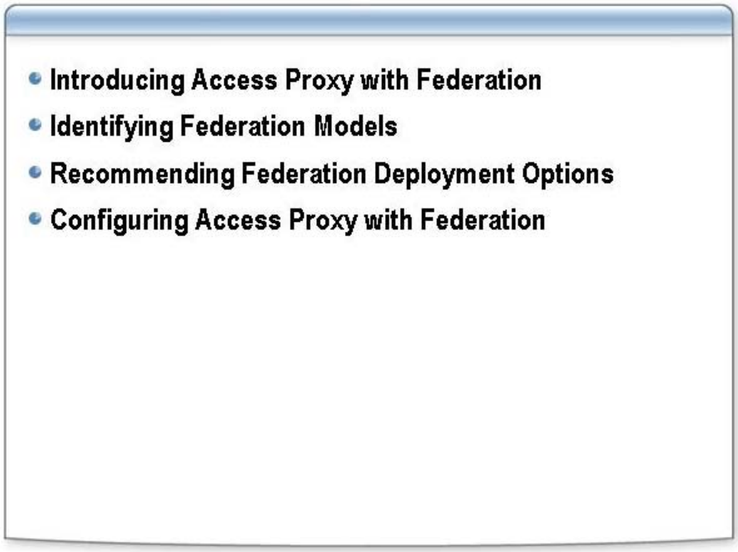
Module 8: Implementing Federation in Live Communications Server 2005 with Service Pack 1

Contents

Overview



- Introducing Access Proxy with Federation
- Identifying Federation Models
- Recommending Federation Deployment Options
- Configuring Access Proxy with Federation

Introduction

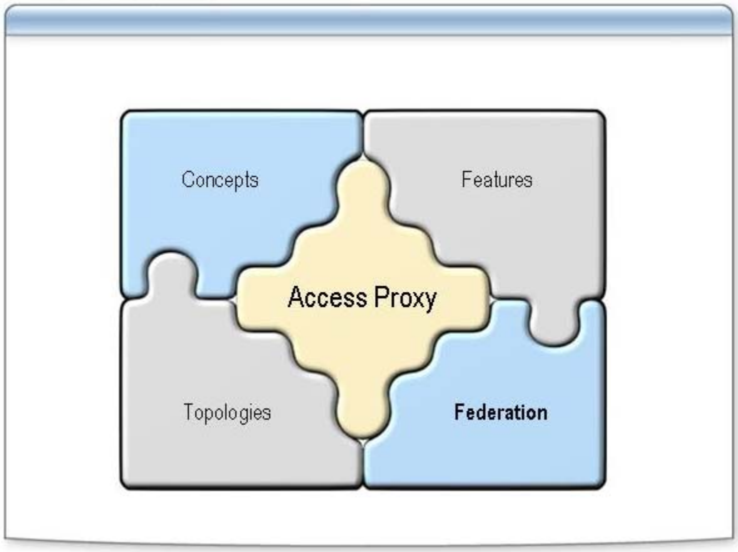
This module explains the procedure for enabling Federation on your Access Proxy server in Microsoft® Live Communications Server. It also describes the different Federation models. Finally, this module explains how to deploy and configure an Access Proxy server for Federation.

Objectives

After completing this module, you will be able to:

- Describe the concepts, features, and topology of an Access Proxy server that supports Federation.
- Explain the Federation deployment scenarios.
- List the requirements and recommendations for enabling Federation on an Access Proxy.
- Configure Federation on an Access Proxy server.

Lesson: Introducing Access Proxy with Federation



Introduction

When you enable Federation on your Access Proxy server, your LCS 2005 with SP1 infrastructure will be able to exchange Session Initiation Protocol (SIP) traffic with mutually trusted SIP domains. Federation enables employees in separate organizations to use instant messaging to discuss business related topics in real time.

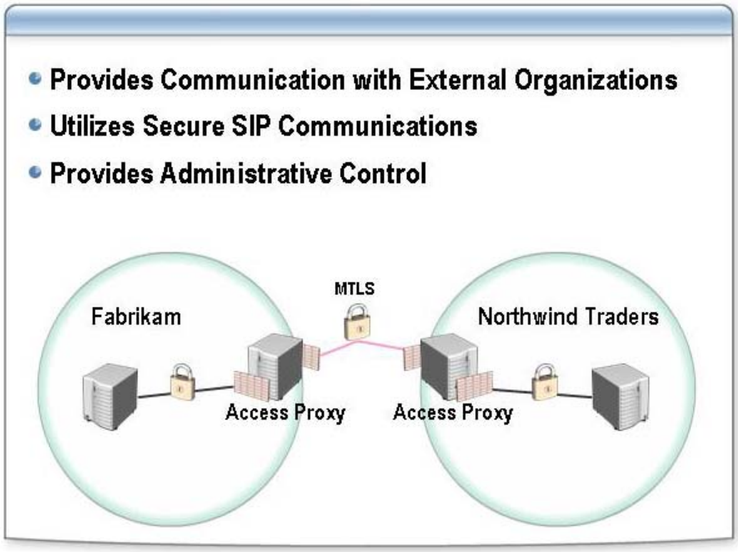
Lesson objectives

This lesson introduces the Access Proxy server configured to support Federation, which you may want to install in either a LCS 2005 with SP1 Standard or Enterprise Edition environment. This lesson also describes the concepts, features, and topologies of Federation.

After completing this lesson, you will be able to:

- Explain the purpose of enabling Federation on your Access Proxy server.
- List the features of Federation.
- List each topology Federation supports.
- Describe the concepts, features and topology of an Access Proxy server with Federation.

What Is Access Proxy Server with Federation?



- Provides Communication with External Organizations
- Utilizes Secure SIP Communications
- Provides Administrative Control

Introduction

Live Communications Server 2005 with SP1 extends existing federation support to include a variety of new scenarios. These new scenarios include Enhanced Federation.

Federation

Federation is the ability to establish trust relationships between your organization and one or more external networks, so that users can initiate instant messaging (IM) sessions, exchange notifications, and subscribe to user presence across network boundaries. Federation makes it possible to extend the benefits of instant messaging and presence awareness throughout your organization's entire business sphere.

Secure SIP Connections

The Access Proxy server with Federation is configured to only allow Mutual Transport Layer Security (MTLS) encryption. All communication traffic between your LCS 2005 with SP1 infrastructure and external LCS 2005 with SP1 enterprise deployments is encrypted. Message content is protected while in transit across public networks.

Administrative Control

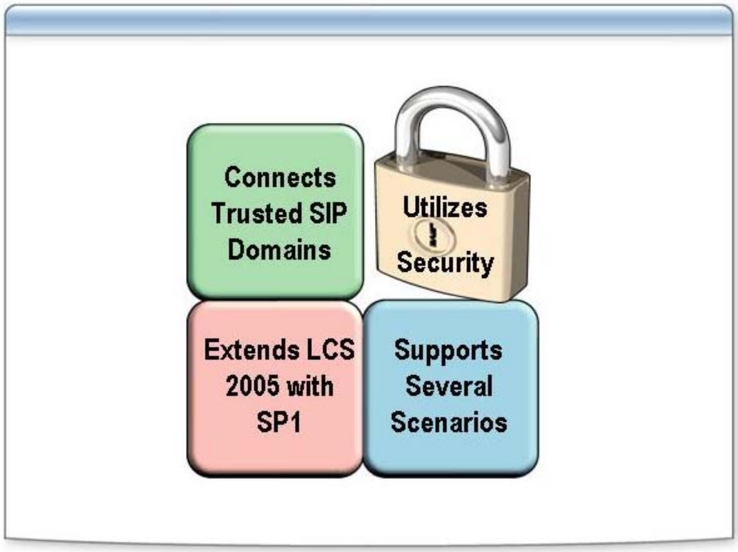
When enabling Federation on your Access Proxy server, you are configuring your Access Proxy server to trust valid certificates from other LCS 2005 with SP1 Access Proxies. However, you maintain full control of your internal LCS 2005 with SP1 infrastructure. You decide which of your users are enabled to participate in Federation, and you can make decisions about other configuration settings as well, such as configuring how to block Spam over Instant Messaging (SPIM).

Federation Scenarios

Business partners, subsidiaries, and customers with their own internal LCS 2005 with SP1 deployment, can be trusted as Federation partners. Federation enables your key employees to communicate with partners, subsidiaries and customers in real time, as if you all resided in the same SIP domain.

Suppliers can also be Federation partners. Instant messaging supported by an Access Proxy server with Federation could notify your warehouse employees that a large shipment will arrive before scheduled, or could provide instant updates on any delays.

Identifying Federation Features and Benefits



Connects Trusted SIP Domains

Utilizes Security

Extends LCS 2005 with SP1

Supports Several Scenarios

Introduction

An Access Proxy server with Federation extends LCS 2005 with SP1 by allowing features such as instant messaging and presence awareness to be enabled between users located in different companies and organizations. Federation differs from an Access Proxy server with Remote User Access because instead of allowing your users to access their own private LCS 2005 with SP1 deployment, Federation allows certain features to be used between your internal users and the employees of organizations that participate in a Federated partnership.

Live Communications Server 2005 with SP1 provides several Federation options. When you enable your Access Proxy server with Federation, the following topologies can be configured:

- Direct Federation
- Enhanced Federation through:
  - Restricted Federation
  - Unrestricted Federation
- Clearinghouse

Trusted SIP Domains

Each Access Proxy server enabled with Federation requires digital certificates. You can decide which companies will be trusted to participate in Federation with your company based on the Federation model you choose.

Security Considerations

All Federation connections are encrypted using Mutual Transport Layer Security (MTLS), in which each partner's Access Proxy must present a valid certificate to the participating Federation partner.

Administrators in each domain can authorize or deny federated access for individual users or groups of users. Administrators can also block federated partners from obtaining presence information or from using IM with particular users.

Extends IM Benefits

When Federation is properly configured on your Access Proxy server, users have access to presence information and instant messaging capabilities from your designated federated partners. Federation also enables the following features of your LCS 2005 with SP1 infrastructure between your users and trusted Federation partners:

- Obtaining notifications
- Configuring User Block Lists
- Configuring User Allow Lists

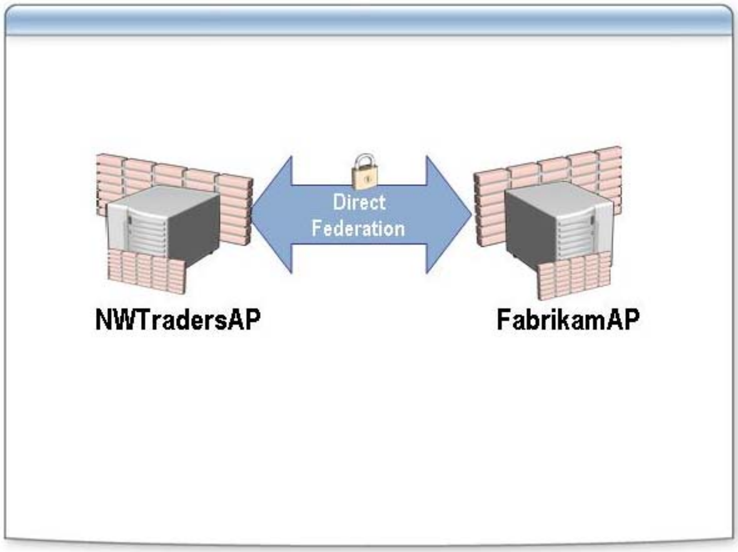
Users can use LCS 2005 with SP1 to communicate in the following ways:

- Internal users with federated partners
- Remote users with federated partners
- Internal users with federated partners working remotely
- Remote users with remote federated partners

Deployment Scenarios

Federation can be configured for Direct Federation or Enhanced Federation. Enhanced Federation is a new deployment scenario in LCS 2005 with SP1.

What Is Direct Federation?



