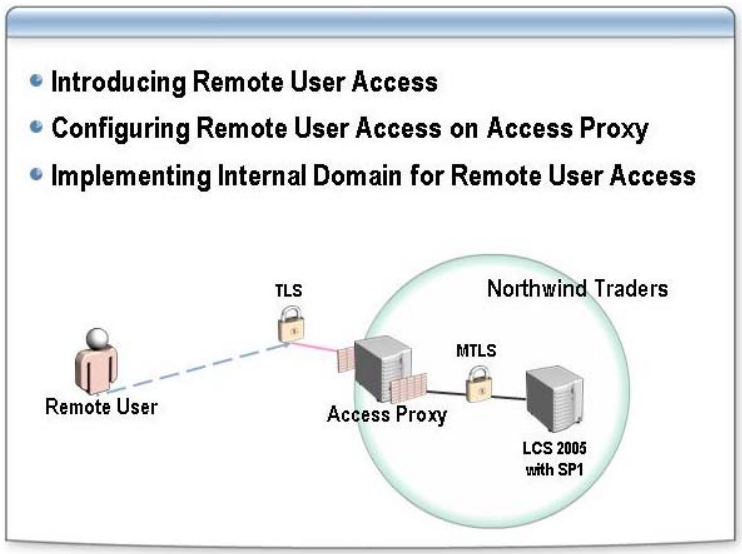
Microsoft®

Module 7: Implementing Remote User Access with Live Communications Server 2005 with SP1

Contents

Overview



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 remote users. Remote User Access enables remote or roaming users of your organization to access Live Communications Servers from outside your intranet without using a Virtual Private Network (VPN) connection.

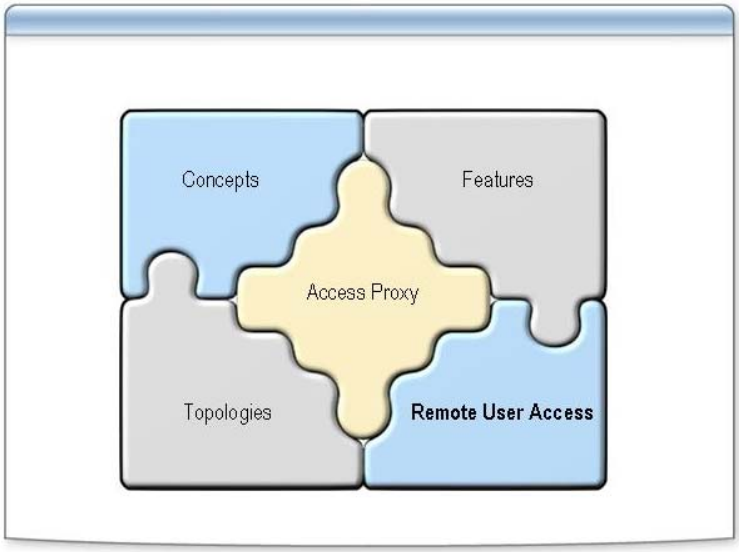
Note An Access Proxy server is required if you plan to support remote users.

Objectives

After completing this module, you will be able to:

- Describe concepts, features, and topologies of a Remote User Access implementation.
- Explain how to configure an Access Proxy server for Remote User Access capabilities.
- Prepare the internal domain for Remote User Access.

Lesson: Introducing Remote User Access



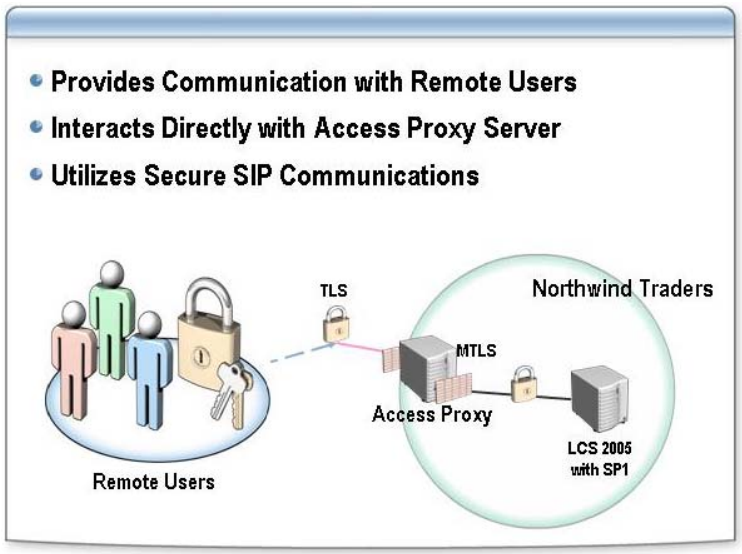
Lesson objectives

This lesson introduces Remote User Access, which is available with either LCS 2005 with SP1 Standard or Enterprise Editions. This lesson describes the concepts, features, and topologies of Remote User Access.

After completing this lesson, you will be able to:

- Describe the concepts of LCS 2005 with SP1 Remote User Access.
- Explain the features of Remote User Access.
- Identify a Remote User Access topology.
- Plan a Remote User Access deployment.
- Describe concepts, features, and topologies of a Remote User Access implementation.

What Is Remote User Access?



Remote User Access

LCS 2005 with SP1 enables remote users, such as those who work at home or on the road, to access your organization's internal SIP domains.

You can configure the Remote User Access feature on an Access Proxy server. After configuring Remote User Access, your organization’s users will be able to connect to internal Live Communications Servers from an external location.

Access Proxy Connection

Remote users connect directly to the corresponding Access Proxy server. Direct network connectivity between your internal networks to your remote users is not recommended. An Access Proxy server provides an additional layer of network security for your remote and internal users.

Secure SIP Connections

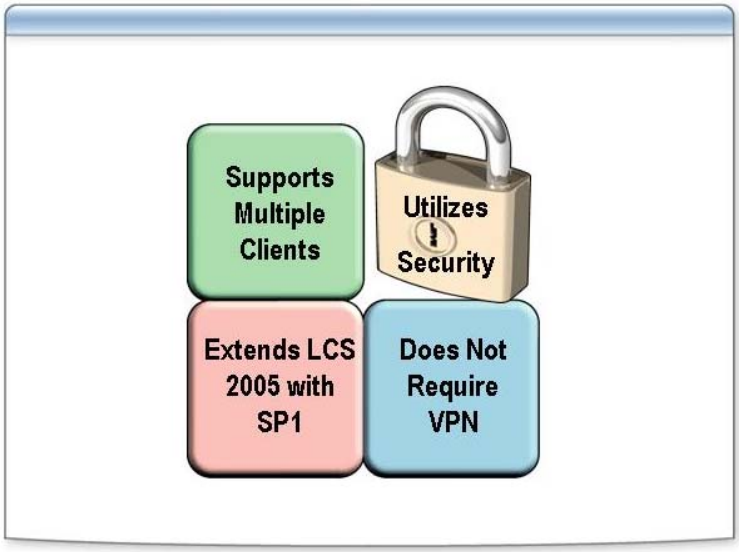
The Access Proxy server can be configured to allow only Mutual Transport Layer Security (MTLS) encryption. All communication traffic between LCS 2005 with SP1 servers is encrypted, and message content is protected while in transit across public networks. Client to server connections can use TLS as well as Secure Sockets Layer (SSL) to encrypt network traffic.

