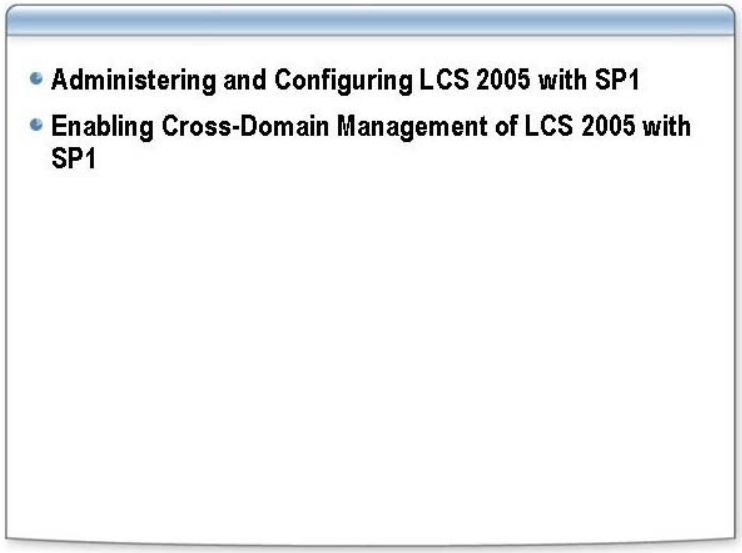
Microsoft®

Module 4: Administering Live Communications Server 2005 with SP1

Contents

Overview



Introduction

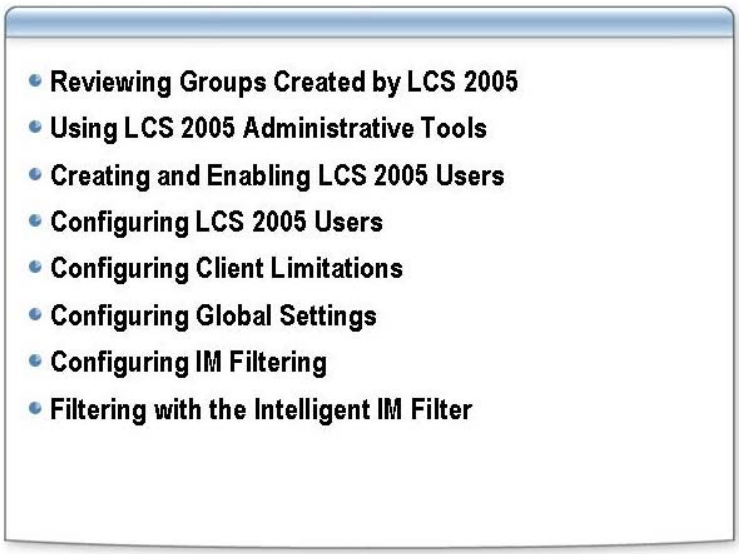
There are several methods for administering Microsoft® Live Communications Server 2005 with SP1 (LCS 2005 with SP1). There are also several post-installation tasks required to enable and configure your users and servers to use LCS 2005 with SP1. This module looks at the various tools and consoles used to administer users and servers in LCS 2005 with SP1, and shows you how to configure global, user, and server settings for LCS 2005 with SP1. You will also learn how to enable several cross-domain management scenarios for LCS 2005 with SP1.

Objectives

After completing this module, you will be able to:

- Administer and configure LCS 2005 with SP1.
- Enable cross-domain management of LCS 2005 with SP1.