Introduction

Direct Federation is a trusted peer-to-peer connection between two SIP domains. It requires that you specify both the Access Proxy and the SIP domain of each federated partner and that your partners do the same for you. Both Live Communications Server 2005 and Live Communications Server 2005 with SP1 support direct federation with as many as 300 partners.

Definition

Direct Federation occurs when two organizations each list the other as a federated partner and establish symmetrical deployments with a mutual trust relationship. Direct Federation provides the highest level of control, because you must specify both the destination domain and the corresponding Access Proxy for each partner.

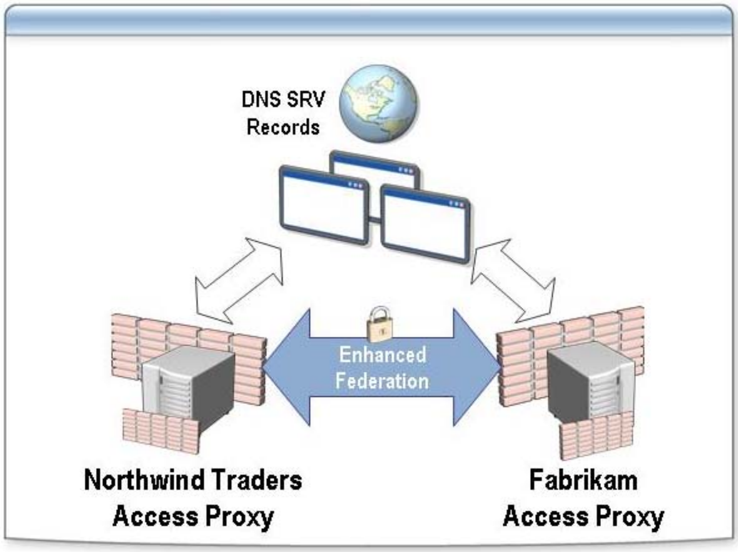
To set up a Direct Federation between Fabrikam and Northwind Traders, you will need to configure the **Allow List** on each Access Proxy server: NWTradersAP and FabrikamAP. The **Allow List** will include the fully qualified domain name (FQDN) of the federated partner's Access Proxy server and the FQDN of the destination domain.

Issues

Direct Federation provides a high degree of security and control. However, Direct Federation requires more maintenance than even Restricted Enhanced Federation. For this reason, Direct Federation is recommended only for partners who have neither upgraded to SP1 nor published a service record (SRV) for their domain. Direct Federation may also remain attractive for organizations with particularly diligent security requirements.

Exchanging and updating connection information for each partner can become burdensome when the number of partners is large. Eventually, some type of Enhanced Federation or use of either an IM service provider or a Clearinghouse becomes a reasonable alternative. These alternatives each provide easier ways than Direct Federation to enable Federation with large numbers of partners, although each also has limitations that you should consider.

What Is Enhanced Federation?



Introduction

Enhanced Federation is new in LCS 2005 with SP1. Enhanced Federation eliminates the need to specify the Access Proxy of every federated partner. You no longer have to manually specify the FQDN of your organization's Access Proxy to your partners.

Definition

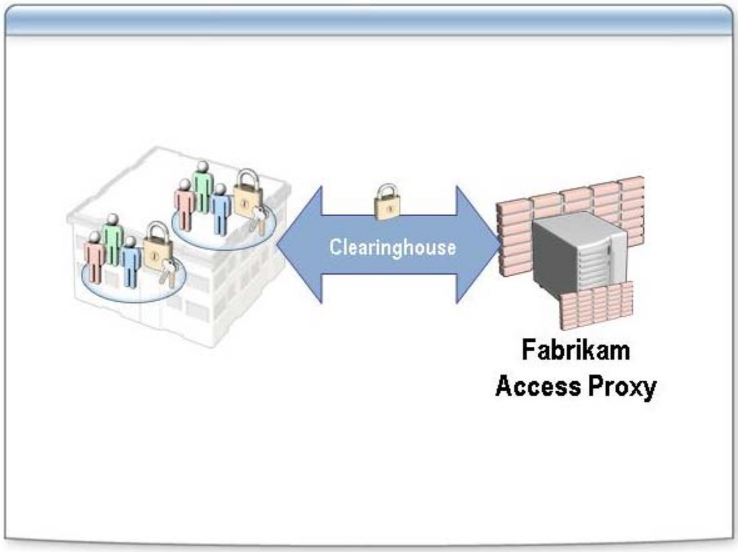
Enhanced Federation uses DNS SRV resolution to identify and connect dynamically to other LCS 2005 with SP1 domains. Enhanced Federation encrypts messages traversing the Internet and requires that the servers at both ends of a connection present valid certificates. Enhanced Federation comes in two varieties:

- **Restricted Federation**. When you enable Enhanced Federation on an Access Proxy, Restricted Enhanced Federation is enabled by default. This setting allows connections only with SIP domains that you specify. Restricted Enhanced Federation is the recommended model for enterprise-to-enterprise Federation. Restricted Enhanced Federation is the easiest way to initiate and maintain Federation with a large number of domains, while retaining the ability to restrict access to your deployment.
- **Unrestricted Federation**. Unrestricted Enhanced Federation allows connections with any SIP domain that presents a valid certificate. You can, however, block IM from unwelcome sources either by adding undesired domains to the Access Proxy's Block list or by copying their certificates from the Access Proxy's Microsoft Management Console (MMC) to the non-trusted certificates store on local computers. If these conditions are acceptable, Unrestricted Enhanced Federation provides the easiest way to federate with a large number of partners.

Issues

Enhanced Federation greatly reduces the overhead of initiating and maintaining Federation with multiple partners, but it reduces the amount of control you have over incoming SIP traffic. Before you configure an Access Proxy for Enhanced Federation, it is essential to review the Federation needs of your organization and the degree of control over incoming SIP traffic that you require.

What Is a Clearinghouse?



Introduction

The Clearinghouse federates directly with each of its members and acts as a trusted broker for exchanging information among them. An Access Proxy server that acts as a Clearinghouse does not distribute SIP traffic directly, but instead passes it to internal servers that perform the necessary authentication and that possess the necessary routing logic. In most cases, where one Clearinghouse partner is attempting to communicate with another Clearinghouse partner, the traffic is routed back to the Access Proxy to be routed appropriately. A Clearinghouse member can typically accept federation with all other members, or it can deny access to certain organizations while allowing access to the rest.

Default Route

There are two scenarios for configuring an Access Proxy to work with a Clearinghouse. When your Access Proxy server is enabled as a federated partner with a Clearinghouse, the Default Route is configured. This will forward your outbound SIP traffic to a Clearinghouse.

Act as Clearinghouse

The other scenario is to configure your Access Proxy server to act as a Clearinghouse. If your company is a service provider that wants to offer Clearinghouse services, you can use Microsoft SIP Processing Language (MSPL) and the Live Communications Server 2005 application programming interface (API) to implement customer business logic for any given set of community policies or regulatory rules. The Access Proxy itself does not distribute incoming traffic to member domains. It simply passes that traffic to an internal SIP server (such as a Director) that implements the custom routing logic.

Note Very few Live Communications Server 2005 deployments are likely to set themselves up as a Clearinghouse. Unless you are deploying an Access Proxy for use as a Clearinghouse, you should not use this scenario.

Planning for Federation

- Determining Business Partners
- Establishing Communication with Partners
- Scheduling Implementation Timeframe
- Testing Implementation
- Enabling Federation Topology
- Enabling Federation Users

Introduction

Many of your previous infrastructure deployments have required careful planning. Enabling Federation on your Access Proxy server should receive the same attention to detail as your Remote User Access implementation.

Determine Business Partners

Determining your Federation topology may simply depend on the number of business partners with which your company plans to use LCS 2005 with SP1 features. The following list includes reasons why you may choose Direct Federation:

- Your company has strict security policies.
- Your company only wants to federate with its single subsidiary.
- Your environment has a one-to-one relationship with a supplier or distributor.
- A small and finite list of federated partners is approved by your business.
- You have not upgraded to SP1 or published a SRV record for your domains.
- You have more than one domain name.
- You will have less than 300 federated partners.
- You can obtain the FQDN of your Federated partner’s Access Proxy server and SIP domain.
- You have time to maintain all the technical and business information for each Federated partner.

You may choose Enhanced Federation if you identify with the following list:

- As a supplier or distributor, your company will have one-to-many Federation relationships.
- You do not have a finite list of federated partners.
- You wish to enable Enterprise to Public Cloud.
- You require Federation with more than 300 federated partners.

- You have LCS 2005 with SP1 implemented.
- You want to reduce the amount of overhead and maintenance when working with Federated partners.
- You want to reduce the amount of Federation rules, but want to maintain administrative control by using Restricted Enhanced Federation.
- You know the domain names of the Federated partners you will allow in the Enhanced Federation table.
- Your company will allow any domain with a valid certificate to communicate with your Access Proxy through Unrestricted Enhanced Federation.
- You do not want use a Clearinghouse.

Use the following list to determine whether you can implement a Clearinghouse Federation model:

- Set up a default route if you want to use LCS 2005 with SP1 features with a domain that is included in a Clearinghouse.
- A default route to a Clearinghouse cannot be configured on the same Access Proxy server as Enhanced Federation.
- A default route to a Clearinghouse cannot be configured on the same Access Proxy server that is acting as a Clearinghouse.

Establish Communication

The level of communication between your federated partners may differ based on the Federation topology. For example, Direct Federation will require you to manually list your federated partner's infrastructure information and obtain the following:

- The fully qualified domain name (FQDN) of your federated partner's SIP domain.
- Your federated partner's Access Proxy server's FQDN.
- If your federated partner has multiple SIP domains you want to partner with, the FQDN for each SIP domain.

If you use Direct Federation, you will need to determine who will provide the information stated above, their business contact information, best time to contact, and which method of communication he or she prefers.

You will also need to create and maintain a list which matches the infrastructure information stored in the Allow List to the business contact information of your Federated partner(s).

Schedule Implementation

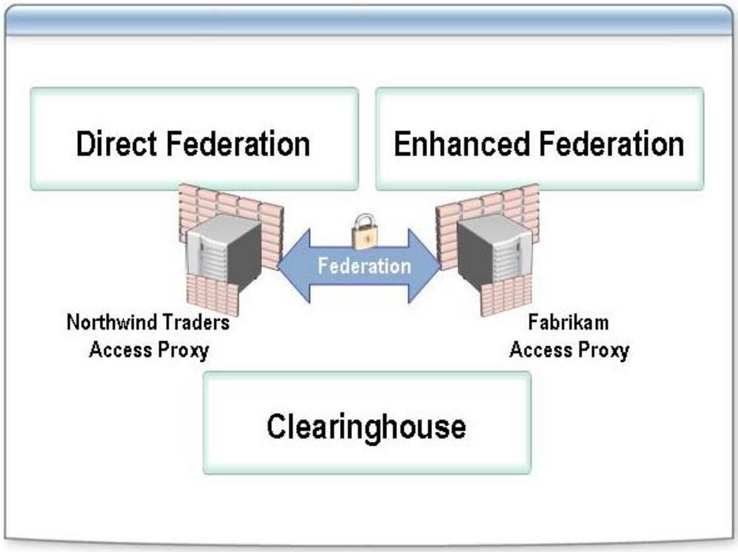
Determine an implementation schedule between you and your federated partner. It is not technically required, but it is considerate when working with federated partners in different time zones or those who require change control.

Even if you choose to enable Restricted Enhanced Federation, it might be considerate for you to notify your Restricted Enhanced Federation partner of a general timeframe when you will add them to the Allow List. Likewise, your Enhanced Federation partner should do the same.

Test Implementation

After you have configured your Access Proxy server with the Direct Federation partner, it is important to test the implementation. By default, you will need to enable your internal test user for Federation. After it is enabled, test the LCS 2005 with SP1 features such as instant messaging and presence awareness.