Scenarios

Logistic employees, working for organizations that provide shipping and delivery services, are examples of remote users. A logistic worker could alert team members of potential delays by simply searching his or her roaming contact list for presence information on a mobile phone. If the contact is online, an instant message could be sent that contains notification of the delay.

Airline pilots and crew are another example of remote users. If you have experienced travel delays at airports, you can appreciate the number of schedule changes that can occur. Instant messaging supported by Remote User Access could notify flight attendants, allowing the attendants to keep passengers informed at all times.

Considering Features of Remote User Access



Introduction

In the information worker age, individuals can work from home, office, car, and plane. Access to up-to-date information is critical. You want to assure your organization that LCS 2005 with SP1 provides secure communications to external users.

Remote User Access extends the features of LCS 2005 with SP1 on multiple clients while enforcing security. Remote user access does not require Virtual Private Network (VPN) connectivity.

Extends LCS 2005 with SP1

Telecommuters and remote users can take advantage of LCS 2005 with SP1 features. Remote users can:

- Maintain a roaming contact list.
- Use IM to contact co-workers.
- Search for corporate IM users.
- Display presence information.

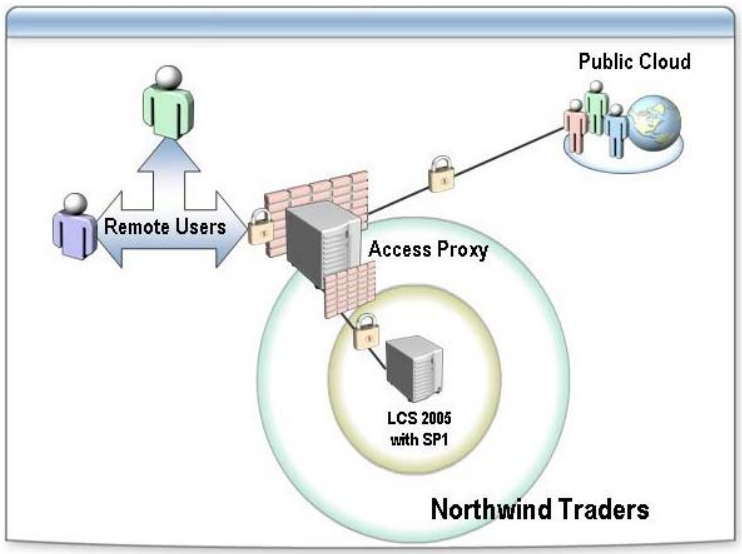
Multiple Clients

Remote users can use the following clients to access the internal LCS 2005 with SP1 network:

- Microsoft Office Communicator
- Office Communicator Web Access
- Microsoft Windows® Messaging 5.0 and 5.1

Important If IM over VPN is required, different DNS settings apply to different LCS 2005 with SP1 clients. External Microsoft Office Communicator clients can use **_sipinternaltls._tcp.**<*domain*> DNS service (SRV) record to detect the internal SIP server. External Windows Messenger 5.1 clients will continue to connect directly to the Access Proxy, using the **_sip._tls.**<*domain*> SRV record.

Identifying a Remote User Access Topology



Introduction

The Access Proxy role in LCS 2005 with SP1 supports the following basic topologies:

- Remote User Access
- Enterprise to Enterprise Federation through:
  - Enhanced Federation
  - Direct Federation
- Enterprise to Public Cloud

Important LCS 2005 with SP1 can be extended by enabling Remote User Access. Remote User Access does not need to be implemented before Enterprise to Enterprise Federation and Enterprise to Public Cloud topologies.

Remote User Access Topology

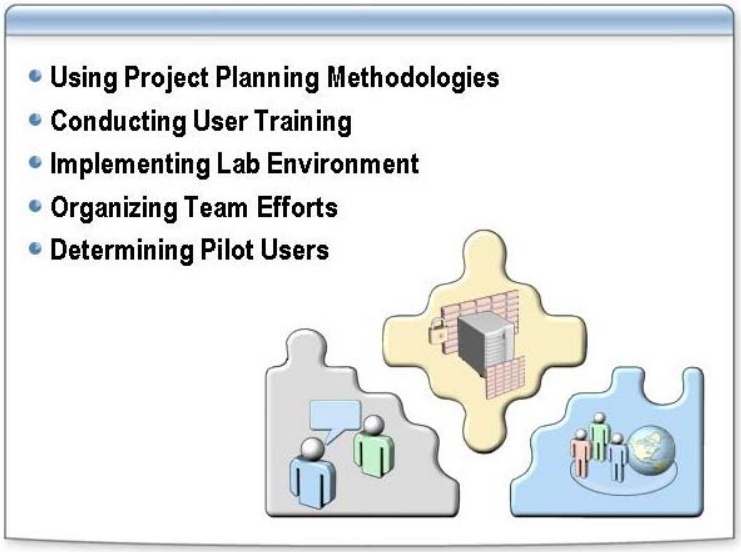
When Remote User Access is properly configured on your Access Proxy server, users have access to presence information and instant messaging capabilities from a public network.

While many remote clients in your environment may log on over a VPN to gain access to a computer running Live Communications Server, a VPN connection might not be available or practical in certain deployments.

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

- Remote users to internal users
- Remote users to remote users
- Remote users to public cloud
- Remote users to federated internal users
- Remote users to federated remote users

Planning for Remote User Access



Introduction

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

Consider the lessons learned from your previous deployments. Each corporate environment is different. Training your implementation team with step-by-step deployment guides might produce a successful implementation, while change control procedures or formal project plans might be required in other companies.

Project Planning

All LCS 2005 with SP1 deployments benefit from project planning. Project planning uses your technical team members to help with the following activities:

- Identifying all deployment tasks
- Prioritizing task dependencies
- Listing task duration
- Assigning implementation responsibilities
- Obtaining executive and management support

User Training

Previous deployments might have made you aware of how important user training can be before a deployment begins. Initiating user training before a deployment could reduce the number of users contacting your helpdesk after deployment. User training may include:

- Hosting classroom seminars.
- Conducting online training.
- Distributing cheat sheets.
- Scheduling training luncheons.

Lab Testing

With virtual software options, an entire Remote User Access lab environment could be set up to create training documentation, step-by-step guides, and

disaster recovery processes. Lab testing could also be used to refine your project plan.

Team Coordination

Lab testing may help you determine the tasks that require coordination with other teams. For example, opening the firewall ports for Remote User Access could be another team's responsibility.

Review internal procedures for requesting firewall port configuration with your networking and security teams. Understanding team coordination procedures (change control or Microsoft SharePoint® Portal form requests) could be beneficial if completed early.

Pilot Users

After lab testing and creating user training documentation, a small group of users could be designated as a pilot group. It is recommended to designate several technical users before extending the pilot trial to executives or upper management.