Lesson: Administering and Configuring LCS 2005 with SP1



Introduction

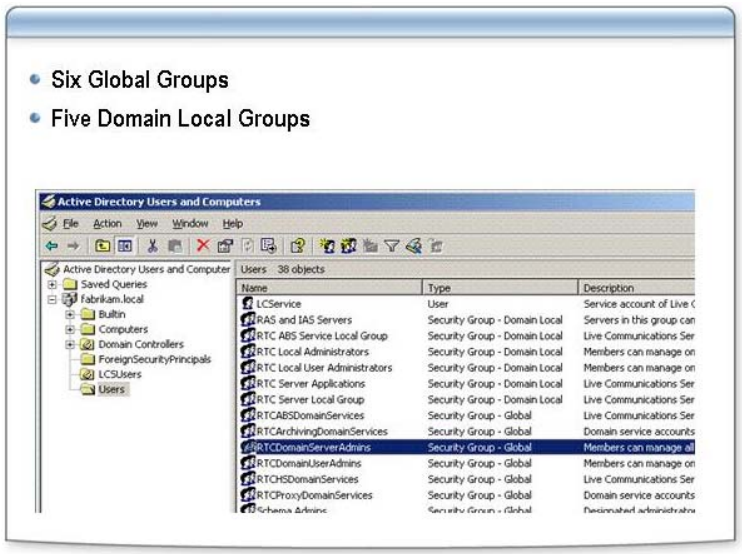
This lesson introduces the administration tools available for LCS 2005 with SP1, and shows you how to use them. You will learn how to create and enable users for LCS, configure LCS user settings, configure global settings for LCS, and how to configure and install instant messaging (IM) filtering programs.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the global and domain local groups created by LCS 2005 with SP1.
- Use LCS 2005 with SP1 administrative tools.
- Create and enable users for LCS 2005 with SP1.
- Configure LCS 2005 with SP1 user settings.
- Configure client limitation settings for LCS 2005 with SP1.
- Configure global settings for LCS 2005 with SP1.
- Configure instant message filtering on LCS 2005 with SP1.
- Install and use the Intelligent IM Filter application in LCS 2005 SP1.

Reviewing Groups Created by LCS 2005



Introduction

Live Communications Server 2005 with SP1 manages permissions by creating global groups and domain local groups. The global groups are responsible for domain-wide administration, and the local groups are responsible for pool and server administration.

Global Groups

LCS 2005 with SP1 creates six global groups, as listed below. The first two groups listed support the administrative model, and the others support permissions for the services.

- **RTCDomainServerAdmins**. Members of this group are generally tasked with deployment, pool, and server configurations and operations, as well as with management of enterprise-wide global settings. Server administrators control the global settings in Active Directory® and the configuration settings for an Enterprise Pool or Standard Edition Server. The settings are stored in Windows Management Instrumentation (WMI) and the configuration database. Server administrators are added to the Administrators group on each Enterprise Edition Server and Standard Edition Server to configure certificates. Server administrators can move users between any two Enterprise Pools or Standard Edition Servers, so have write permissions on some user attributes in Active Directory; but they cannot enable users or manage user search permissions. Server administrators also have the Admin role on the user database to perform database maintenance operations.
- **RTCDomainUserAdmins**. Members of this group are generally tasked with enabling and configuring users, managing user search permissions, troubleshooting users, and moving users between pools and servers. The user administrators receive limited read permission on the global settings in Active Directory, but have full read and write permissions on all user settings. User administrators also receive permissions on WMI similar to those granted to server administrators, in order to support configuring user settings and data through WMI; however, user administrators have only read permissions on the configuration database.

LCS 2005 with SP1 also creates four domain global service groups.

- **RTCHSDomainServices**. Gives permissions to the service accounts of the Enterprise Pools and Standard Edition Servers. RTCHSDomainServices allows the pool and servers to read user information inside Active Directory that is required for routing, user search, archiving, and authorizing user capabilities (federation, remote internet access, and public IM cloud connectivity). RTCHSDomainServices also allows the pool and servers to access the global settings and topology information stored inside the Active Directory forest root domain. For an Enterprise Pool deployment, the Enterprise Edition Servers of the Enterprise Pool will also use this group to access the Enterprise Pool Back-End user and configuration databases. Also, for an archiving deployment, Enterprise Pools and Standard Edition servers will use the RTCHSDomainServices group to write messages to the destination queue (Microsoft Messaging Queue) of the Archiving Service.
- **RTCArchivingDomainServices**. Gives permission to the service accounts of any Archiving service to access the Archiving Service Database. This group supports the two-tiered deployment topology, in which the archiving service component and the database are on separate computers.
- **RTCABSDomainServices**. Gives permission to the service accounts of an Address Book Service to access the Enterprise Pool Back-End User Database that the Address Book Service leverages to retrieve user information from Active Directory. The Address Book Server is an offline address book that can be used by the Live Communicator client for easy search of users for instant messaging and voice calls. For details, see the Address Book Service or Communicator documentation.
- **RTCProxyDomainServices**. Gives the service accounts of a forwarding Proxy permission to write messages to the destination queue (Microsoft Messaging Queue) of a remote Archiving Service.

Domain Local Groups

In addition to these global groups, LCS 2005 with SP1 creates five local groups on any Standard Edition Server or Enterprise Edition Server of an Enterprise Pool.

