisioning with one or more of the public IM service providers (MSN, AOL, and Yahoo!). After you purchase separate service licenses for public IM connectivity, you complete a Web form for initiating provisioning requests.

Provisioning

When you initiate provisioning, you will need:

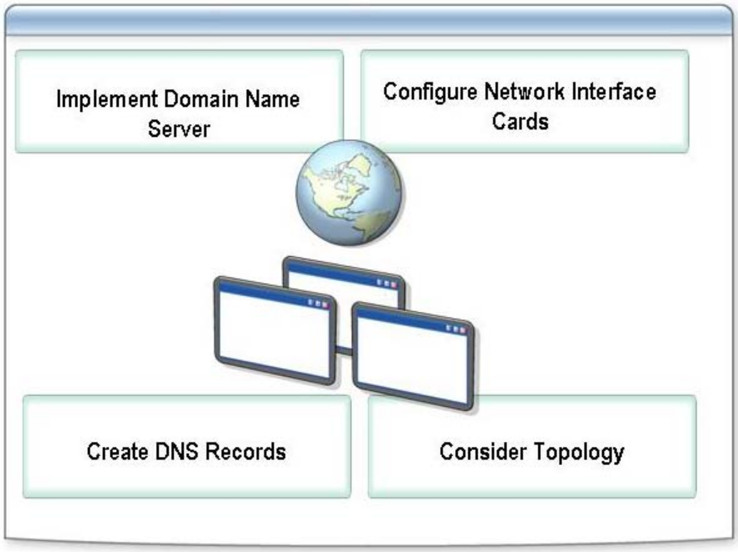
- Your master agreement number.
- Your Microsoft Business Agreement, which establishes the general terms and conditions of its relationship with Microsoft. Contact your software benefits administrator for this information.
- Your Enrollment Agreement Number.
- Your company's purchase of licenses for public IM connectivity. Contact your software benefits administrator for this information.
- The names of your organization's SIP domains.
- The FQDN of your organization's Access Proxy.
- Your network administrator's contact information.
- Names of the public IM service providers with which you wish to federate.

A representative at Microsoft will send you an e-mail message confirming that your provisioning information has been received and your request is in the process of being validated. Upon validation, you will receive a second e-mail message verifying that your information has been forwarded to the appropriate public IM service providers and providing an estimate of how long the process is likely to take. If the request is not validated, you will receive an e-mail message explaining how to resolve the issues responsible for the denial.

After your Access Proxy and SIP domains have been validated, the information will be forwarded to the public IM service providers with which you wish to connect. The Public IM service providers will then provision their routing tables to direct instant messages targeting your SIP domains to the Access

Proxy specified in the form. Once provisioning is complete, each public IM service provider informs Microsoft, and you will receive a final e-mail message confirming that the process is complete. After you have received this final message, you can establish a connection from your Access Proxy to the public IM service providers to which you wish to connect.

Preparing DNS for an Access Proxy Server


Implement Domain Name Server
Configure Network Interface Cards
Create DNS Records
Consider Topology

Introduction

An Access Proxy configured for Federation and with Public IM Connectivity enabled relies extensively on DNS, so a functioning DNS environment is essential for Public IM Connectivity. Specifically, there must be certain DNS records present — DNS Address (A) records that map a host name to an IP address, and Service (SRV) records that advertise the availability of a particular service.

To use DNS, you must configure your Access Proxy server with the IP address of one or more a DNS servers. You also configure DNS on each Access Proxy server differently based on the topology you require. The DNS settings are also different when setting up a Public Edge and a Private Edge.

Creating DNS Records

Regardless of the topology you choose, you must create:

- On your internal DNS server, an Address (A) record that maps to the IP address of the Access Proxy server's Private Edge.
- On your external DNS server, an Address (A) record that maps to the IP address of the Access Proxy server's Public Edge.

You should also perform the following steps if you plan to enable Enhanced Federation:

- Create a DNS SRV record of**_sipfederationtls._tcp.<domain>**
- Point the **_sipfederationtls._tcp.<domain>** record to the A record of the Access Proxy.