Providing pilot users a communication method for feedback is very important. You could use the following feedback methods:

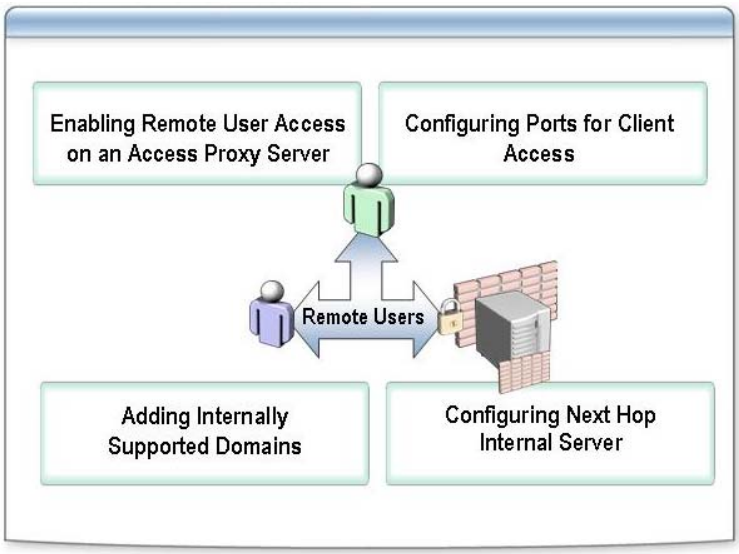
- E-mailing to a generic mailbox or distribution list
- Updating a SharePoint discussion form
- Scheduling bi-weekly meetings
- Conducting a Live Meeting

Remote Users

After your pilot trial has been completed and all recommendations and lessons have been implemented, you can determine which users to enable for Remote User Access. Enabling Remote User Access can be completed in bulk or on a per-user basis.

Your entire organization may not require Remote User Access privileges. Consider the user groups who travel the most or manage multiple geographic locations. Does your company have a large sales force with regional account managers? These questions will help you prioritize enabling remote access based on the needs of your users.

Lesson: Configuring an Access Proxy Server for Remote User Access



Introduction

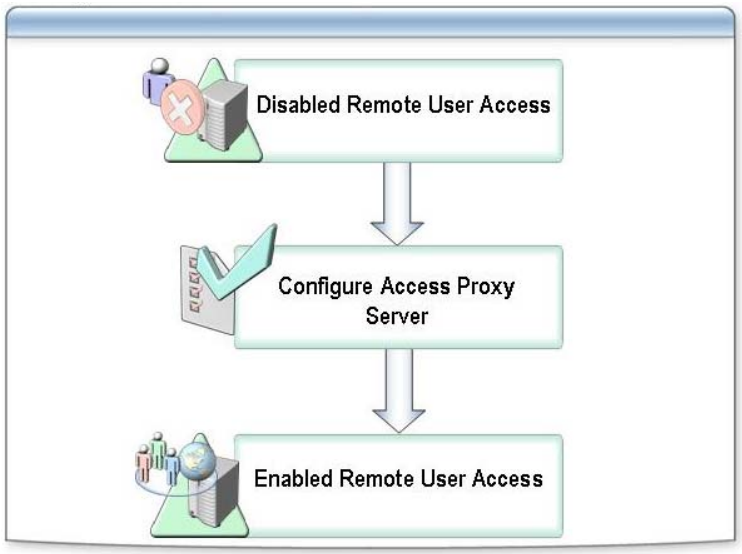
This lesson describes how to configure your Access Proxy server for Remote User Access. Configuration must be completed in order for your remote users to take advantage of LCS 2005 with SP1 features.

Lesson objectives

After completing this lesson, you will be able to:

- Enable Remote User Access on an Access Proxy Server.
- Configure ports for client access.
- Add internally supported domains.
- Configure next hop internal server.
- Explain how to configure an Access Proxy server for Remote User Access capabilities.

Enabling Remote User Access on an Access Proxy Server



Introduction

Enabling Remote User Access requires an existing LCS 2005 with SP1 internal infrastructure. You will also want to provide a perimeter network where the Access Proxy server will be located.

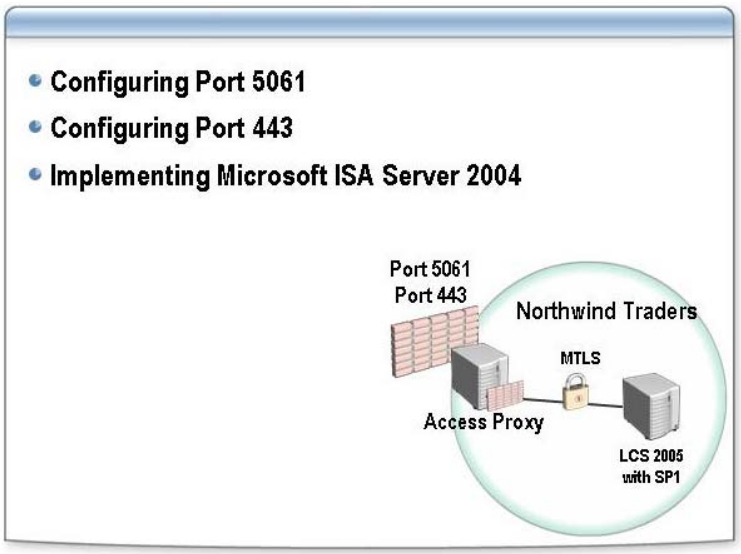
The same Access Proxy server can also support Enterprise to Enterprise Federations or Enterprise to Public IM Connectivity.

Setup Procedures

Enable your Access Proxy server for Remote User Access by completing 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. If necessary, expand **Services and Applications**.
4. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
5. In the **Properties** dialog box, click the **Public** tab.
6. Select **Allow client connections for remote access**.
7. Click **OK** on the **Public** tab.
8. In the **Properties** dialog box, click the **General** tab.
9. Select **Allow remote user access to your network**.
10. Click **OK** on the **General** tab.

Configuring Ports for Client Access



Introduction

You can configure multiple ports for your Remote User Access implementation. By default, LCS 2005 with SP1 uses port 5061, but there may be occasions when you want to change this setting or add different ports.

If you have remote users (consultants, for example) who need to connect to Live Communications Server from an external network, such as at a client's location, then the default port may not be suitable. If the client has an advanced firewall, such as Microsoft Internet Security and Acceleration (ISA) Server 2004, then unless the network administrator has specifically opened port 5061, the remote users will not be able to connect to LCS. In this scenario, port 443 is the best choice because it is likely that this port is open.

Configure Ports

To configure ports on your Access Proxy, 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. If necessary, expand **Services and Applications**.
4. Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**.
5. In the **Properties** dialog box, click the **Public** tab.
6. Under **Listening ports**, click **Add** to add a port to the list.
7. In the **Add Listening Port** dialog box, enter the port you want to use for remote user access.
8. Click **OK** on the **Public** tab.

Caution Mutual Transport Layer Security (MTLS) cannot be used in conjunction with port 443. If you want to use port 443, you must clear the Authenticate remote server (Mutual TLS) checkbox.

Microsoft ISA Server 2004

An Access Proxy server can utilize a perimeter network configured with an advanced firewall such as Microsoft ISA Server 2004. Microsoft ISA Server 2004 can provide firewall services on both sides of a perimeter network.