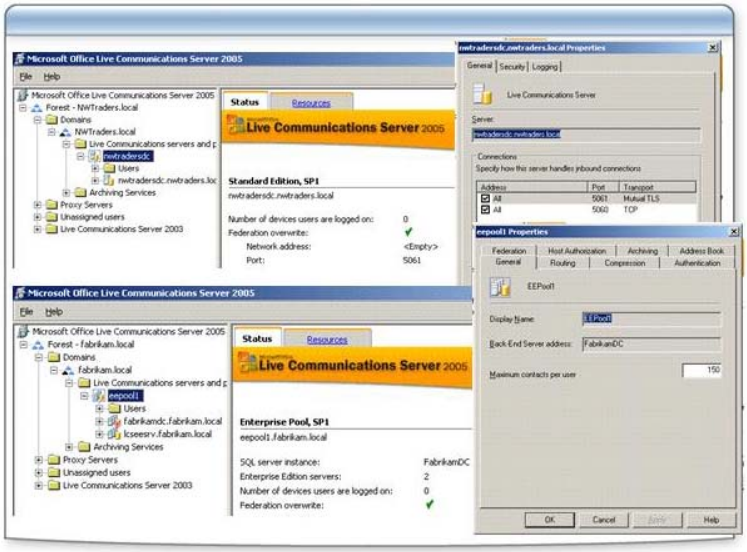
- RTC Local Administrators
- RTC Local User Administrators
- RTC Server Local Group

These three local groups give local rights and permissions on each Standard Edition Server or Enterprise Edition Server to their respective member domain global groups (RTCDomainServerAdmins, RTCDomainUserAdmins, and RTCHSDomainServices, respectively).

They are also used to allocate permissions on the user database and the configuration database for a Standard Edition Server, because the Standard Edition Server uses a Microsoft Data Engine (MSDE) instance, which supports only local execution. For an Enterprise Pool, database permissions are given to the domain global groups because the Enterprise Pool uses SQL Server™ 2000, which supports remote execution.

- **RTC ABS Service Local Group**. Gives limited local permissions to an Address Book Server on the user database of a Standard Edition Server MSDE instance. The Address Book Server leverages the LCS user database to retrieve user information from Active Directory.
- **RTC Server Applications**. Authorizes applications that are to be loaded by the LCS 2005 service (rtcsrv) when the service is started.

Using LCS 2005 Administrative Tools



Introduction

For both Standard Edition Servers and Enterprise pools, all pool-level settings are stored in the configuration database (RTCConfig) in the MSDE or SQL Server, respectively. Server-level settings include server-specific settings and are stored for each server in the WMI repository. Both types of settings are managed by the LCS 2005 WMI provider and are accessible by using the Live Communications Server 2005 administrative console, the LcsCmd.exe command-line tool, or the WMI interface.

Once LCS 2005 with SP1 Enterprise Edition is installed, configure your servers by using the following methods:

- **Live Communications Server 2005 administrative snap-in**. You can access the administrative snap-in on any LCS server joined to an Active Directory domain, or any computer joined to an Active Directory domain where the LCS 2005 administration tools are installed.
- **LCS 2005 command-line (LcsCmd.exe) export-import configuration tool**. LcsCmd.exe offers to export pool and server-level configuration settings from an existing server or a lab deployment to ensure a consistent configuration. LcsCmd.exe is installed on each LCS server and is also on the product CD.
- **WMI to programmatically modify settings**. All pool and server settings are exposed through the WMI interfaces. Scripts and tools are available from the LCS 2005 Resource Kit.

Configuring LCS with the Administrative Console

After you have installed LCS 2005 with SP1, use the Live Communications Server 2005 administrative snap-in to configure your server.

To start the administrative snap-in, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005**. The Live Communications Server 2005 administrative snap-in displays your LCS topology.

There are three different nodes in the tree view for Standard Edition Server or an Enterprise Edition Server:

- The <*forest*> node allows you to manage forest-level global settings that apply to all domains, pools and servers in LCS.
- The <*pool*> node allows you to manage pool-level settings that apply to all Enterprise Edition Servers within a pool or the Standard Edition Server. To access pool level settings, right-click the Enterprise pool and then click Properties.
- The <*FQDN*> node of each server allows you to manage individual server settings applied to the computer itself. To access server-level settings, expand the Enterprise pool, then right-click the fully qualified domain name (FQDN) of the server and click Properties.

Exporting Pool and Server Settings Using the Command-Line Tool

The LcsCmd.exe command-line tool provides a way to export and import all the pool-level and server-level settings as a group using the ImportPoolConfig, ExportPoolConfig, ImportServerConfig, and ExportServerConfig commands. Import and export settings ensure uniform configuration among servers or pools in your environment or to backup a configuration for recovery purposes. You can backup an existing configuration before making any changes so you can restore the existing settings if a problem arises.