Configuring Network Interface Cards

You must configure the network interface cards for your Public Edge or Private Edge to point to valid DNS servers. The Private Edge points to internal DNS servers, while the Public Edge points to one or more publicly accessible DNS servers.

To complete this task, perform the following steps:

1. In Control Panel, select **Network Connections**.
2. In the **Network Connections** window, right-click the relevant **Local Area Connection** icon, and click **Properties**.
3. In the **Network Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and click the **Properties** button.
4. Select **Use the following DNS server addresses**, and then enter the IP address of the relevant DNS server.

Additional Resources

If you want more information on DNS configurations for Public IM Connectivity, review “Live Communications Server 2005 Document: Deploying Access Proxy and Director” on the Microsoft Web site, at: http://www.microsoft.com/downloads/details.aspx?FamilyId=9F8BDD90-D6A5-4F1A-8DFA-782B3870FD7F&displaylang=en.

Planning for Certificates

Introduction

MTLS encrypted connections with Public IM providers require certificates to be installed on the Access Proxy, but the certificate requirements are slightly different from Federation. Public IM Connectivity does require a public certificate from a public certificate authority.

Public Edge Certificate

With Public IM connectivity, you must purchase and configure a certificate from a public CA that is acceptable to the public IM service provider. Examples of acceptable certificates include those from EnTrust, VeriSign, and Thawte. LCS 2005 with SP1 requires standard Web server certificates for connection to Yahoo! and MSN, whereas AOL requires certificates that support both client and server enhanced key usage (EKU).

Private Edge Certificate

The Private Edge can use a certificate from a Windows Server 2003 CA. If you have an existing Windows Server 2003 CA, you can obtain a certificate for the Private Edge from an existing Windows Server 2003 CA. You can also use a public certificate on the Private Edge.

Additional Resources

If you do not have an existing Public Key Infrastructure, review "Live Communications Server 2005 Document: Configuring Certificates" on the Microsoft Web site, at:
www.microsoft.com/downloads/details.aspx?FamilyId=779DEDAA-2687-4452-901E-719CE6EC4E5A&displaylang=en

Lesson: Configuring Access Proxy Settings for Public IM Connectivity

- Obtaining a Public Certificate
- Configuring an Access Proxy for Public IM Connectivity
- Enabling Users for Public IM Connectivity

Introduction

The last phase of deploying an Access Proxy server for public Instant Message connectivity is the configuration phase. Obtain a public certificate, configure the Access Proxy for Public IM Connectivity, and enable your users for the Public IM Connectivity to work properly.

Lesson Objectives

After completing this lesson, you will be able to:

- Obtain a Public Certificate.
- Configure an Access Proxy for Public IM Connectivity.
- Enable Users for Public IM Connectivity.
- Configure Access Proxy server settings for PIC.

Obtaining a Public Certificate for an Access Proxy Server with Public IM Connectivity

- Visit Public CA Provider's Web Site
- Purchase Suitable Certificate
- Generate Certificate Signing Request
- Submit Certificate Signing Request

Introduction

A public certificate is required on your Access Proxy when you choose to enable public IM connectivity. Third-party certificate authorities (CA) have the following advantages:

- Customers have a greater degree of confidence when conducting secure transactions outside the organization.
- Customers can take advantage of the provider's understanding of the technical, legal, and business issues associated with certificate use.

Obtaining a public certificate involves the following steps:

1. Verify that your CA is on the default list of trusted CAs for a Windows enterprise CA.
2. Generate a Certificate Signing Request (CSR).
3. Submit the CSR to the public CA.

Determining CA Providers

For Public IM Connectivity, you must use a certificate issued by a public certificate authority that is in the default list of trusted root certification authorities.

To review the list of trusted root certification authorities, perform the following steps:

1. Click **Start**, and then click **Run**.
2. On the **Open** box, type **mmc**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. On the **Add/Remove Snap-in** dialog box, click **Add**.
4. On the **Available Standalone Snap-ins** box, click **Certificates**, and click **Add**.