However, when you use ISA Server 2004 in combination with LCS 2005 with SP1, remote users can only use presence and instant messaging facilities. The following features are not supported:

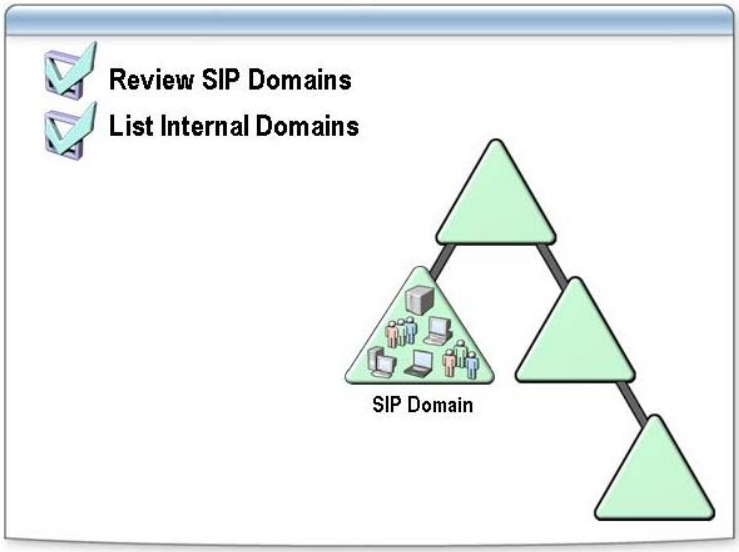
- Audio
- Video
- Data collaboration
- File transfer

Additional Resources

If you want to implement a perimeter network with Microsoft ISA Server 2004, review “Configuring Microsoft Office Live Communications Server 2003 Standard Edition with ISA Server 2004 on the Microsoft Web site, at: http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/tls-isa.mspx?pf=true.

Even though this document was written for Live Communications Server 2003, the concepts apply to Live Communications Server 2005.

Adding Internally Supported 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 configure an Access Proxy to support Remote User Access, you need to specify each internal domain that includes an installation of LCS 2005 with SP1. You can review the list of internal domains(s) that have an installation of LCS 2005 with SP1 in the global settings.

Internal SIP Domain

A Live Communications Server 2005 with SP1 infrastructure relies on your Active Directory® configuration. It is important to understand the definition of a SIP domain.

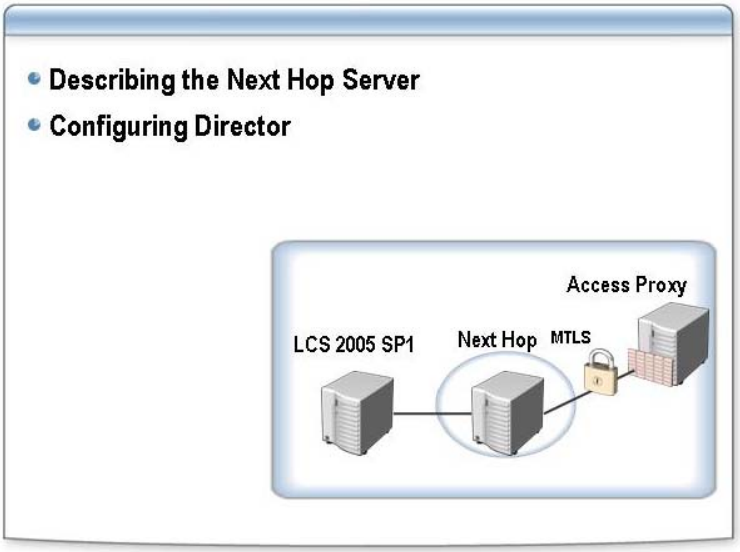
A SIP domain is any domain with an installation of LCS 2005 with SP1. Hence, you might have multiple SIP domains in your Active Directory forest.

If you are not aware of all your internal SIP domains, you may obtain and review the global list of SIP domains. Review the properties of the forest node on an internal LCS 2005 with SP1 server to obtain the global list of SIP domains.

Additional Resources

If you want more information on SIP domains, 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.

Configuring Next Hop Internal Server



Introduction

When an Access Proxy server accepts incoming SIP traffic from your remote users, this traffic must be delivered to the internal network. You must designate the Next Hop server. Your Access Proxy server will forward all inbound data to your Next Hop server.

Next Hop Server

Your Access Proxy server will forward all inbound data to your Next Hop server. A Next Hop server can be an internal LCS 2005 with SP1 server. Alternatively, the Next Hop server could host the Director server role.

Director Server

A Director server can act as the second line of defense when it deploys 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.

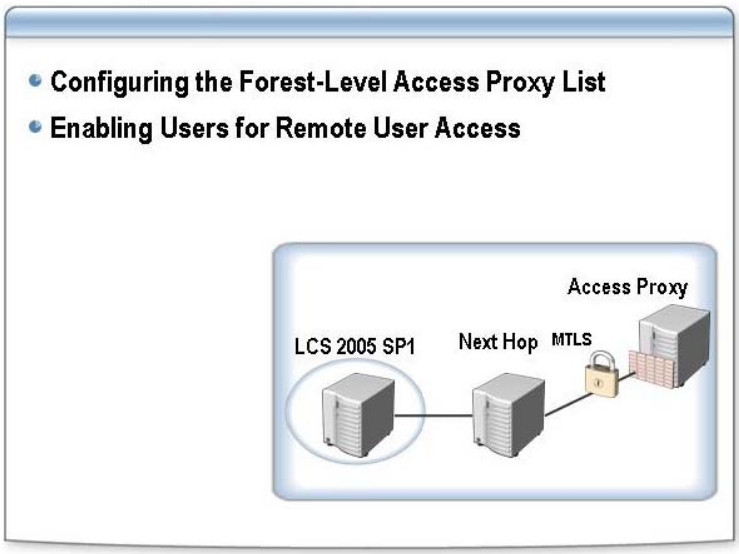
If you decide to implement a Director, the Director provides authentication against Active Directory for traffic forwarded from the Access Proxy server.

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

Additional Resources

If you want more information on configuring your Next Hop server, 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.

Lesson: Implementing Internal Domain for Remote User Access



Introduction

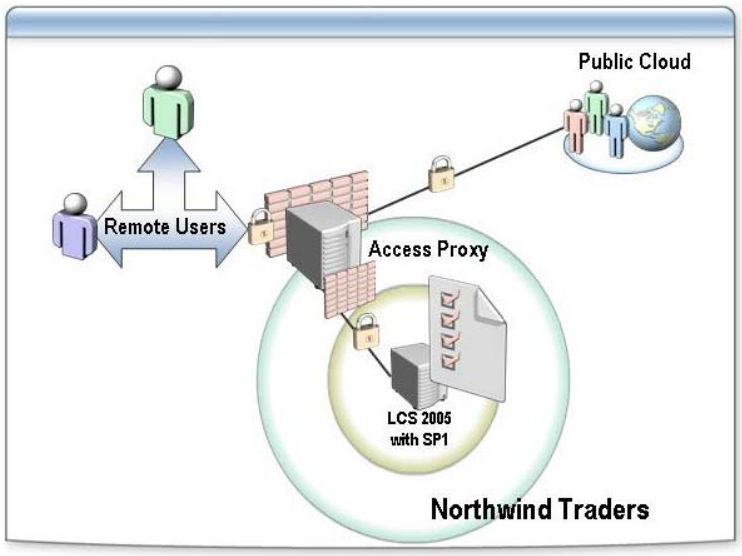
This lesson describes how to configure your internal SIP domain to use the Access Proxy server with the enabled feature of Remote User Access. Configuration on your internal domain must be completed in order for your remote users to access the LCS 2005 with SP1 features by using their SIP clients.