Lesson: Configuring Federation Models



Introduction

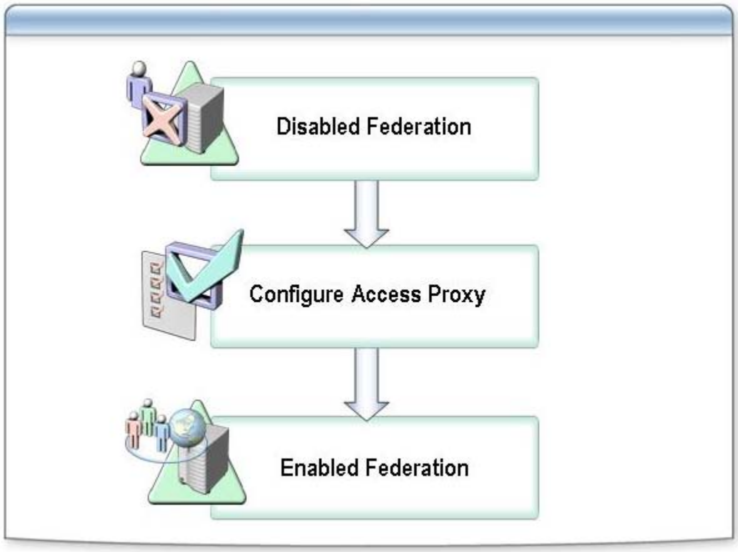
This lesson covers the procedures that you must implement to configure Federation on a LCS 2005 with SP1 Access Proxy server, depending on the Federation topology you have chosen. This lesson applies to either a LCS 2005 with SP1 Standard or Enterprise Edition environment.

Lesson objectives

After completing this lesson, you will be able to:

- Enable Federation.
- Configure Direct Federation.
- Enable Enhanced Federation.
- Determine Clearinghouse usage.
- Explain each deployment scenario of Federation.

Enabling Federation Models



Enable Federation Topology

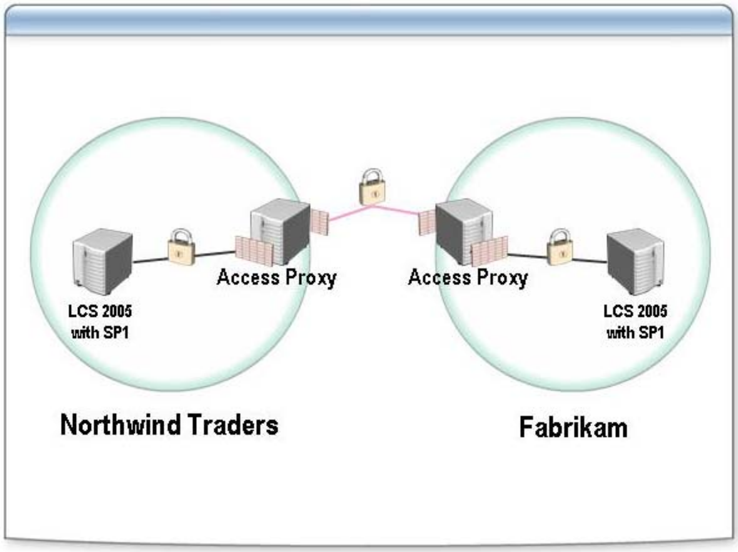
To enable your federation topology on your Access Proxy server, perform the following steps:

1. On the Access Proxy, open **Computer Management**. 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 **General** tab, select **Federate with other domains**.

Note Enabling Federation activates controls for specifying a default route, acting as a Clearinghouse, and enabling archiving disclaimer notifications. If you want to enable any of these features, you can do so now by selecting the appropriate check boxes.

5. Click **OK**.

Configuring Direct Federation



Direct Federation Partners

For each Direct Federation partner, you must enter both the FQDN of its Access Proxy and the SIP domain name on the **Allow** tab. If a federated partner has multiple SIP domains, you must create a separate entry for each domain with which you want to federate. If you do not want to federate with one or more of a direct partner's domains, do not enter the names of those domains in the Allow list.

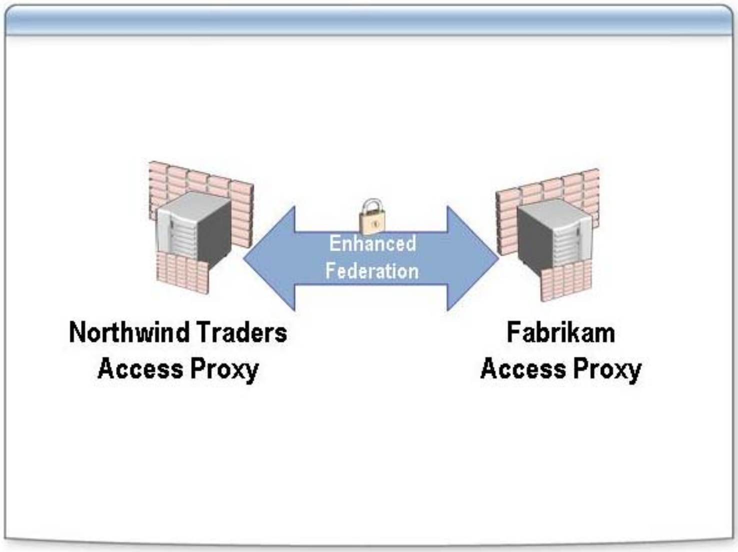
You must repeat the federation procedure for each partner with which you want to federate. If the number of partners makes entering and maintaining the required information too difficult, consider using Restricted Enhanced Federation, a Clearinghouse, or Federation with an IM service provider.

Configuring Direct Federation

To configures your Access Proxy for Direct Federation with partners specified in the Access Proxy's Allow list, perform the following steps:

1. On the Access Proxy, open **Computer Management**. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**.
2. If necessary, in the navigation pane of the Computer Management console, expand **Services and Applications**.
3. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
4. In the **Properties** dialog, click the **Allow** tab.
5. In the **Allow** dialog, click **Add**.
6. In the **Federated Partner Access Proxy** text box, tyoe the FQDN (fully qualified domain name) of the Access Proxy of your federated partner.
7. In the **Federated Partner Domain Name**, type the name of the domain to which messages will be routed.
8. Select an option for filtering incoming communications. Click **Help** for assistance. Click **OK**.

Configuring Enhanced Federation



Configuring Enhanced Federation

To configure an Access Proxy for Enhanced Federation, perform the following steps:

1. On the Access Proxy, open **Computer Management**.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**.
3. Expand **Services and Applications**.
4. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
5. On the **Enhanced Federation** tab, select the **Enable Enhanced Federation** check box. If the check box is unavailable, click the **General** tab and ensure that the **Federate with other Domains** check box is selected and that the **Use Default Route to Clearinghouse** check box is cleared.
6. To enable Unrestricted Enhanced Federation with all external domains, click **Allow Federation with Any Domain**. To allow Restricted Enhanced Federation only with domains that you specify, click **Allow Only Federated Domains Listed Below**.

Caution Allowing Enhanced Federation with any domain enables any computer that presents a valid certificate to connect to your internal SIP domain and send unsolicited messages to any user in that domain. For this reason, Restricted Enhanced Federation is the default and recommended configuration.

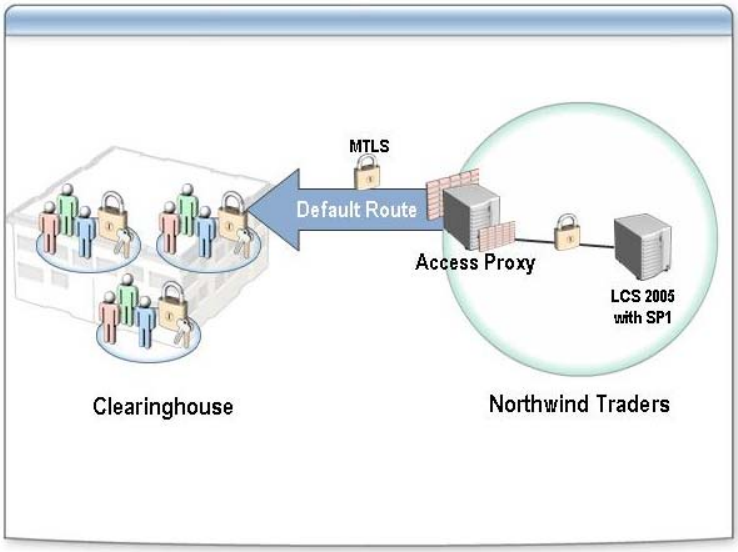
7. If you select **Allow Only Federated Domains Listed Below**, click **Add** to add a domain to the enhanced federation table. In the **Add Enhanced Federation Domain** dialog box, add the name of a SIP domain with which you want to enable enhanced federation, and then click **OK**. Wildcard characters are not accepted.
8. When your federated relationships are correctly configured, click **OK**.

Important You should enter exact SIP domain names with external companies with which you expect to federate. You should not enter only root domains, such as com or org, in this list. If you enter root domains, all organizations with these suffixes will be able to federate with your organization if they have Enhanced Federation enabled.

If you select **Allow Only Federated Domains Listed Below** and you do not enter any domains in the table, Enhanced Federation will not be possible with any domain. Activating the table and leaving it blank is equivalent to disabling Enhanced Federation by clearing the **Enable Enhanced Federation** check box.

If a domain that is added as a federated partner also appears in the table of blocked SIP domains on the **Block** tab, the domain will not be available. The **Blocked SIP Domains** table takes precedence over all other Federation settings. To enable Enhanced Federation with such a domain, you must remove it from the **Blocked SIP Domains** table, as well as adding it to the **Enhanced Federation** table.

Configuring Clearinghouse



Clearinghouse Configuration

The usual procedure for routing outbound SIP traffic to a Clearinghouse is to configure a default route on the Access Proxy. All outbound SIP traffic that is not routed to a Direct Federation partner is routed using the default route.

You cannot specify a default route and enable Enhanced Federation on the same Access Proxy. If you want to enable Enhanced Federation and use a Clearinghouse on the same Access Proxy, you must configure the Clearinghouse as an IM service provider.

To specify a default route to a Clearinghouse, perform the following steps:

1. On the Access Proxy, open **Computer Management**.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**.
3. Expand **Services and Applications**.
4. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
5. On the **Enhanced Federation** tab, ensure that you have cleared the **Enable Enhanced Federation** check box.
6. On the **IM Provider** tab, ensure that you have removed all IM service providers.

Important AOL, MSN® and Yahoo! appear by default in the IM service providers table. If you want to configure a default route on an Access Proxy server, you must remove these providers. On the **General** tab, ensure that **Federate with other Domains** is selected, and then select **Use Default Route to Clearinghouse**.

7. Type the FQDN of the Clearinghouse you are using.
8. Click **OK**.

Lesson: Identifying Federation Deployment Considerations

- Verifying DNS configuration
- Planning for certifications
- Enabling Federation users

Introduction

Implementing Federation on a LCS 2005 with SP1 Access Proxy server requires a dependable underlying network infrastructure. These infrastructure requirements include the following list:

- Domain Name Service (DNS) configuration
- Certificate selection
- Federation user selection

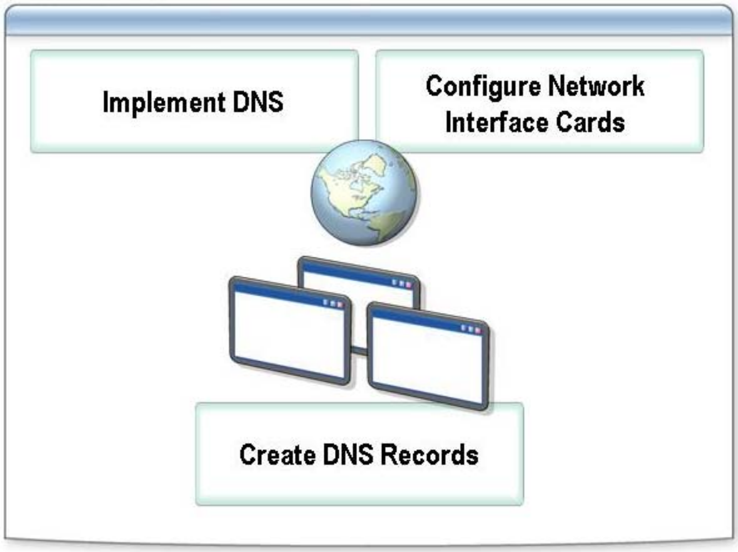
Without these infrastructure requirements, Federation will not function correctly. Hence, it is important for you to review and configure the existing infrastructure before deploying an Access Proxy server with Federation.