5. Select **Computer account**, and then click **Next**.
6. On the **Select Computer** dialog box, ensure that the **Local computer: (the computer this console is running on)** check box is selected, and then click **Finish**.
7. Click **Close**, and then click **OK**.
8. In the navigation pane of the **Certificates** console, expand **Certificates (Local Computer)**.
9. On the **Certificates** snap-in, expand **Certificates**, and then click **Trusted Root Certification Authorities**.

Purchasing Certificate

After you have determined the appropriate CA provider, you can complete the transaction by purchasing a public certificate. Purchasing a public certificate will require you to generate a Certificate Signing Request (CSR).

Certificate Signing Request

You must create a CSR and give it to your CA provider. You can use the Windows Server 2003 utility Certreq.exe to generate a certificate signing request from an .inf file.

To generate a CSR, complete the following steps:

1. Log on to your Live Communications Server computer as a member of the **RTCLocalAdmins** group.
2. Open a Command Prompt window. At the command prompt, go to the **system32** subdirectory in the Windows installation directory (by default <drive letter>**:\WINDOWS\system32**), where certreq.exe is installed.
3. At the command prompt, type**: certreq -new PolicyFileIn RequestFileOut**

Submit CSR

After you have generated the CSR (certificate signing request), access the public CA (certification authority) site to request your certificate. The request process will vary depending on the CA you choose, but in each case you generally need to supply your organization and contact information. You must also download the root CA chain of the public CA and install it on the local computer store of the Access Proxy. To submit a request to a public certification authority, complete the following steps:

1. Open the output file, and copy and paste the contents of the CSR into the appropriate text box, beginning with:

   ```
   -----BEGIN NEW CERTIFICATE REQUEST-----
   ```

   And ending with:

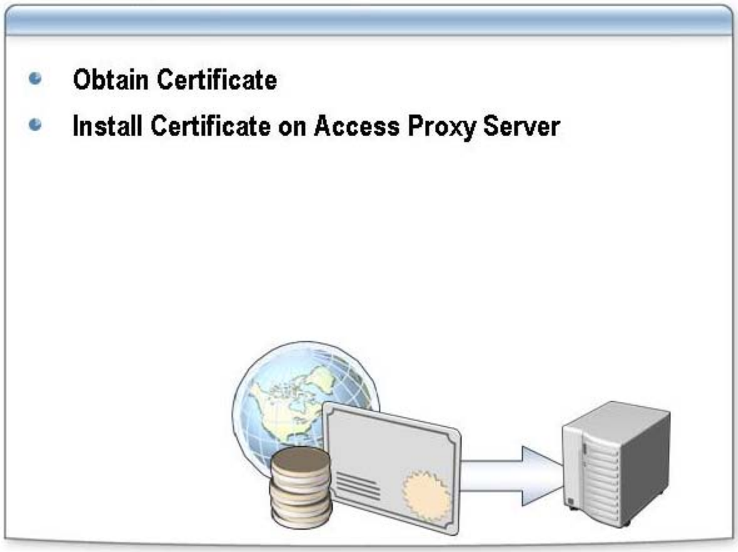
   ```
   -----END NEW CERTIFICATE REQUEST
   ```

2. If prompted, select the following options:
   - Microsoft as the server platform
   - IIS as the version
   - Web Server as the usage type
   - PKCS7 as the response format
3. When the public CA has verified your information, you will receive an e-mail message containing text required for your certificate.
4. Copy the text from the e-mail message and save the contents in a text file (.txt) on your local computer.

Additional Resources

To create your **PolicyFileIn** and **RequestFileOut** files, review "Live Communications Server 2005 Document: Configuring Certificates" on the Microsoft Web site, at: www.microsoft.com/downloads/details.aspx?FamilyId=779DEDAA-2687-4452-901E-719CE6EC4E5A&displaylang=en.