Lesson objectives

After completing this lesson, you will be able to:

- Configure the forest-level Access Proxy List
- Enable users for Remote User Access privileges.
- Prepare the internal domain for Remote User Access

Configuring the Forest-Level Access Proxy List



Introduction

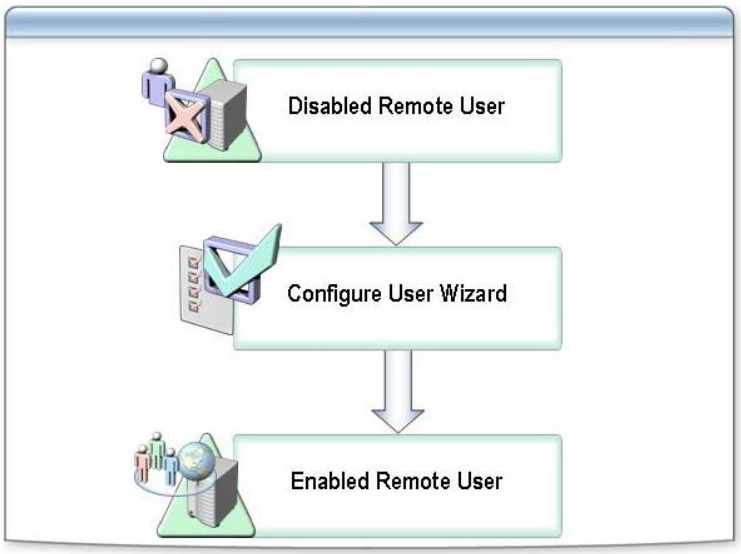
Your internal domain must be configured to identify the Access Proxy server. If you deploy an Access Proxy array in your perimeter network, the array must also be included in this Access Proxy list.

Updating Access Proxy List

To update the Access Proxy List, perform the following steps:

1. Log on to an internal Live Communications Server.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005**.
3. In the console tree, right-click the **Forest** node.
4. Click **Properties** for the forest node.
5. Click the **Access Proxy** tab.
6. Add the **FQDN** of each Access Proxy or array of Access Proxies that you have deployed in the perimeter of your network.

Enabling Users for Remote User Access



Introduction

After you have configured your Access Proxy and list of internal domain(s) with LCS 2005 with SP1 for Remote User Access, you must authorize your internal users. Unless your internal users are authorized, they will not be able to take advantage of the Remote User feature.

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

To enable users for Remote User Access with the Configure User Wizard, 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

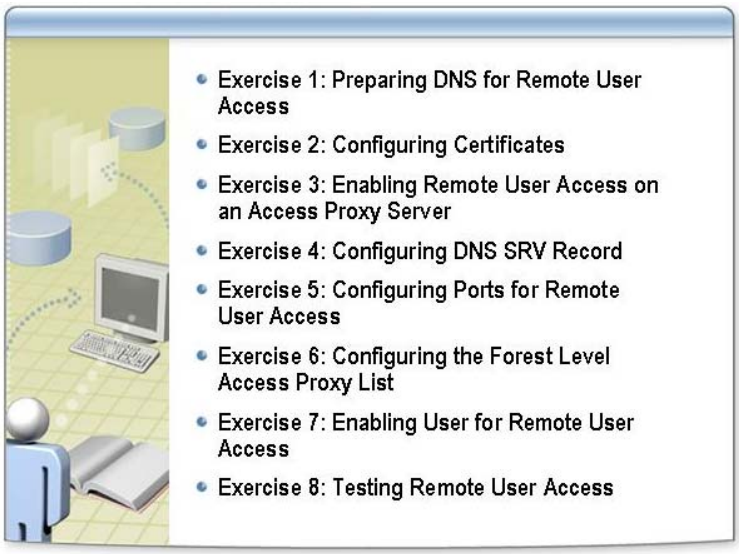
To enable multiple user accounts for remote access, you may find it more convenient to use the Live Communications Server management console.

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**.

Note Review Lesson 1: Introducing Remote User Access to help you plan which users and groups should be enabled with Configure Users Wizard.

Lab 7: Configuring Access Proxy Settings for Remote User Access



Objectives

After completing this lab, you will be able to:

- Prepare DNS on the Client1 server for Remote User Access capabilities.
- Configure Certificates for Remote User Access.
- Configure an Access Proxy server for Remote User Access capabilities.
- Configure Domain Name Service (DNS) Service Location (SRV) Record.
- Prepare the internal domain for Remote User Access.
- Test Remote User Access.

Estimated time to complete this lab: **40 minutes**

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

Introduction

Fabrikam wants to enable employees working remotely to connect to LCS 2005 with SP1. This requires the network administrator to configure Remote User Access.

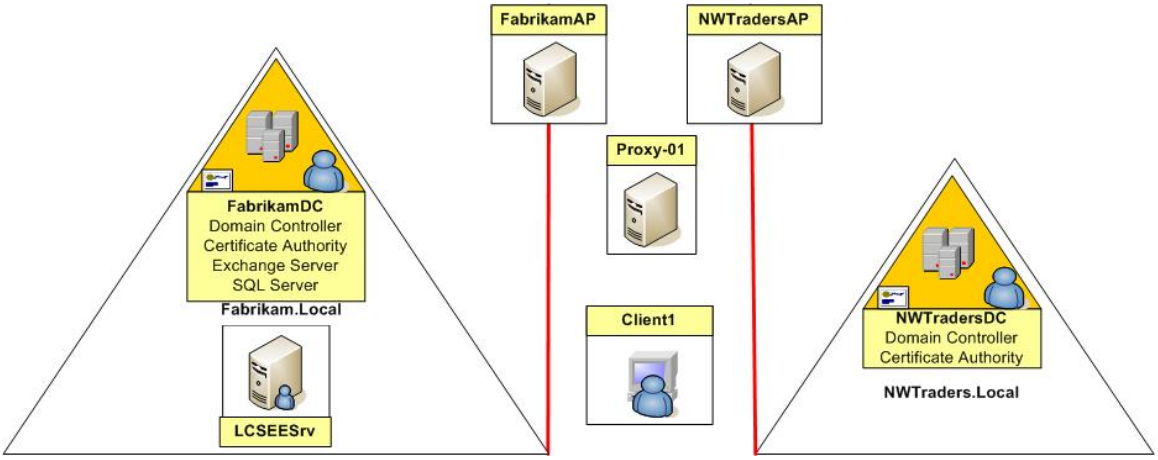
In this lab you will prepare your Access Proxy server and your internal SIP domain for Remote User Access. You will also configure your ports for client access. After you configure your Access Proxy server, you will configure your internal SIP domain.

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 Remote User Access privileges.