Lesson Objectives

After completing this lesson, you will be able to:

- Configure DNS for an Access Proxy server with Federation implementation.
- Plan for Access Proxy server with Federation certificates.
- Enable your Federation users.
- List the requirements and recommendations for deploying an Access Proxy server with Federation.

Preparing DNS for an Access Proxy Server with Federation



Implement DNS

Configure Network Interface Cards

Create DNS Records

Introduction

An Access Proxy with Federation implementation relies on DNS, so a functioning DNS environment is essential for Federation. 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:

- An A record that maps to the IP address of the Access Proxy server for the Private Edge on your internal DNS servers.
- An A record that maps to the IP address of the Access Proxy server for the Public Edge on your external DNS servers.

You might also complete the following 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's Public Edge.

Configuring Network Interface Cards

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

To complete this task, perform the following steps:

1. In Control Panel, select **Network Connections**.

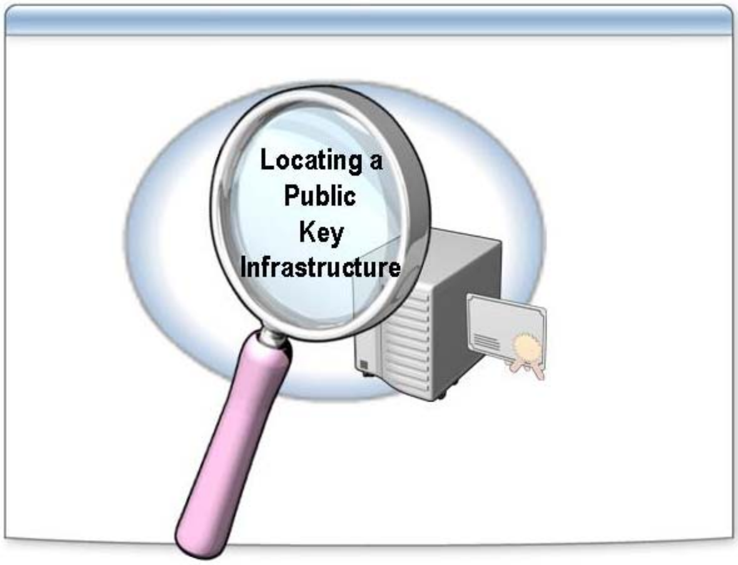
2. In the **Network Connections** window, right-click the relevant **Local Area Connection** icon, and click **Properties**.
3. In the **Network Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and click the **Properties** button.
4. Select **Use the following DNS server addresses**,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

Note You are likely to have a fixed IP address for both the Public and Private Edges on the Access Proxy server.

Additional Resources

If you want more information about DNS configurations for Federation, 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

Live Communications Server 2005 with SP1 requires each Access Proxy participating in Federation to have a digital certificate properly installed and configured.

You obtain these certificates from a Public Key Infrastructure (PKI). Your company might have an existing Microsoft Windows® 2003 certification authority (CA) infrastructure or use a third-party CA.

Important An Access Proxy with only a single DNS name only requires one certificate. However, when you configure a Public Edge and Private Edge, each edge could have its own DNS name, which requires two certificates.

The certificate installation process depends on the location of the Access Proxy server.

Windows 2003 Certification Authority

If you have an existing Windows 2003 CA and you are deploying the Access Proxy server on the internal network, you can obtain a certificate from the existing Windows 2003 CA.

Third-Party Certification Authority

You may obtain a certificate from a third-party certificate authority in any of the following scenarios:

- Deploying an Access Proxy server in a perimeter network
- Implementing Public IM connectivity
- Using Enhanced Federation
- Configuring Direct Federation with multiple federation partners

Direct Federation Certificates

When you enable Federation with a few partners, use your Enterprise subordinate CA. To use a certificate from your Enterprise subordinate CA, your federating partners must either trust the CA or cross-sign the certificate that you use.

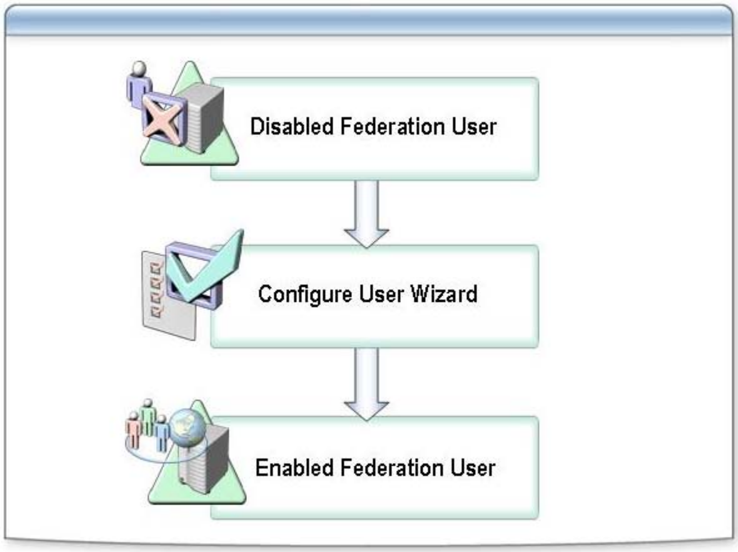
Clearinghouse Federation Certificates

When you configure your Access Proxy to use a Clearinghouse, the Clearinghouse usually issues you a certificate. Your Access Proxy server will trust the Clearinghouse CA.

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.

Enabling Users for Federation



Disabled Federation User

Configure User Wizard

Enabled Federation User

Introduction

After you have configured your Access Proxy with Federation, you must enable your internal users to communicate with Federated partners. Unless your internal users are authorized, they will not be able to take advantage of LCS 2005 with SP1 features when communicating with Federated partners.

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

To enable users for Federation, 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**.

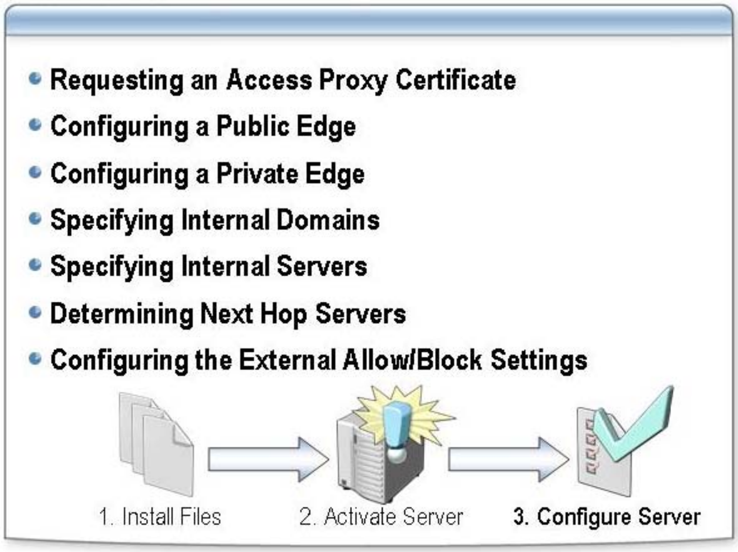
Live Communications Server Console

To enable multiple user accounts for Federation, 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 then 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 Federation** 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**.

Lesson: Configuring Access Proxy Settings for Federation



- Requesting an Access Proxy Certificate
- Configuring a Public Edge
- Configuring a Private Edge
- Specifying Internal Domains
- Specifying Internal Servers
- Determining Next Hop Servers
- Configuring the External Allow/Block Settings

Introduction

After you have deployed your Access Proxy server, you will need to configure it for Federation. The location of an Access Proxy server determines the post-setup configuration process.

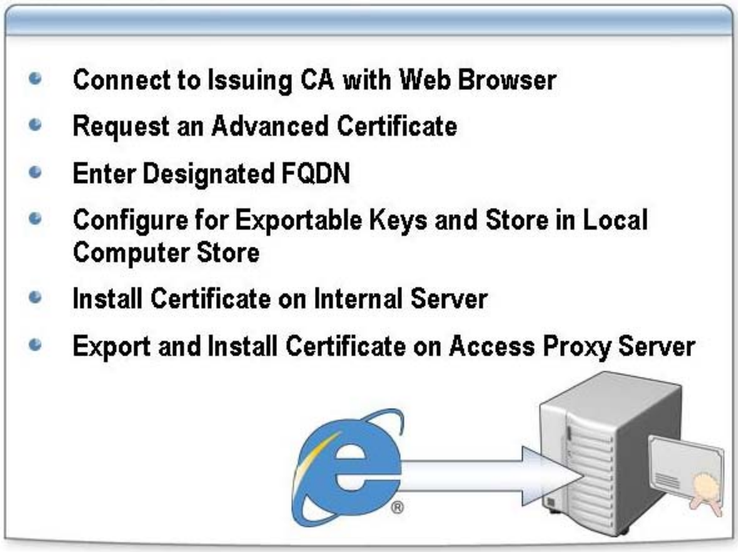
Important It is very important not to overlook the Federation configuration steps, or issues may arise, such as your users not being able to communicate properly with your Federated partner's users.

Lesson Objectives

After completing this lesson, you will be able to:

- Obtain an Access Proxy Certificate.
- Plan configuration of the Public Edge.
- Describe how to configure the Private Edge.
- Identify Internal Domains.
- Identify Internal Servers.
- Explain the Next Hop Internal Server.
- Configure the External Allow/Block Settings.
- Configure an Access Proxy server in a perimeter network.

Requesting an Access Proxy Certificate for Federation



- Connect to Issuing CA with Web Browser
- Request an Advanced Certificate
- Enter Designated FQDN
- Configure for Exportable Keys and Store in Local Computer Store
- Install Certificate on Internal Server
- Export and Install Certificate on Access Proxy Server

Introduction

To support MTLS encryption, you need to install one or more certificates on the Access Proxy server for Federation.

Windows 2003 Certificate Request

This example assumes you are obtaining a certificate from an internal Windows 2003 certificate authority. If you want to include Direct Federation with your default route to a Clearinghouse, you should obtain a public certificate.

To request a certificate, perform the following steps:

1. Log on to an internal LCS 2005 with SP1 server with administrative credentials.

> Caution Do not log on to the Access Proxy at this time.

2. Select **Start**, and then click **Run**. Type **http://<Issuing CA Server Name>/certsrv**, and then click **OK**.
3. Select **Request a Certificate**.
4. Select **Advanced certificate request**.
5. Click **Create and submit a request to this CA**.
6. In the **Certificate Template** box, click the Web Server template that you duplicated as part of the enrollment procedure for the internal LCS server.
7. Type the Fully Qualified Domain Name (FQDN) of your Access Proxy server Private Edge in the **Identifying Information** box.
8. Accept the default value in **Key Options** and check that the **CSP** is set to **Microsoft RSA SChannel Cryptographic Provider**.
9. Select the **Mark keys as exportable** check box.
10. Select the **Store certificate in the local computer certificate store** check box, and then click the **Submit** button.
11. Select **Yes** if a **Potential Scripting Violation** message box appears.