Configuring an Access Proxy with a Public Certificate



- Obtain Certificate
- Install Certificate on Access Proxy Server

Introduction

You can use the Certreq.exe tool to import your public certificate. How you use the tool to request and install a certificate will vary depending on the topology of your LCS 2005 with SP1 deployment. On a single Access Proxy, you can run the tool and install the certificate. For an array of Access Proxies, run Certreq.exe on a separate server, and then export the certificate to each server in the Access Proxy array.

Importing Certificate

When the public CA issues you a certificate, you receive an e-mail message containing the contents of your certificate.

To import the certificate, perform the following steps:

1. Copy the text in the e-mail message, beginning with:

   ```
   -----BEGIN CERTIFICATE-----
   ```

   And ending with:

   ```
   -----END CERTIFICATE
   ```

2. Paste the contents into a blank text file (.txt).
3. In the <drive letter>**:\WINDOWS\system32** directory, save the file with extension .txt. This is the directory where you stored Certreq.exe.
4. At the command prompt, type: **certreq -accept FullResponseFileIn**.
5. **FullResponseFileIn** is the name of the .txt file you saved in step 3.

Verify Certificate

To verify that the certificate was successfully imported on your Access Proxy server, complete the following steps:

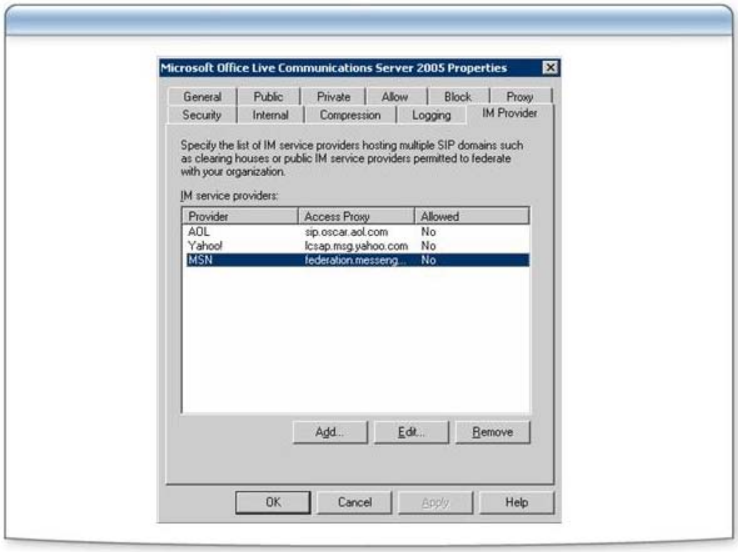
1. Click **Start**, and then click **Run**. In the **Open** box, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**.
3. In the **Add/Remove Snap-in** dialog box, click **Add**.

4. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In **Certification Snap-ins**, click **Computer Account**, and then click **Next**.
7. In the **Select Computer** dialog box, ensure that **Local computer (the computer this console is running on)** is selected. This option is the default. Leave the **Allow the selected computer to be changed when launching from the command line** check box clear.
8. Click **Finish**, click **Close**, and then click **OK**.
9. In the navigation pane of the Certificates console, expand **Certificates**, expand **Personal**, and then expand **Certificates**. Verify that the new certificate appears in the results pane of the console. You can identify the new certificate by its name and time stamp.

Additional Resources

For more information about requesting a certificate from a third-party certificate authority, review “Live Communications Server 2005 Document: Configuring Certificates” on the Microsoft Web site, at: http://www.microsoft.com/downloads/details.aspx?FamilyId=779DEDAA-2687-4452-901E-719CE6EC4E5A&displaylang=en.

Configuring Access Proxy for PIC



Specify the list of IM service providers hosting multiple SIP domains such as clearing houses or public IM service providers permitted to federate with your organization.