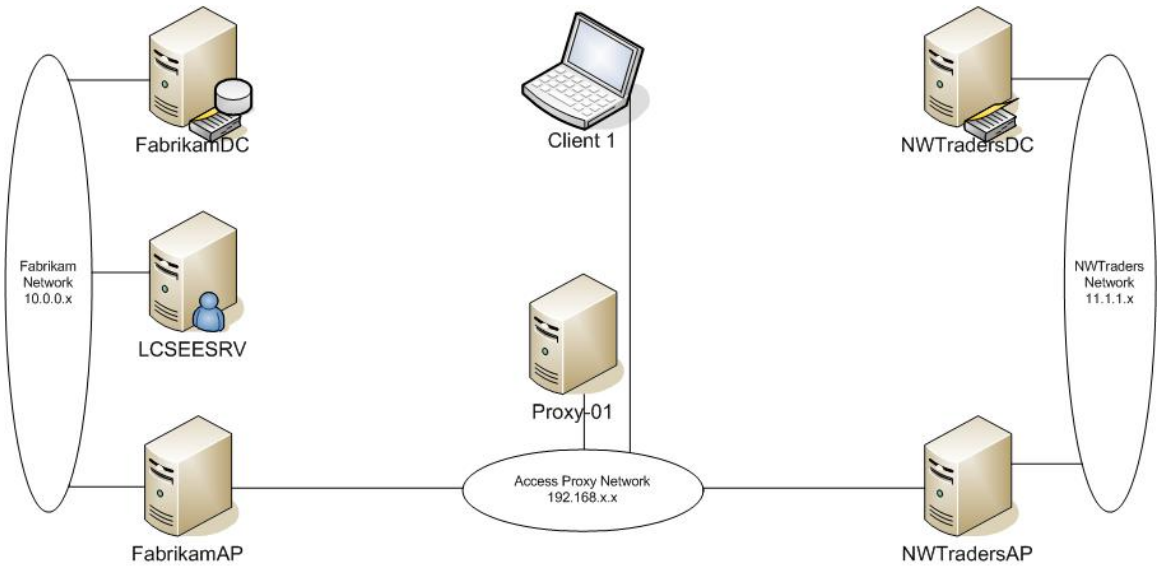
Remote User Access should only be enabled after a Standard or Enterprise Edition Live Access Proxy server has been implemented in your perimeter network environment.

Network Topology

The labs in this course use virtual machines. To configure the virtual machines so that they are 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 figure.



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 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-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
Preparing Domain Name Service Records to Install Remote User Access.

Scenario

Matt Dillon, the network administrator for Fabrikam, has been tasked to enable remote users to connect to LCS 2005 with SP1. To do this, he has a client computer that he wants to use for testing the remote access functionality from his home. This client computer is not a member of the Fabrikam domain, so needs its DNS settings configured.

Description

In this exercise, you will configure the Host file and the DNS name of the Client1 desktop. If DNS is not properly configured, incoming requests would not detect your SIP domain information nor be able to route messages to your corporate users. This is the first procedure you need to complete in order to prepare your environment for Remote User Access.

Tasks	Detailed Steps
Important: Perform this exercise on the **7034A-Client1-B** virtual machine.	
1. Configure Host File.	**a.** Log on to the **7034A-Client1-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start** , and then **Run**. **c.** In the **Open** box, type **%windir%\system32\drivers\etc**\, and click **OK**. **d.** Edit the **hosts** file with Notepad. **e.** Under the localhost entry, add the following entry on a separate line: **192.168.0.10 FabrikamAP.Fabrikam.local** **f.** Save the **hosts** file. **g.** Exit Notepad.
1. Prepare the DNS name of the Client1 server.	**a.** On **7034A-Client1-B**, click **Start**, right-click **My Computer**, and click **Properties**. **b.** On the **System Properties** dialog box, click the **Computer Name** tab, and then click **Change**. **c.** On the **Computer Name Changes** dialog box, click **More**. **d.** On the **DNS Suffix and NetBIOS Computer Name** dialog box, in the **Primary DNS suffix of this computer** box, type **Workgroup.local**, and then click **OK**. **e.** On the **Computer Name Changes** dialog box, click **OK**. **f.** On the **You must restart this computer for the changes to take effect** dialog box, click **OK**. **g.** On the **System Properties** dialog box, click **OK**. **h.** On the **System Settings Change** dialog box, click **Yes** to restart the workstation.

Exercise 2
Prepare Certificate for the Remote Client

Scenario

For the remote client to be able to communicate securely with the LCS 2005 with SP1 server, the client requires a certificate from a trusted CA. Matt needs to request this certificate from the Fabrikam CA.

Description

In this exercise, you will configure the Client1 desktop by installing a certificate. This is the first procedure you need to complete to prepare your environment for Remote User Access capabilities.

Tasks	Detailed Steps
Important: Perform this exercise on the **7034A-FabrikamAP-B** virtual machine.	
1. Install certificate chain 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 **http://FabrikamDC/certsrv**, and then click **OK**. **d.** For the **Microsoft Certificate Services – EECA Welcome** page, under **Select a task**, click **Download a CA certificate, certificate chain, or CRL**. **e.** On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Download CA certificate chain**. **f.** On the **File Download** dialog box, click **Save**. **g.** Save the file as **C:\Client1_Chain.p7b**. **h.** On the **Download Complete** dialog box, click **Close**. **i.** Close the Internet Explorer® window.
2. Copy certificate chain on Client1	**a.** Log on to **7034A-Client1-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start** , and then click **Run**. **c.** In the **Open** box, type **\\FabrikamAP\c$**, and then click **OK**. **d.** Right-click **C:\Client1_Chain.p7b**, and then click **Copy**. **e.** Click **Start**, and then click **Run**. **f.** In the **Open** box, type **C:**, and then click **OK**. **g.** Right-click on the Windows Explorer window, and click **Paste**.
3. Install a certificate path on Client1.	**a.** Switch to the **7034A-Client1-B** workstation. **b.** Click **Start**, and then click **Run**. **c.** In the **Open** box, type **mmc**, and then click **OK**. **d.** On the Microsoft Management Console, on the **File** menu, click **Add/Remove Snap-in**. **e.** On the **Add/Remove Snap-in** page, click **Add**.

	f. On the **Add Standalone Snap-in** dialog box, in the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**. **g.** On the **Certificates Snap-in** dialog box, click **Computer account**, and then click **Next**. **h.** On the **Select Computer** dialog box, ensure the **Local computer** check box is selected, and then click **Finish**. **i.** On the **Add Standalone Snap-in** dialog box, click **Close**. **j.** On the **Add/Remove Snap-in** page, click **OK**. **k.** On the **Certificates** console, expand **Certificates (Local Computer)**. **l.** Expand **Trusted Root Certification Authorities**. **m.** Right-click **Certificates**, point to **All Tasks**, and then click **Import**. **n.** On the **Certificate Import Wizard**, click **Next**. **o.** On the **File to Import** page, click **Browse**. **p.** On the **Open** page, type **C:\Client1_Chain.p7b**, and then click **Open**. **q.** On the **File to Import** page, click **Next**. **r.** On the **Certificate Store** page, verify the default value is selected for **Place all certificates in the following store**.  *Verify the Trusted Root Certification Authorities option is displayed for the Certificate store.* **s.** Click **Next**. **t.** On the **Completing the Certificate Import Wizard**, click **Finish**. **u.** On the **Certificate Import Wizard** dialog box, click **OK**.
4. Request the Certificate on FabrikamAP.	**a.** On the **7034A-FabrikamAP-B** server, click **Start**, and then click **Run**. **b.** In the **Open** box, type **http://FabrikamDC/certsrv**, and then click **OK**. **c.** On the **Welcome** page, in the **Select a Task** box, click **Request a certificate**. **d.** On the **Request a Certificate** page, click **advanced certificate request**. **e.** On the **Advanced Certificate Request** page, click **Create and submit a request to this CA**. **f.** On the **Certificate Template**, click the **LCS2005EE** template. **g.** Under **Identifying Information for Offline Template**, in the **Name** field, type **Client1.Workgroup.local**.  *The DNS name of the Access Proxy server was completed in Exercise 1.* **h.** In the **Key Options** page, in **CSP**, ensure **Microsoft RSA SChannel Cryptographic Provider** is selected. **i.** Select the **Mark keys as exportable** check box.