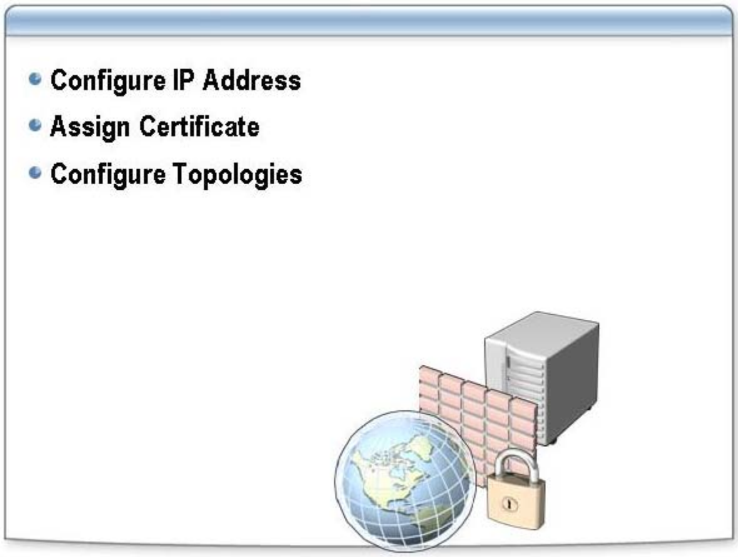
12. Install the certificate on the internal server.
13. Export the certificate to the Access Proxy server.
14. Install the certificate on the Access Proxy server.

Note A second external certificate can be obtained for a Public Edge. The external certificate will be configured with the FQDN of the Public Edge.

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 a Public Edge



- Configure IP Address
- Assign Certificate
- Configure Topologies

Introduction

A Public Edge is part of a defense-in-depth strategy that separates the Internet from your internal network. After you register your certificate(s), assign an IP address for your network interface card as well as a certificate.

After you have configured your LCS 2005 with SP2 Access Proxy, you must complete additional certificate configuration for the Access Proxy with Federation. This section discusses additional Access Proxy certificate configuration.

Determining Certificate Requirements

The Access Proxy has a public interface used for external connections and a private or internal interface for internal connections. For the external interface, a public certificate is recommended for Federation. However, a certificate issued by an internal CA is supported.

Federation requires you to download the internal issuing CA certificate chain and to download the external issuing CA certificate chain. Each CA certificate chain must be installed to the Trusted Root Certification Authorities for the local computer account. The internal and external issuing CA can be the same, for example, if both interfaces use the same internal issuing CA.

Setting IP Addresses

You may need to work with your network infrastructure team to obtain an external IP address, which you then configure on the Access Proxy server, and configure your corporate firewall to publish your Access Proxy server.

Note The Public Edge must have a static IP address.

To assign the IP address to the Public Edge, perform the following steps:

1. Log on to the Access Proxy server with administrative permissions.
2. Access the Control Panel and review the properties of the Network Connections.

3. Right-click the network interface card that you want to configure, and then select **Properties**.
4. Click **Internet Protocol (TCP/IP**), and then click **Properties**.
5. Review the **General** tab, and then click **Use the following IP address**.
6. Type the IP address you have designated for the Public Edge, and then click **OK**.

Assign Certificate

After you have configured the IP address, you can assign the certificate to the Public Edge. To do so, perform the following steps:

1. Open the **Computer Management** console, and then expand the **Services and Applications** node.
2. Right-click Microsoft Office Live Communications Server 2005, and then click **Properties**.
3. Click the **Public** tab.
4. Review the list of IP addresses and select the Public Edge IP address.
5. Click **Select Certificate**.
6. Select the certificate assigned to the Pubic Edge network interface card.
7. Click **OK**.

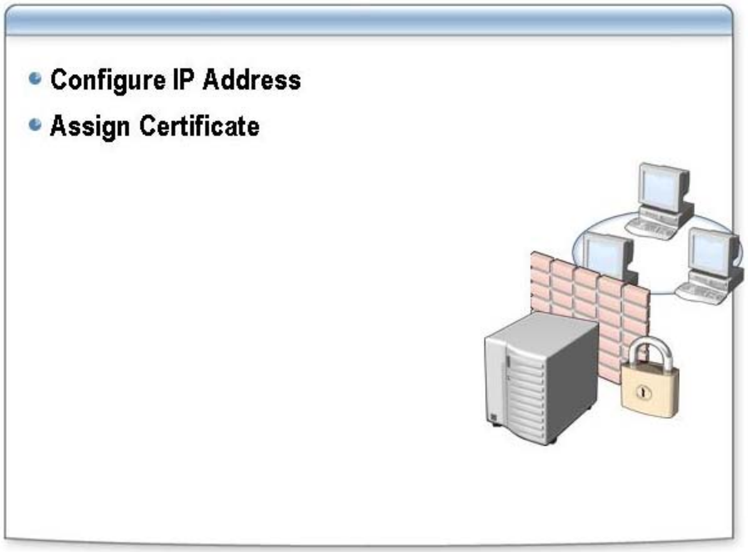
Important Before exiting from the Live Communications Server 2005 with SP1 properties, review the Configuring Topologies section below.

8. If you are not configuring topologies, click **Apply**.

Configuring Topologies

If you are planning to use multiple topologies, you can enable these features in the properties of the Live Communications Server 2005 on the Access Proxy server. On the properties of the Live Communications Server 2005 on the Access Proxy server, Federation can be enabled as well as other topologies such as Remote User Access.

Configuring a Private Edge



- Configure IP Address
- Assign Certificate

Introduction

A Private Edge supports the outbound SIP traffic from your corporate users. After you have registered your certificate(s), assign an IP address for your network interface card as well as a certificate.

When you have configured your Access Proxy with Federation, you must complete additional certificate configuration for the Access Proxy. This section discusses additional Access Proxy certificate configuration.

The Access Proxy has a public interface used for external connections and a private or internal interface for internal connections. You can use a private certificate on the internal interface if your company has deployed an internal CA. This configuration allows you to communicate with the internal servers.

Note The Private Edge must have a static IP address.

Determining IP Address

You may need to work with your network infrastructure team to obtain a static IP address that can be configured on the Access Proxy server.

To assign the IP address to the Private Edge, perform the following steps:

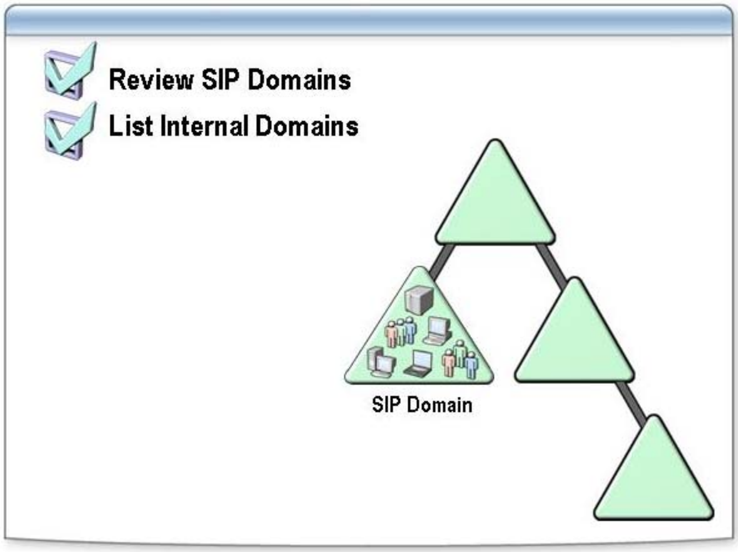
1. Log on to the Access Proxy server with administrative permissions.
2. Access the Control Panel and review the properties of the Network Connections.
3. Right-click the network interface card that you want to configure, and then select **Properties**.
4. Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. Review the **General** tab and click **Use the following IP address**.
6. Type the IP address you have designated for the Private Edge, and then click **OK**.

Assign Certificate

After you have configured the IP address, you can assign the certificate to the Private Edge. To do so, perform the following steps:

1. Open the **Computer Management** console, and then expand the **Services and Applications** node.
2. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
3. Click the **Private** tab.
4. Review the list of IP addresses and select the Private Edge IP address.
5. Click **Select Certificate**.
6. Select the certificate assigned to the Private Edge network interface card.
7. Click **OK**.
8. Click **Apply**.

Specifying Internal Domains


Review SIP Domains

List Internal Domains

Introduction

Every Live Communications Server 2005 with SP1 deployment includes global settings. These global settings define the overall configuration of the system.

When you add an Access Proxy into the LCS 2005 with SP1 environment, you need to specify the internal SIP domain(s) manually. An Access Proxy server will not query Active Directory for the overall configuration information, because it is designed to be joined to a workgroup instead of a domain.

Note If your Access Proxy is joined into a domain, it still will not query Active Directory information.

You can review the list of internal SIP domains(s) in the global settings.

Review SIP Domains

A Live Communications Server 2005 with SP1 infrastructure relies on your Active Directory configuration. You can have multiple LCS 2005 with SP1 domains in your Active Directory Forest.

If you are not aware of all your internal SIP domains that include an installation of LCS 2005 with SP1, you can obtain the list by performing the following steps:

1. Log on to a Live Communications Server on your internal network.

Note Do not carry out this procedure on the Access Proxy server.

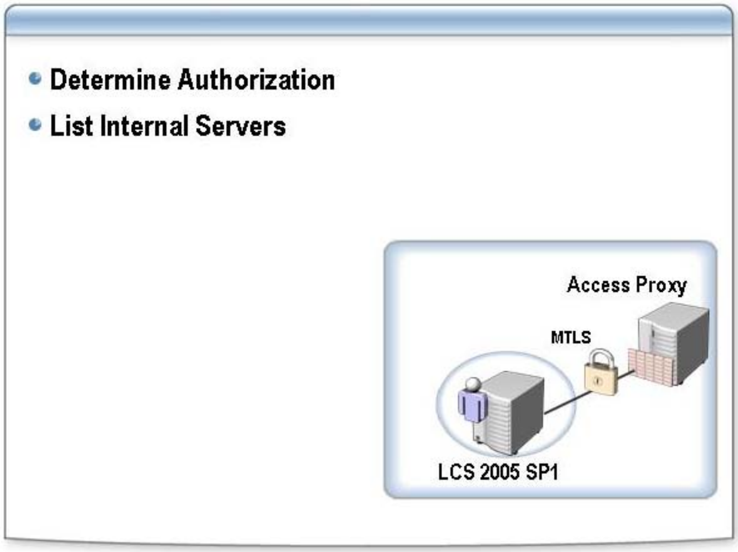
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005**.
3. Right-click the **Forest** node, and then select **Properties**.
4. Review the **Internal** tab for the list of internal SIP domains.
5. Click **Cancel**.

List Internal Domains

If you have multiple internal domains, you must to specify each one. To do so, perform the following steps:

1. Log on to the Access Proxy server with administrative permissions.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**.
3. In the **Computer Management** console, expand the **Services and Applications** node.
4. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
5. Click the **Internal** tab.
6. Click **Add Domain** in the **Internal SIP domains supported by Live Communications servers in your organization** section.
7. Click **OK** to close the **Add SIP Domain** dialog box.
8. Repeat the **Add Domain** process until you have added each SIP domain.
9. Click **OK** to close the **Microsoft Office Live Communications Server 2005 Properties** dialog box.

Specifying Internal Servers



- Determine Authorization
- List Internal Servers

Introduction

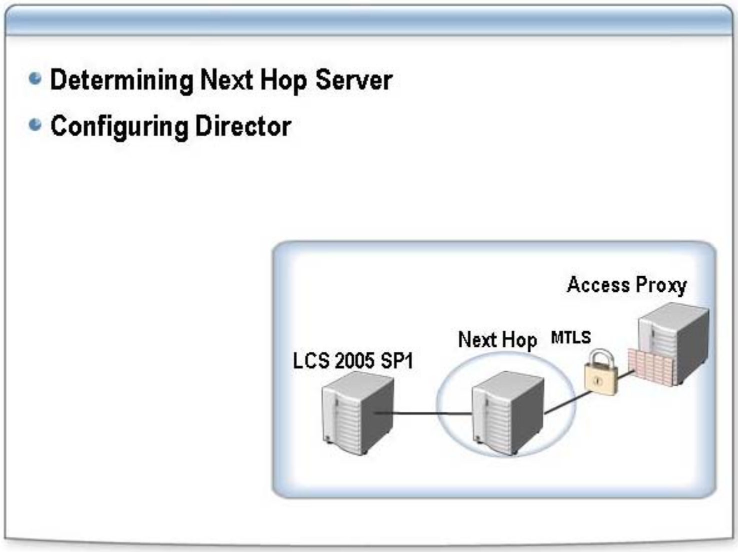
By design, an Access Proxy server enforces security since it is located in a perimeter network and maintains a list of internal servers authorized to communicate with it. You can specify which internal servers can connect directly with an Access Proxy server.