IM service providers:

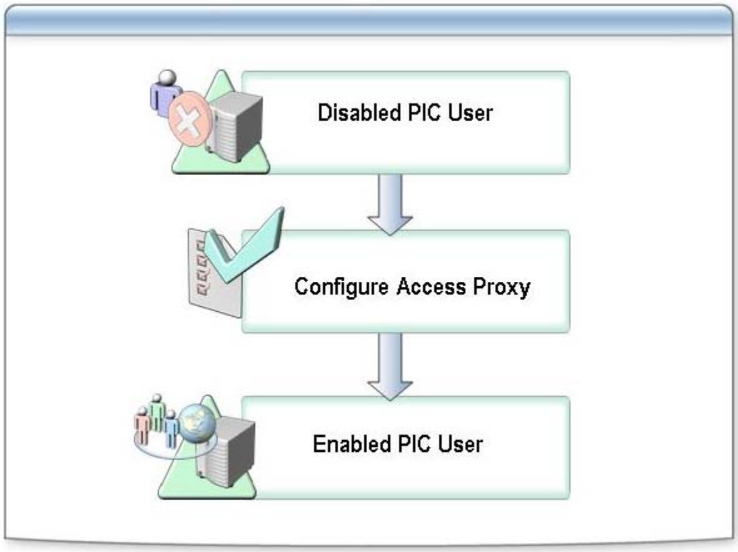
Provider	Access Proxy	Allowed
AOL	sip.oscar.aol.com	No
Yahoo!	lcsap.msg.yahoo.com	No
MSN	federation.messeng...	No

After you have provisioned Federation with public IM service providers, configured DNS, and a public certificate on your Access Proxy, you can now complete the configuration process by enabling your Access Proxy to connect to the public IM service providers with whom you have exchanged provisioning information.

To enable a connection to a public IM service provider, perform the following steps:

1. On the Access Proxy, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**.
2. If necessary, expand **Services and Applications**.
3. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
4. On the **IM Provider** tab, select the public IM service provider that you want to enable, and then click **Edit**.
5. In the **Edit IM Service Provider** dialog box, select the **Allow this IM Service Provider** checkbox, and then click **OK**.
6. Click **OK** or **Apply** to continue.

Enabling Users for Public IM Connectivity



Introduction

After you have configured your Access Proxy server and the LCS 2005 with SP1 Forest Level for Federation and Public IM Connectivity, you must authorize your internal users to communicate with users with accounts with public IM service providers. Unless your internal users are authorized, they will not be able to take advantage of LCS 2005 with SP1 features when communicating with MSN, Yahoo!, or AOL users.

Configuration Tools

You can enable users for Public IM Connectivity by using either the Active Directory® Users and Computers snap-in or the Live Communications Server 2005 Administrative snap-in on a Live Communications Server attached to your SIP domain. The easiest way to authorize multiple users is to use the Configure Users Wizard.

Important Before you can perform the following procedures, you must first authorize users for Live Communications Server as described in the Standard Edition and Enterprise Edition deployment guides. You must also be logged on as a member of the RTCDomainUserAdmins group.

Active Directory Users and Computers

You can enable users for Public IM Connectivity with the Active Directory Users and Computers snap-in. You can control who is and who is not enabled for Public IM Connectivity on an individual basis. By default, users are not enabled for Public IM Connectivity.

To enable users for Public IM Connectivity, perform the following steps:

1. On an internal Live Communications Server, click **Start**.
2. Click **Run**.
3. In the **Open** box, type **dsa.msc**, and then click **OK**.
4. Select the organizational unit where your user accounts reside.
5. In the **Users** pane, select one or more users, right-click the selection, and then click **Configure Users** to run the **Configure User Wizard**.