	j. On the **Key Options** page, select the **Store certificate in the local computer certificate store** check box, and then click **Submit**. **k.** On the **Potential Scripting Violation** dialog box, click **Yes**.
5. Install the certificate on the FabrikamAP server.	**a.** On the **Certificate Issued** page, click **Install this certificate**. **b.** If you receive a **Potential Scripting Violation** dialog box, click **Yes**. **c.** Close Internet Explorer.
6. Export certificate from FabrikamAP server.	**a.** Click **Start** , and then click **Run**. **b.** In the **Open** box, type **mmc**, and click **OK**. **c.** In the Management Console, on the **File** menu, click **Add/Remove Snap-in**. **d.** On the **Add/Remove Snap-in** dialog box, click **Add**. **e.** On the **Add Standalone Snap-in** dialog box, in the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**. **f.** On the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**. **g.** Ensure the **Local computer (the computer this console is running on)** check box is selected, and then click **Finish**. **h.** On the **Add Standalone Snap-in**, click **Close**. **i.** On the **Add/Remove Snap-in**, click **OK**. **j.** On the MMC Management console, expand **Certificate (Local Computer)**, expand **Personal**, and then click **Certificates**. **k.** Right-click the **Client1.Workgroup.local** certificate, point to **All Tasks**, and then click **Export**. **l.** On the **Welcome to the Certificate Export Wizard**, click **Next**. **m.** On the **Export Private Key** page, click **Yes, export the private key**, and then click **Next**. **n.** On the **Export File Format** page, accept the default values, and then click **Next**. **o.** On the **Password** page, enter and confirm the password **pass@word1**, and then click **Next**. **p.** On the **File to Export** page, in the **File name** box, type **C:\Client1Export**, and click **Next**. **q.** On the **Completing the Certificate Export Wizard**, click **Finish**. **r.** On the **Certificate Export Wizard** message box, click **OK**. **s.** Close the Management Console window and do not save changes.
7. Copy certificate on Client1.	**a.** Log on to **7034A-Client1-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start** , and then click **Run**. **c.** On the **Open** box, type **\\FabrikamAP\c$**, and then click **OK**. **d.** Right-click **C:\Client1Export.pfx**, and then click **Copy**.

	e. Click **Start** , and then click **Run**. **f.** On the **Open** box, type **C:**, and then click **OK**. **g.** Right-click on the Windows Explorer window, and click **Paste**.
8. Install the certificate on Client1 desktop.	**a.** Click **Start** , and then **Run**. **b.** On the **Open** page, type **mmc**, and click **OK**. **c.** In the Management Console, on the **File** menu, click **Add/Remove Snap-in**. **d.** On the **Add/Remove Snap-in** dialog box, click **Add**. **e.** On the **Add Standalone Snap-in** dialog box, in the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**. **f.** On the **Certificates snap-in** dialog box, click **Computer account**, and then click **Next**. **g.** On the **Select Computer** dialog box, ensure **Local computer: (the computer this console is running on)** is selected, and then click **Finish**. **h.** On the **Add Standalone Snap-in** dialog box, click **Close**. **i.** On the **Add/Remove Snap-in** dialog box, click **OK**. **j.** On the MMC console, expand **Certificates (Local Computer)**. **k.** Right-click **Personal**, point to **All Tasks**, and then click **Import**. **l.** On the **Welcome to the Certificate Import Wizard** page, click **Next**. **m.** On the **File to Import** page, in the **File name** box, type **C:\Client1Export.pfx**, and then click **Next**. **n.** On the **Password** page, in the **Password** box, type **pass@word1**, ensure the **Mark this key as exportable box** check box is clear, and then click **Next**. **o.** On the **Certificate Store** page, click **Place all certificates in the following store**, and ensure **Personal** is selected, and then click **Next**. **p.** On the **Completing the Certificate Import Wizard** page, click **Finish**. **q.** On the **Certificate Import Wizard** message box, if the import was successful, click **OK**.

Exercise 3
Enable Access Proxy for Remote User Access

Scenario

Matt now has to enable the Remote User Access feature on each Access Proxy server. Fabrikam only has one Access Proxy server, so this is not too difficult a task.

Description

In this exercise, you will configure the Access Proxy server by enabling the Remote User Access feature. This is the first procedure you need to complete to prepare your environment for Remote User Access capabilities.

Tasks	Detailed Steps
Important: Perform this exercise on the **7034A-FabrikamAP-B** virtual machine.	
1. Enable Remote User Access.	**a.** Log on to **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and click **Computer Management**. **c.** Expand **Services and Applications**. **d.** Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**. **e.** On the **Microsoft Office Live Communications Server 2005 Properties** dialog box, click the **Public** tab. **f.** On the **Listening ports** section, click **Edit**. **g.** On the **Edit Listening Port** dialog box, select the **Allow client connections for remote access** check box, and then click **OK**. **h.** On the **Public** tab, click **Apply**. **i.** Click the **General** tab. **j.** Select the **Allow Remote User Access to Your Network** check box, and then click **OK**. **k.** In the left-hand pane, right-click **Microsoft Office Live Communications Server 2005**, and click **Refresh**. **l.** Note that on the **Status** tab, the **Allow remote user access** status changes from a cross to a checkmark.

Exercise 4
Enable Domain Name Service Record

Scenario

The remote clients need to be able to contact the Access Proxy offering Remote Access facilities. This configuration requires Matt to create a DNS Service Location Record (SRV) for the Access Proxy.

Description

In this exercise, you will configure the the _sip_tls.<domain> record on the Proxy-01 server. Proxy-01 is the external DNS server in this environment.

Tasks	Detailed Steps
 **Important:** Perform this exercise on the **7034A-Proxy01-B** virtual machine.	
1. Enable DNS SRV record for Remote User Access.	**a.** Log on to **7034A-Proxy01-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and click **DNS**. **c.** In the dnsmgmt console, expand **PROXY-01**, and then expand **Forward Lookup Zones**. **d.** Right-click **Fabrikam.local**, and then click **Other New Records**. **e.** On the **Resource Record Type** dialog box, in the **Select a resource record type** list, click **Service Location (SRV)**, and then click **Create Record**. **f.** On 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 **FabrikamAP.Fabrikam.local**. **i.** In the **New Resource Record** box, type **OK**. **j.** On the **Resource Record Type** dialog box, click **Done**.

Exercise 5
Configuring Ports for Remote User Access

Scenario

Matt needs to check that his Access Point settings support Remote User Access. To do this, he must check that port 5061 on the Public interface of the Fabrikam Access Point is listening for incoming connections.

Description

In this exercise, you will check that the port settings support Remote User Access.

Tasks	Detailed Steps
Important: Perform this exercise on the **7034A-FabrikamAP-B** virtual machine.	
1. Check Ports on the 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 click **Computer Management**. **c.** Expand **Services and Applications**. **d.** Right-click **Microsoft Office Live Communications Server 2005**, and click **Properties**. **e.** On the **Properties** dialog box, click the **Public** tab. **f.** On the **Listening ports** section, check that there is an entry of **5061**. **g.** In the **Properties** dialog box, click **OK**. **h.** Close the Computer Management console.

Exercise 6
Configuring the Forest-Level Access Proxy List

Scenario

Matt now needs to set up the address of the Access Proxy server in the Forest configuration. However, he thinks he might have done this already, so he's just going to check if that is the case.

Description

In this exercise, you will check the settings for the forest-level Access Proxy server list.