List Internal Servers

If you have multiple internal servers, you need to specify each one. To do so, perform the following steps:

1. Log on to the Access Proxy server with administrative permissions.
2. Open the **Computer Management** console and expand the **Services and Applications** node.
3. Right-click **Microsoft Office Live Communications Server 2005**, and then select **Properties**.
4. Click the **Internal** tab.
5. Click **Add Server** in the **Internal servers authorized to connect to this Access Proxy server** section.
6. Type the **Server name** in FQDN form for the computer that is allowed to communicate with this Access Proxy server.
7. Click **OK** in the **Add Live Communications Server** dialog box.
8. Repeat the **Add Server** process until each designated internal SIP server is added.
9. Click **OK** to close the **Microsoft Office Live Communications Server 2005 Properties** dialog box.

Determining Next Hop Servers



- Determining Next Hop Server
- Configuring Director

Introduction

When an Access Proxy server accepts incoming SIP traffic, this traffic must be delivered to the internal network. You will need to designate a Next Hop server.

Next Hop Server

A Next Hop server can be an internal LCS 2005 with SP1 server. Alternatively, the Next Hop server could be the Director server role, introduced with Live Communications Server 2005 with SP1.

Director Server

A Director server can act as the second line of defense when deploying Federation or Remote Access to LCS 2005 with SP1. The Director server sits behind the corporate network perimeter between the Access Proxy and the pool server in the internal network. Directors are part of the corporate Active Directory infrastructure.

Important It is recommended that you implement a Director server to provide an extra layer of security.

If you decide to implement a Director, the Director provides authentication against Active Directory for traffic forwarded from the Access Proxy server.

Note A Director does not host users. Its only function is for authentication purposes.

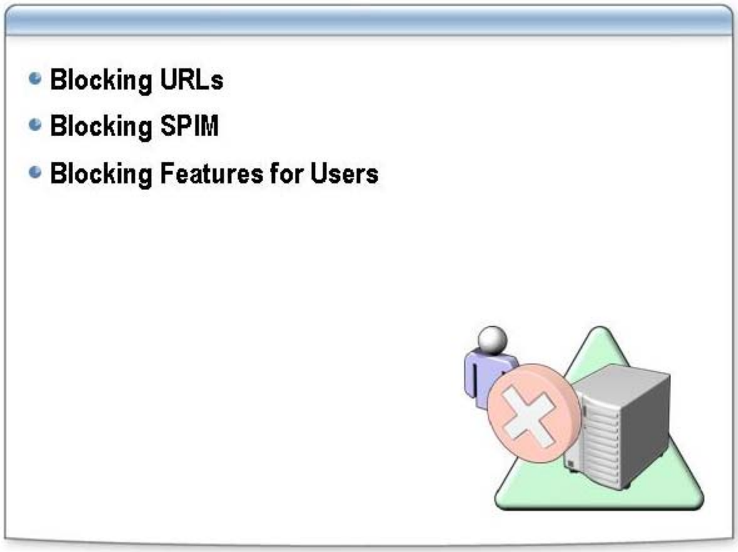
Configure Next Hop Server

To configure the Next Hop server, perform the following steps:

1. Log on to the Access Proxy server with administrative permissions.
2. Open the **Computer Management** console, and expand **Services and Applications**.
3. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
4. Click the **Internal** tab.

5. Review the **Next hop network address** and then either type:
    a. The FQDN of the Director server.
    b. The FQDN of an internal LCS 2005 with SP1 server or Enterprise pool.
2. In the **Port** box, type **5061**.
3. Click **OK** to close the **Microsoft Office Live Communications Server 2005 Properties** dialog box.

Configure the External Allow/Block Settings



- **Blocking URLs**
- **Blocking SPIM**
- **Blocking Features for Users**

Introduction

Many security enhancements are available for an LCS 2005 with SP1 Access Proxy server. Security enhancements include:

- Blocking attacks
- Blocking unsolicited messages (SPIM)
- Blocking features at a user level

Blocking Attacks

The IM URL Filter Application (IMFilter.am) utility blocks URLs from being sent directly to an Office Communicator or Windows Messaging client. This utility installs on the following servers:

- LCS 2005 with SP1, Standard Edition
- LCS 2005 with SP1, Enterprise Edition
- Director
- Access Proxy

Note There is an improved version of the Intelligent Instant Message Filter available for download from the Microsoft.com Web site, at: http://www.microsoft.com/downloads/details.aspx?familyid=0ED13372-F3D2-40F0-BA5D-C880359A40F5.

Users can still send a URL that is intended for business use by including an underscore symbol (_) before the URL link. If an underscore and URL appears in an instant messaging conversation, the receiving user must:

- Start a browser session.
- Copy the URL link.
- Paste the URL link into browser window.
- Remove the underscore character.

Important By default, the IM URL Filter utility is enabled and it will block file transfers. It is recommended that you accept the default settings.

Blocking SPIM

You can control SPIM by filtering it based on rules you define in a LCS 2005 with SP1 deployment. The SPIM filters can differ between the following topologies:

- Federation
- Public IM Connectivity

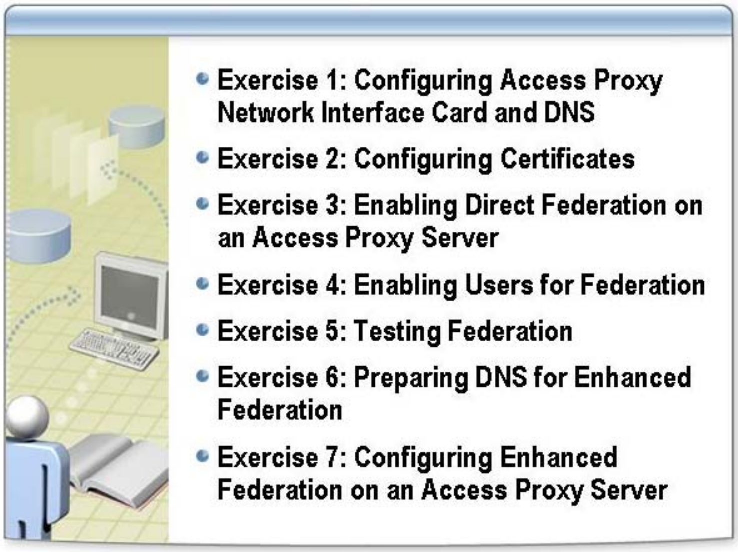
The Access Proxy server reviews the message filter settings and then accepts or rejects the incoming messages based on user verification of the sender.

Blocking Features for Users

There may be a requirement for you to block a user or group of users from using the features of LCS 2005 with SP1. To block users from participating in Federation, Public IM Connectivity, or Remote User access, perform the following steps:

1. Log on to an internal LCS 2005 with SP1 server.
2. Expand the **Forest** node, expand the **Domain** node, and expand the domain that contains the users you want to configure.
3. Expand the **Live Communications servers and pools** node.
4. On either the Enterprise Pool or the LCS server node, select the **Users** container.
5. Right-click the user(s) you want to configure, and then click **Configure Users**. The **Configure Live Communications Server Users Wizard** appears.
6. Check **Configure Federation**.
7. For each selected option, check **Block Users**.
8. Click **Next**.
9. Check that the operation completes successfully, then click **Finish**.

Lab 8: Configuring Access Proxy for Direct Federation and Enhanced Federation



- Exercise 1: Configuring Access Proxy Network Interface Card and DNS
- Exercise 2: Configuring Certificates
- Exercise 3: Enabling Direct Federation on an Access Proxy Server
- Exercise 4: Enabling Users for Federation
- Exercise 5: Testing Federation
- Exercise 6: Preparing DNS for Enhanced Federation
- Exercise 7: Configuring Enhanced Federation on an Access Proxy Server

Objectives

After completing this lab, you will be able to:

- Configure Access Proxy network interface card and DNS for Direct Federation.
- Configure certificates for Federation.
- Configure an Access Proxy server for Direct Federation capabilities.
- Enable users for Federation.
- Test communication between federated partners.
- Set up DNS for Enhanced Federation.
- Configure an Access Proxy server for Enhanced Federation capabilities.

Estimated time to complete this lab: **50 minutes**

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

Introduction

Fabrikam and NWTraders have entered into a partnership arrangement that requires selected employees from both companies to co-operate closely. Both companies run LCS 2005 with SP1, so are able to use Federation to implement secure IM communications. Matt Dawson and Holly Holt have been tasked with the job of setting up Federation between the organizations.

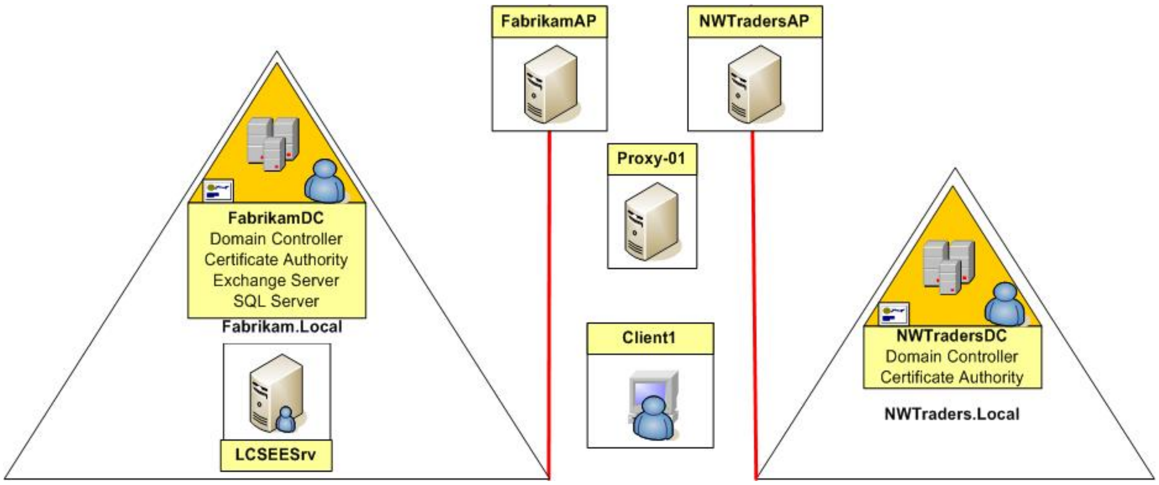
In this lab, you will prepare your Access Proxy server and your internal SIP domain for Direct Federation and Enhanced Federation. You will also configure your ports for client access. After configuring your Access Proxy server, you will configure your internal SIP domain.

Your internal SIP domain will require a list of Access Proxy server(s) installed on your perimeter network as well as enabling each user for Federation privileges.