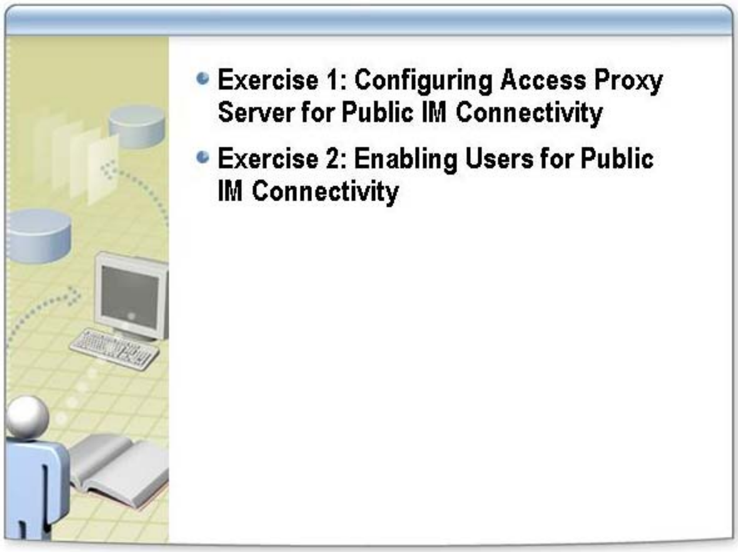
Live Communications Server Console

To enable multiple user accounts for Public IM Connectivity, you may find it more convenient to use the Live Communications Server management console.

To enable multiple users, perform the following steps:

1. On an internal Live Communications Server, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005**.
2. Expand the forest node, expand the **Live Communications Servers and Pools** node, and then expand the domain node and any child nodes until you reach the folder where your user accounts reside.
3. Right-click the folder where your user accounts reside and click **Configure Users** to run the **Configure User Wizard**.
4. On the **Welcome to the Configure User Wizard** page, click **Next**.
5. On the **Configure User Settings** page, select **Configure Public IM Connectivity**, and then click **Allow Users** for each selection.
6. On the **Configure Operation Status** page, if you want to export the log, click Export to save the XML file.
7. Click **Finish**.

Lab 9: Enabling Public IM Connectivity



- Exercise 1: Configuring Access Proxy Server for Public IM Connectivity
- Exercise 2: Enabling Users for Public IM Connectivity

Objectives

After completing this lab, you will be able to:

- Configure an Access Proxy server for Public IM Connectivity capabilities.
- Enable users for Public IM Connectivity.

Estimated time to complete this lab: **10 minutes**

Important: At the end of this lab, leave the VPC images running.

Introduction

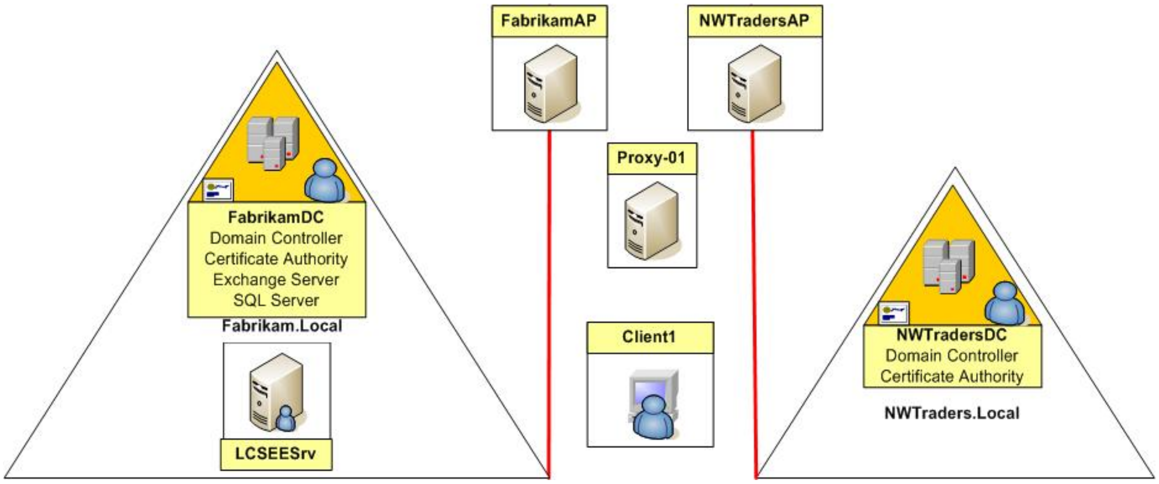
Fabrikam wants to enable its sales employees to conduct IM conversations with users of public IM networks, including AOL, MSN and Yahoo! Matt Dawson, the network manager for Fabrikam, has been tasked to enable this connectivity. However, Fabrikam only wants incoming connections from public IM users that are already known to Fabrikam sales department employees.