Tasks	Detailed Steps
 **Important:** Perform this exercise on the **7034A-LCSEESRV-B** virtual machine.	
1. Check the Access Proxy List on Forest Node.	**a.** Log on to **7034A-LCSEESRV-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and click **Live Communications Server 2005**. **c.** On the **Microsoft Office Live Communications Server 2005** console, right-click **Forest** node, and click **Properties**. **d.** On the **Live Communications Server Global Properties** dialog box, click **Access Proxy** tab. **e.** Check that an entry exists for **FabrikamAP.Fabrikam.local**. **f.** On the **Live Communications Server Global Properties** dialog box, click **OK**. **g.** Close the Microsoft Office Live Communications Server 2005 console.

Exercise 7
Enabling Users for Remote User Access

Scenario

After configuring Remote User Access on his Access Proxy server, Matt can now enable his users for Remote User Access. He does this by using the LCS wizard in Active Directory Users and Computers.

Description

In this exercise, you will configure your users for Remote User Access.

Tasks	Detailed Steps
Important: Perform this exercise on the **7034A-FabrikamDC-B** virtual machine.	
1. Configure Public Edge.	**a.** Log on to **7034A-FabrikamDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**. **c.** On the **Active Directory Users and Computers console**, expand **fabrikam.local**, and click the **LCSUsers** organizational unit. **d.** Select the five user accounts in the **LCSUsers** OU. **e.** Right-click those users, and then click **Configure Live Communications Users**. **f.** On the **Welcome to the Configure Users Wizard** page, click **Next**. **g.** On the **Configure User Settings** page, click **Configure Remote Access**. **h.** Ensure **Allow Users** is selected, and click **Next**. **i.** On the **Configure Operation Status** page, wait until all the operations have succeeded, and then click **Finish**. **j.** Close Active Directory Users and Computers.

Exercise 8
Test Remote User Access

Scenario

Finally, Matt can check that his remote users can connect into the Fabrikam LCS 2005 with SP1 enterprise pool. He does this by using Office Communicator 2005 on the Client1 virtual machine to talk to Jim Kim in Sales. However, because Client1 is in a workgroup and not in the Fabrikam domain, Matt forgot that it does not have Office Communicator 2005 installed through group policy, so he has to install Communicator manually. Finally, Matt checks that he can search for one of his internal users while connected as a remote user.

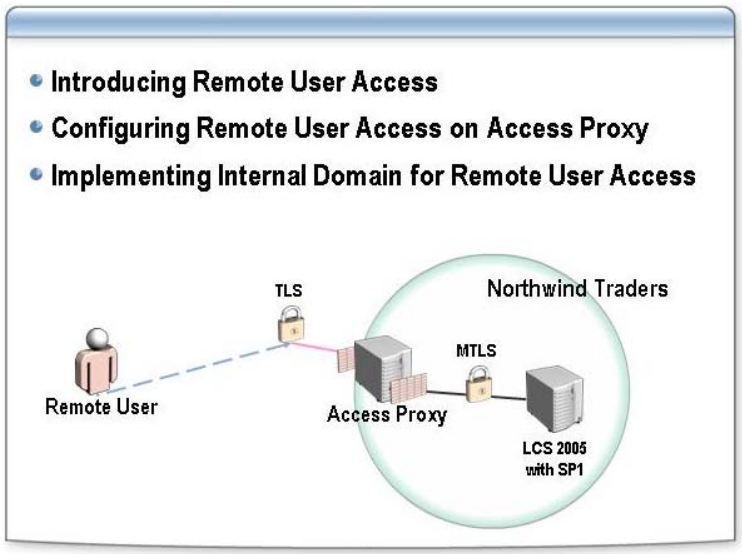
Description

In this exercise, you will send an instant message from your remote user to an internal user.

Tasks	Detailed Steps
Important: Perform this exercise on the **7034A-LCSEESRV-B** virtual machine.	
1. Prepare internal user.	**a.** Log on to **7034A-LCSEESRV-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **All Programs**, and then click **Microsoft Office Communicator 2005**. **c.** On the **Sign-In Account** dialog box, log on as **jim@fabrikam.local** with a **Password** of **pass@word1**, and then click **OK**. **d.** Verify Jim Kim's presence information is set to **Online**.
2. Prepare Remote User.	**a.** Log on to **7034A-Client1-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, and click **My Computer**. **c.** Browse to **E:\Demo Files\Office Communicator 2005\bits**, and double-click **Communicator.msi**. **d.** On the **Welcome to Microsoft Office Communication 2005 Setup** page, click **Next**. **e.** On the **End-User License Agreement** page, click **I accept the terms in the License Agreement**, and click **Next**. **f.** On the **Product Identification** page, click **Next**. **g.** On the **Configure Microsoft Office Communicator 2005** page, accept the default path, and click **Next**. **h.** On the **Microsoft Office Communicator 2005 installation completed** page, click **Finish**. **i.** Click **Start**, point to **All Programs**, and then click **Microsoft Office Communicator 2005**. **j.** If a **The page cannot be displayed** Web page appears, close the Internet Explorer Window. **k.** On the **Microsoft Office Communicator** page, click **Actions** , and

	then click **Options**. **l.** In the **Sign-in name** box, type **Matt@Fabrikam.local**. **m.** In **My account name**, click **Advanced**. **n.** On the **Advanced Connection Settings** dialog box, click **Configure settings**. **o.** In the **Server name or IP address** box, type **FabrikamAP.Fabrikam.local**. **p.** Under **Connect using**, click **TLS**. **q.** On the **Advanced Connection Settings** dialog box, click **OK**. **r.** On the **Options** page, click **OK**. **s.** On the **Microsoft Office Communicator**, click **Sign In**. **t.** Type **matt@fabrikam.local** for the user name. **u.** In the **Sign-In Account** dialog box, in the **User name** box, type **matt@fabrikam.local**, and in the **Password** box, type **pass@word1**. **v.** Verify that Jim Kim's presence information is set to **Online**. **w.** If Jim Kim is showing as away, switch to the **7034A-LCSEESRV-B** virtual machine, and click the Communicator window. **x.** Switch back to **7034A-Client1-B**, and check that Jim Kim is online. **y.** Start an Microsoft Office Communicator session between Matt and Jim Kim.
3. Add internal user to remote user's contact list.	**a.** In Microsoft Office Communicator, click on **Contacts**. **b.** Click **Add a Contact**. **c.** On the **Add a Contact** dialog box, accept the defaults, and click **Next**. **d.** Type **Jeff@Fabrikam.local** for the email address, and then click **Next**. **e.** On the **Success!** page, click **Finish**. **f.** Note that Jeff Smith has been added to Matt's contact list. **g.** DO NOT close down the VPC images, but leave them running for Lab 8.

Review



In this module, you learned how Remote User Access can expand the reach of LCS 2005 with SP1 by enabling remote workers to connect to LCS from outside your network.

You learned how to configure your Access Proxy server to support Remote User Access. You saw how to set client access ports and how to enable your users for Remote User Access. You also learned that client-to-server connections can use TLS as well as Secure Sockets Layer (SSL) to encrypt network traffic.

In the next Module, you will look at how an Access Proxy can provide support for federation. Enabling federation gives your internal employees the ability to seamlessly use LCS 2005 with SP1 features with other organizations that have implemented their own internal LCS 2005 with SP1 infrastructure.