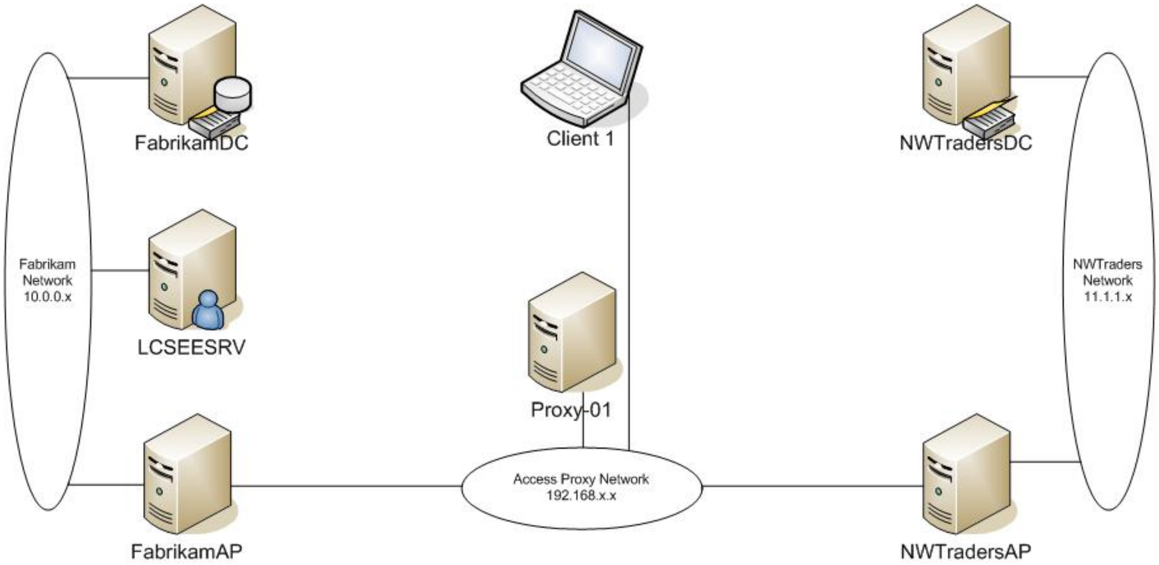
Federation should only be enabled after a Standard or Enterprise Edition Live Access Proxy server has been implemented with Remote User Access enabled in your perimeter network environment.

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


FabrikamDC
Client 1
NWTradersDC
Fabrikam Network 10.0.0.x
LCSEESRV
NWTraders Network 11.1.1.x
Proxy-01
Access Proxy Network 192.168.x.x
FabrikamAP
NWTradersAP

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 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
7034A-LCSEESRV-B	LCSEESRV
7034A-NWTradersDC-B	NWTradersDC
7034A-NWTradersAP-B	NWTradersAP
7034A-Proxy01-B	Proxy-01
7034A-Client1-B	Client1

Important: You should start all these virtual PC images prior to commencing the labs in this module. Some images may already be started from the previous lab.

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

Exercise 1
Configure Access Proxy Network Interface Card and DNS

Scenario

Both Matt and Holly need to configure the Public Edge network cards on their respective Access Proxies to obtain DNS information from an external DNS server. They then need to add the DNS records to enable Direct Federation.

Description

In this exercise, you configure the FabrikamAP and NWTradersAP network cards to obtain DNS information from Proxy-01. You then configure DNS on FabrikamDC and NWTradersDC for Direct Federation.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-FabrikamAP-B.	
1. Configure external network card for FabrikamAP Access Proxy server.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Control Panel**, point to **Network Connections**, right-click **Local Area Connection 2**, and then click **Properties**. **c.** In the **Local Area Connection 2 Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**. **d.** In the **Internet Protocoal (TCP/IP) Properties** dialog box, in the **Use the following DNS server addresses** section, in the **Preferred DNS server** box, type **192.168.0.30**, and then click **OK**. **e.** On the **Local Area Connection 2 Properties** dialog box, click **Close**.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersAP-B.	
2. Configure external network card for NWTradersAP Access Proxy server.	**a.** Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Control Panel**, point to **Network Connections**, right-click **Local Area Connection 2**, and then click **Properties**. **c.** In **Local Area Connection 2 Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**. **d.** In the **Internet Protocoal (TCP/IP) Properties** dialog box, in the **Use the Following DNS Server Addresses** section, in the **Preferred DNS server** box, type **192.168.0.30**, and then click **OK**. **e.** In **Local Area Connection 2 Properties** dialog box, click **Close**.
⚠ **Important:** Perform this exercise on the 7034A-FabrikamDC-B.	
3. Configure DNS on FabrikamDC for Direct Federation.	**a.** Log on to **7034A-FabrikamDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **DNS**.

	c. In the **dnsmgmt** console, expand **Forward Lookup Zones**. **d.** Right-click **fabrikam.local**, and then click **Other New Records**. **e.** In the **Resource Record Type** dialog box, click **Service Location (SRV)**, and then click **Create Record**. **f.** In the **New Resource Reload** dialog box, in the **Service** box, type **_sip_tls**. **g.** In the **Port number** box, type **5061**. **h.** In the **Host offering this service** box, type **FabrikamAP.Fabrikam.local**, and then click **OK**. **i.** Click **Create Record**. **j.** In the **Recourse Record Type** dialog box, click **Done**.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersDC-B.	
4. Configure DNS on NWTradersDC for Direct Federation.	**a.** Log on to **7034A-NWTradersDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **DNS**. **c.** In the **dnsmgmt** console, expand **Forward Lookup Zones**. **d.** Right-click **NWTraders.local**, and then click **Other New Records**. **e.** In the **Resource Record Type** dialog box, click **Service Location (SRV)**, and then click **Create Record**. **f.** In the **New Resource Record** dialog box, in the **Service** box, type **_sip_tls**. **g.** In the **Port number** box, type **5061**. **h.** In the **Host offering this service** box, type **NWTradersAP.NWTraders.local**, and then click **OK**. **i.** In the **Recourse Record Type** dialog box, click **Done**.

Exercise 2
Configure Certificates for Federation

Scenario

Enabling any Federation model requires configuration of certificates so that the Access Proxy servers can establish encrypted communications. Holly and Matt must add each other's certificate chain into their respective trusted root certificates store on both Access Proxies. This exchange of certificates allows Fabrikam to trust certificates issued by NWTraders, and NWTraders to trust certificates issued by Fabrikam.

Description

In this exercise, you exchange certificate chains between FabrikamAP.Fabrikam.local and NWTradersAP.NWTraders.local.

Tasks	**Detailed Steps**
⚠ **Important:** Perform this exercise on the 7034A-FabrikamAP-B.	
1. Configure certificate on FabrikamAP.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, and then click **Run**. **c.** In the **Open** box, type **cmd**, and then click **OK**. **d.** At the command prompt, type **Net Use Z: \\NWTradersAP\c$**, and then press ENTER. **e.** Click **Start**, and then click **Run**. **f.** On the **Open** box, type **mmc**, and then click **OK**. **g.** On the **Microsoft Management Console**, click **File**, and then click **Add/Remove Snap-in**. **h.** On the **Add/Remove Snap-in** page, click **Add**. **i.** In the **Add Standalone Snap-in** dialog box, in the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**. **j.** In the **Certificates Snap-in** dialog box, click **Computer account**, and then click **Next**. **k.** In the **Select Computer** dialog box, verify that **Local computer** is selected, and then click **Finish**. **l.** In the **Add Standalone Snap-in** dialog box, click **Close**. **m.** On the **Add/Remove Snap-in** page, click **OK**. **n.** In the **Certificates** console, expand **Certificates (Local Computer)**. **o.** Expand **Trusted Root Certification Authorities**. **p.** Right-click **Certificates**, point to **All Tasks**, and then click **Import**. **q.** On the **Welcome to the Certificate Import Wizard** page, click **Next**. **r.** On the **File to Import** page, click **Browse**. **s.** On the **Open** page, in the **File name** box, type **Z:\SE_Chain.p7b**, and then click **Open**.

	t. On the **File to Import** page, click **Next**. **u.** On the **Certificate Store** page, ensure that the default value is selected for **Place all certificates in the following store**. *Verify that the Trusted Root Certification Authorities option is displayed for the Certificate store.* **v.** Click **Next**. **w.** On the **Completing the Certificate Import Wizard** page, click **Finish**. **x.** On the **Certificate Import Wizard** message box, click **OK**. **y.** Close the command prompt and the management console. Do not save changes on the management console.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersAP-B.	
2. Configure certificates on NWTradersAP.	**a.** Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, and then click **Run**. **c.** In the **Open** box, type **cmd**, and then click **OK**. **d.** At the command prompt, type **Net Use Z: \\FabrikamAP\c$**, and then press ENTER. **e.** Click **Start**, and then click **Run**. **f.** In the **Open** box, type **mmc**, and then click **OK**. **g.** In the **Microsoft Management Console**, click **File**, and then click **Add/Remove Snap-in**. **h.** On the **Add/Remove Snap-in** page, click **Add**. **i.** In the **Add Standalone Snap-in** dialog box, in the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**. **j.** On the **Certificates Snap-in** page, click **Computer account**, and then click **Next**. **k.** On the **Select Computer** page, ensure that **Local Computer** is selected, and then click **Finish**. **l.** In the **Add Standalone Snap-in** dialog box, click **Close**. **m.** On the **Add/Remove Snap-in** page, click **OK**. **n.** In the **Certificates** console, expand **Certificates (Local Computer)**. **o.** Expand **Trusted Root Certification Authorities**. **p.** Right-click **Certificates**, point to **All Tasks**, and then click **Import**. **q.** On the **Welcome to the Certificate Import Wizard** page, click **Next**. **r.** On the **File to Import** page, click **Browse**. **s.** On the **Open** page, in the **File name** box, type **Z:\EE_Chain.p7b**, and then click **Open**. **t.** On the **File to Import** page, click **Next**. **u.** On the **Certificate Store** page, ensure that the default value is selected for **Place all certificates in the following store**. *Verify that the Trusted Root Certification Authorities option is displayed for the Certificate store.* **v.** Click **Next**.

	w. On the **Completing the Certificate Import Wizard** page, click **Finish**. **x.** On the **Certificate Import Wizard** message box, click **OK**. **y.** Close the command prompt and the management console. Do not save changes on the management console.

Exercise 3
Enable Direct Federation on an Access Proxy Server

Scenario

Now that Matt and Holly have exchanged certificate chains, they must both configure Direct Federation. They have to make these configuration changes at the Forest level on the internal LCS computers. Since they are using Direct Federation, they also have to specify the domain name and the Access Proxy address for each other's Access Proxy and domain.

Description

In this exercise, you enable Direct Federation settings on the Fabrikam and NWTraders Forests, and on the Fabrikam and NWTraders Access Proxies.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-LCSEESRV-B.	
1. Enable Direct Federation on internal LCS 2005 with SP1 server.	**a.** Log on to **7034A-LCSEESRV-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Live Communications Server 2005**. **c.** In the **Microsoft Office Live Communications Server 2005** console, right-click **Forest – fabrikam.local**, and then click **Properties**. **d.** On the **Live Communications Server Global Properties** dialog box, click the **Federation** tab, and then click **Enable federation and public IM connectivity**. **e.** In the **Network address** box, type **FabrikamAP.Fabrikam.local**, and then click **OK**. **f.** Close the Microsoft Office Live Communications Server 2005 management console.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersDC-B.	
2. Enable Direct Federation on internal LCS 2005 with SP1 server.	**a.** Log on to **7034A-NWTradersDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Live Communications Server 2005**. **c.** In the **Microsoft Office Live Communications Server 2005** console, right-click **Forest – NWTraders.local**, and then click **Properties**. **d.** On the **Live Communications Server Global Properties**, click the **Federation** tab, and then click **Enable federation and public IM connectivity**. **e.** In the **Network address** box, type **NWTradersAP.NWTraders.local**, and then click **OK**.

	f. Close the Microsoft Office Live Communications Server 2005 management console.
⚠ **Important:** Perform this exercise on the 7034A-FabrikamAP-B.	
3. Enable Direct Federation on FabrikamAP.	**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.** In the **Computer Management** console, expand **Services and Applications**, right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**. **d.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, on the **General** tab, click **Federate with other domains**. **e.** On the **Public** tab, under **Listening ports**, click the existing entry, and then click **Edit**. **f.** In the **Edit Listening Port** dialog box, select the **Allow server connections for federation or branch offices** check box, and then click **OK**. **g.** On the **Allow** tab, click **Add**. **h.** In the **Add Federated Partner** dialog box, in the **Federated partner Access Proxy** box, type **NWTradersAP.NWTraders.local**. **i.** In the **Federated partner domain name** box, type **NWTraders.local**. **j.** Under **Select an option for filtering incoming communications**, click **Allow all communications from this federated partner**. **k.** On the **Add Federated Partner** dialog box, click **OK**. **l.** On the **Microsoft Office Live Communications Server 2005 Properties** dialog box, click **OK**. **m.** Close the Computer Management console.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersAP-B.	
4. Enable Direct Federation on FabrikamAP.	**a.** Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Computer Management**. **c.** In the **Computer Management** console, expand **Services and Applications**, right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**. **d.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, on the **General** tab, click **Federate with other domains**. **e.** On the **Public** tab, under **Listening ports**, click the existing entry, and then click **Edit**. **f.** On the **Edit Listening Port** dialog box, select the **Allow server connections for federation or branch office** check box, and then click **OK**.

	g. On the **Allow** tab, click **Add**. **h.** On the **Add Federated Partner** dialog box, in the **Federated partner Access Proxy** box, type **FabrikamAP.Fabrikam.local**. **i.** In the **Federated partner domain name** box, type **Fabrikam.local**. **j.** Under **Select an option for filtering incoming communications**, click **Allow all communications from this federated partner**. **k.** On the **Add Federated Partner**, click **OK**. **l.** On the **Microsoft Office Live Communications Server 2005 Properties**, click **OK**. **m.** Close the Computer Management console.