In this lab, you will prepare your Access Proxy server for Public IM Connectivity. You will also authorize users for Public IM Connectivity.

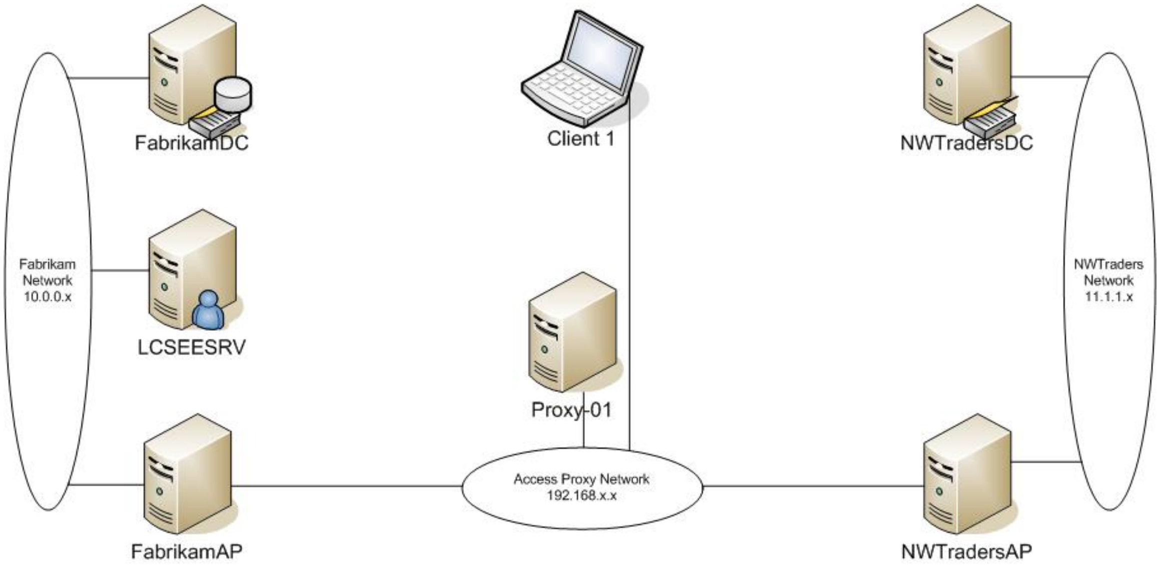
Connectivity to public IM providers requires additional licensing arrangements and a connection to the Internet. These requirements can not be met in a classroom environment, so it is not possible to configure a working example of public IM connectivity in this lab.

Network Topology

The labs in this course use virtual machines. In order to configure the virtual machines to be usable in a lab environment, the network topology has been substantially modified from a typical network configuration. The lab configuration combines many server roles in non-standard ways that are not recommended and are generally not viable in a production network. The network topology used in these labs is shown in the following figures.



Physical Network Topology



Virtual PC Image to Computer NetBIOS Name Mappings

The following table shows the mapping between the VPC images and the computer NetBIOS names for this lab. Please ensure that you use the correct VPC image from the VPC console to start the lab.

VPC Configuration Name	Computer NetBIOS Name
7034A-FabrikamDC-B	FabrikamDC
7034A-FabrikamAP-B	FabrikamAP

⚠ **Important: These virtual PC images should already be started from the previous lab.**

Do NOT close down the VPC images at the end of this lab.

Exercise 1
Enable Public IM Connectivity on an Access Proxy Server

Scenario

Enabling Public IM Connectivity requires Matt to configure the Fabrikam Access Proxy server. This configuration must be completed on each Access Proxy server in the perimeter network.

Description

After you have provisioned Federation with public IM service providers and configured DNS and a public certificate on your Access Proxy, you must configure your Access Proxy to enable connection to the public IM service providers with whom you have exchanged provisioning information.