Exercise 4
Enabling Users for Federation

Scenario

Holly and Matt have successfully configured the server settings for Direct Federation. Their next task is to enable their respective users for Federation. During the testing phase, Holly only wants to enable herself.

Description

In this exercise, you will configure users to participate in Federation.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
1. Configure Fabrikam.local federated users	**a.** Log on to **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 **Active Directory Users and Computers** console, expand **fabrikam.local**, and then click the **LCSUsers** organizational unit. **d.** Select all five users in the organization unit, right-click the users, and then click **Configure Live Communications Users**. **e.** On the **Welcome to the Configure User Wizard** page, click **Next**. **f.** On the **Configure User Settings** page, click **Configure Federation**. **g.** Ensure that **Allow Users** is selected. **h.** On the **Configure User Setting** page, click **Next**. **i.** On the **Configure Operation Status** page, wait for all operations to succeed, and then click **Finish**. **j.** Close Active Directory Users and Computers.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersDC-B virtual machine.	
2. Configure NWTraders.local federated user.	**a.** Log on to **7034A-NWTradersDC-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 **Active Directory Users and Computers** console, expand **NWTraders.local**, and then click the **Users** organizational unit. **d.** In the **Users organizational unit**, right-click **Holly Holt**, and then click **Configure Live Communications Users**. **e.** On the **Welcome to the Configure User Wizard** page, click **Next**. **f.** On the **Configure User Settings** page, click **Configure Federation**.

	g. Ensure that **Allow Users** is selected. **h.** On the **Configure User Settings** page, click **Next**. **i.** On the **Configure Operation Status** page, wait for all operations to succeed, and then click **Finish**. **j.** Close Active Directory Users and Computers.

Exercise 5
Test Federation

Scenario

Holly and Matt have enabled their respective users for Federation. Now they want to see if they can establish communications between Fabrikam and NWTraders. Matt is especially eager to see if he can connect as a remote user and IM someone from the federated organization.

Description

In this exercise, you will send a test instant message between the LCS 2005 with SP1 domains.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-Client1-B virtual machine.	
1. Login as the internal Fabrikam.local LCS 2005 with SP1 user.	**a.** Log on to **7034A-Client1-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **All Programs**, and then click **Microsoft Office Communicator 2005**. **c.** Log on to **Microsoft Office Communicator** as **matt@fabrikam.local** with a password of **pass@word1**.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersDC-B virtual machine.	
2. Login as the internal NWTraders.local LCS 2005 with SP1 user.	**a.** Log on to **7034A-NWTradersDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **All Programs**, and then click **Windows Messenger**. **c.** In the **Sign In to a SIP Communications Service** dialog box, ensure that the **Sign-in name** and **User name** boxes are set to **holly@nwtraders.local**. **d.** In the **Password** box, type **pass@word1**, and then click **OK**. **e.** **Holly Holt** should now appear with a status of **Online**.
3. Add a contact to your contact list.	**a.** On Windows Messenger, click **Tools**, and then click **Add a Contact**. **b.** On the **Add a Contact** dialog box, click **By e-mail address or sign-in name**, and then click **Next**. **c.** On the **Add a Contact** dialog box, type **matt@fabrikam.local**, and then click **Next**. **d.** On the **Success!** page, click **Finish**.
⚠ **Important:** Perform this exercise on the 7034A-Client1-B virtual computer.	
4. Accept the pop-up to allow your federated partner in the contact list.	**a.** Switch to the **7034A-Client1-B** virtual machine. **b.** On the **Communicator** prompt, click **Allow this person to see when you are online and contact you**, ensure the **Add this person to my**

	contact list check box is selected, and then click **OK**. **c.** Right-click Holly Holt's instant messaging presence, and then click **Send An Instant Message**. **d.** On the **User Name – Conversation** page, type **Hey, Holly, we did it!**, and then click **Send**. **e.** Note that a warning appears, alerting you to the fact that parties in this conversation may be archiving the instant messages.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersDC-B virtual computer.	
5. Verify instant message test.	**a.** Switch to the **7034A-NWTradersDC-B** virtual PC. **b.** Verify that the test instant message pop-up has been received. **c.** Reply to Matt's message to check communications in both directions.

Exercise 6
Preparing Domain Name Service (DNS) for Enhanced Federation

Scenario

Enhanced Federation uses DNS SRV resolution to locate external SIP domains. Restricted Enhanced Federation allows connections only with specified domains, whereas Unrestricted Enhanced Federation allows connections with any SIP domain that presents a valid certificate. The default setting for Enhanced Federation is Restricted Enhanced Federation.

Description

In this exercise, you will configure DNS for Fabrikam to support Enhanced Federation.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-Proxy01-B virtual computer.	
1. Configure DNS for Enhanced Federation for Fabrikam.local.	**a.** Log on to **7034A-Proxy01-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **DNS**. **c.** In the dnsmgmt console, expand **PROXY-01**, and then expand **Forward Lookup Zones**. **d.** Click **Fabrikam.local**, right-click **Fabrikam.local**, and then click **Other New Records**. **e.** In the **Resource Record Type** dialog box, in the **Select a resource record type** list, click **Service Location(SRV)**, and then click **Create Record**. **f.** In the **New Resource Record** dialog box, in the **Service** box, type **_sipfederationtls**. **g.** In the **Port number** box, type **5061**. **h.** In the **Weight** box, type **100**. **i.** In the **Host offering this service** box, type **FabrikamAP.Fabrikam.local**, and then click **OK**. **j.** In the **Resource Record Type** dialog box, click **Done**.
⚠ **Important:** Perform this exercise on the 7034A-Proxy01-B virtual computer.	
2. Configure DNS for Enhanced Federation for Northwind Traders.	**a.** In the dnsmgmt console, click **NWTraders.local**. **b.** Right-click **NWTraders.local**, and then click **Other New Records**. **c.** In the **Resource Record Type** dialog box, in the **Resource Record Type** list, click **Service Location(SRV)**, and then click **Create Record**. **d.** In the **New Resource Record** dialog box, in the **Service** box, type **_sipfederationtls**.

	e. In the **Port number** box, type **5061**. **f.** In the **Weight** box, type **100**. **g.** In the **Host offering this service** box, type **NWTradersAP.NWTraders.local**, and then click **OK**. **h.** In the **New Resource Record** dialog box, click **Done**.

Exercise 7

Configuring Enhanced Federation on an Access Proxy Server

Scenario

Now that you have prepared DNS for Enhanced Federation, you must enable Enhanced Federation and configure each Access Proxy's Allow List. When you enable Enhanced Federation, Restricted Enhanced Federation is selected by default. Therefore, you must have at least one entry in your Allow List or Enhanced Federation will not work properly.

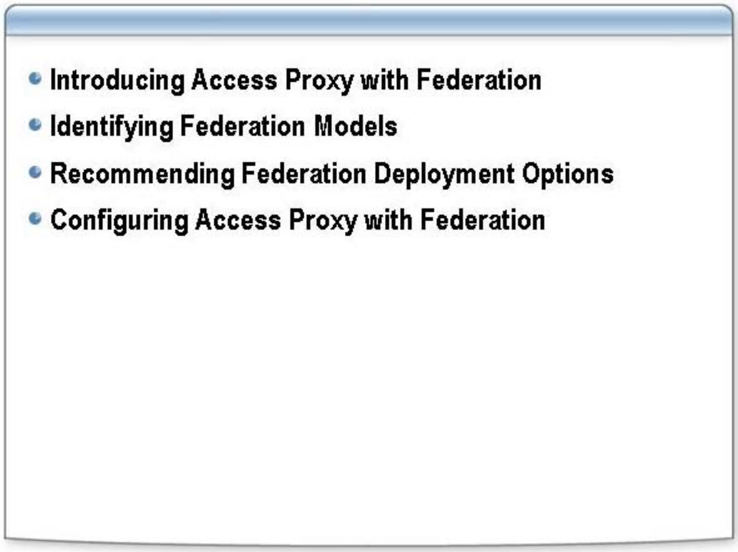
Description

In this exercise, you will configure the FabrikamAP for Enhanced Federation and allow Northwind Traders as a Federation partner.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the internal 7034A-FabrikamAP-B virtual computer.	
1. Enable Enhanced Federation on Fabrikam's Access Proxy server.	**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.** In the **Computer Management** console, expand **Services and Applications**, right-click **Live Communications Server 2005**, and then click **Properties**. **d.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, on the **Enhanced Federation** tab, select the **Enable enhanced federation** check box. **e.** Click **Allow only federation domains listed below** to enable Enhanced Federation with Northwind Traders. **f.** On the **Enhanced Federation** tab, click **Add**. **g.** In the **Add Allowed Enhanced Federation Domain** dialog box, in the **Domain Name** box, type **NWTraders.local**, and click **OK**. **h.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, click **OK**. **i.** Close the Computer Management console.
⚠ **Important:** Perform this exercise on the 7034A-NWTradersAP-B virtual computer.	
2. Enable Enhanced Federation on Northwind Traders's Access Proxy server.	**a.** Log on to **7034A-NWTradersAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Computer Management**. **c.** In the **Computer Management** console, expand **Services and Applications**, right-click **Live Communications Server 2005**,

	and then click **Properties**. **d.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, on the **Enhanced Federation** tab, select the **Enable enhanced federation** check box. **e.** Click **Allow only federation domains listed below** to enable Enhanced Federation with Northwind Traders. **f.** On the **Enhanced Federation** tab, click **Add**. **g.** In the **Add Allowed Enhanced Federation Domain** dialog box, in the **Domain Name** box, type **NWTraders.local**, and then click **OK**. **h.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, click **OK**. **i.** Close the Computer Management console. **j.** **DO NOT** close down the VPC images, but leave them running for Lab 9.

Review



- Introducing Access Proxy with Federation
- Identifying Federation Models
- Recommending Federation Deployment Options
- Configuring Access Proxy with Federation

In this module, you learned that the Access Proxy server with Federation can be configured with the following models:

- Enhanced Federation
  - Restricted Enhanced Federation
  - Unrestricted Enhanced Federation
- Direct Federation
- Clearinghouse
  - Default Route
  - Act as Clearinghouse

You also learned that special considerations must be identified before choosing a Federation model. Your decision for choosing your Federation model could be a technical or business reason.

In the next module, you will learn how to configure your Access Proxy server for Public IM Connectivity. Public IM Connectivity provides encrypted communications between your users and members of AOL, Yahoo!, and MSN.