In this exercise, you will configure the Access Proxy server by enabling the Public IM Connectivity.

Tasks	**Detailed Steps**
⚠ **Important:** Perform this exercise on the 7034A-FabrikamAP-B virtual machine.	
1. Enable Public IM Connectivity.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Computer Management**. **c.** On the Computer Management console, expand **Services and Applications**. **d.** Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**. **e.** On the **IM Provider** tab, in the **IM service provider** list, click **AOL**, and then click **Edit**. **f.** On the **Edit IM Service Provider** dialog box, select the **Allow this IM service provider** check box. **g.** In the **Select an option for filtering incoming communications** section, click **Allow communications only from users on recipient's contact list**. **h.** On the **Edit IM Service Provider** dialog box, click **OK**. **i.** Repeat steps e to h for **MSN** and **Yahoo!**. **j.** On the **Microsoft Office Live Communications Server 2005 Properties** dialog box, click **OK**. **k.** Close the Microsoft Office Live Communications Server 2005 console.

Exercise 2
Enable Users for Public IM Connectivity

Scenario

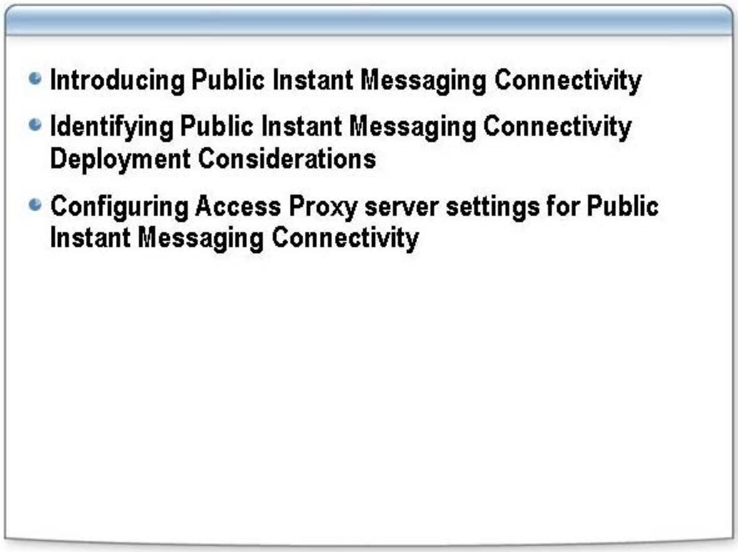
Matt now needs to enable Public IM connectivity for the sales department users. Because he is currently running a pilot program, he is only going to enable public IM access for Jim Kim.

Description

In this exercise, you will enable a user for Public IM Connectivity by using the Active Directory Users and Computers management console.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
1. Enable users.	**a.** Log on to the **7034A-FabrikamDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. **c.** In the Active Directory Users and Computers console, expand the **fabrikam.local** domain, and click the **LCSUsers** organizational unit. **d.** In the **LCSUsers** organizational unit, double-click **Jim Kim**. **e.** In the **Jim Kim Properties** dialog box, click the **Live Communications** tab, and then click **Advanced Settings**. **f.** In the **User Advanced Settings** dialog box, select the **Enable public IM connectivity** check box, and then click **OK**. **g.** In the **Jim Kim Properties** dialog box, click **OK**. **h.** Close the Active Directory Users and Computers console. **i.** **DO NOT** close the VPC images, but leave them running for the Lab 10.

Review



- Introducing Public Instant Messaging Connectivity
- Identifying Public Instant Messaging Connectivity Deployment Considerations
- Configuring Access Proxy server settings for Public Instant Messaging Connectivity

In this module, you learned that the Access Proxy server with Public IM Connectivity requires additional licenses and a provisioning process. You also learned that Public IM Connectivity provides encrypted communications between your users and members of AOL, Yahoo!, and MSN.

In the next module, you will learn the security features available for LCS 2005 with SP1. You will understand the potential threats and how to use group policy for securing your LCS 2005 with SP1 infrastructure.