When you import server-specific settings, any computer settings that are unique to a computer are not imported. For example, when you import settings from one server to another, the IP address is not overwritten. You must configure these settings manually.

Configuring Settings Using WMI Interfaces

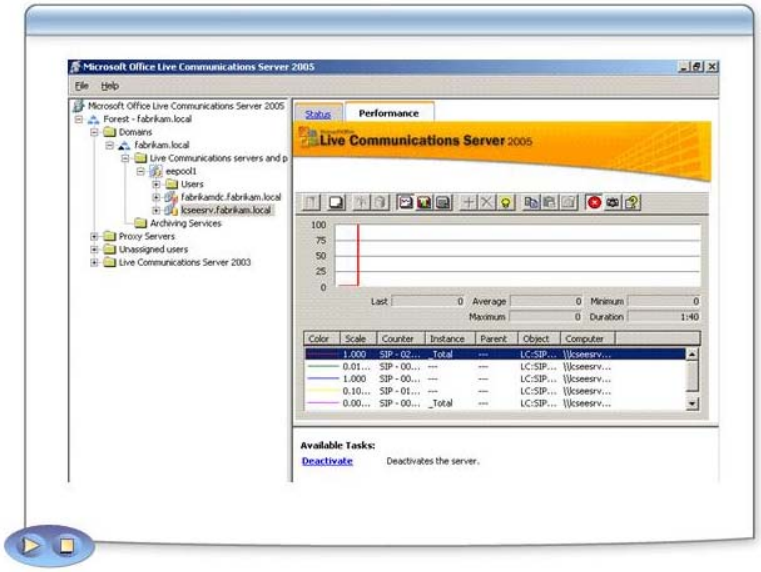
All settings available from the Live Communications Server 2005 administrative snap-in and from the LcsCmd.exe tools are also exposed in the WMI interfaces. Both the administrative snap-in and the command-line tools use the WMI interface to configure settings. Scripts and tools are available from the Live Communications Server 2005 Resource Kit. These interfaces are documented in the Live Communications Server 2005 Resource Kit documentation.

You can use these interfaces to programmatically manage your server and pool configuration settings. For example, you can create a script or tool that configures your required settings for static routes or archiving, and then use this script to uniformly configure multiple servers.

WMI is also used as the interface for all data stored for LCS. In addition to server-level and pool-level settings, you can also manage global settings, user Session Initiation Protocol (SIP) settings, and user data using WMI interfaces. The Resource Kit provides samples for the following tasks:

- Populating contacts for all users hosted on Enterprise Edition Server. For example, you can add all users in a department or a smaller company to everyone’s contact list so your users do not have to manually add these contacts.
- Enabling groups of users for LCS. You can programmatically enable users for SIP, host them on a specific server, and configure the required settings.

Using the LCS 2005 Administration Console



Introduction

Use the Live Communications Server 2005 administrative snap-in to manage any Live Communications Servers in your forest.

The console pane (the left pane) provides an Active Directory view of your Live Communications Server infrastructure and offers administrative tasks you can perform at various levels of this topology. The details pane (the right pane) displays status information. You can manage global settings that apply to all Live Communications Servers within your forest, domain settings, Enterprise pool and Standard Edition server settings, Proxy and Archiving service settings, and individual server settings for each of these types of servers. The console allows you to manage:

- **LCS Global Properties**. These are configured through the properties of the forest node, and include settings for:
  - Supported SIP domains
  - Client search options
  - User limitations
  - User archiving settings
  - Trusted access proxies
  - Global federation and public IM connectivity route
- **Pool-level Properties**. These are configured through the properties of the pool node, and include settings for:
  - Static routes for outbound connections
  - Server and client connection compression
  - Authentication protocol
  - Pool-specific federation route
  - Archiving

  - Address Book
- **Server-level Properties**. These are configured through the properties of the server node, and include settings for:
  - Inbound connections
  - MTLS authentication certificates
  - Logging

Console Views

Depending on the node you select in the tree pane, the views in the console vary slightly. If you select the Forest, Domain or Pool node in the tree pane, the details pane displays the Status tab and the Resources tab. However, if you select the node of server in the pool then the details pane displays the Status tab and the Performance tab.

Status Tab

The Status tab shows the current status of the selected node. For example if you select a Pool node and click the Status tab, it provides pool-specific information such as the SQL server instance the pool is running on, the number of Enterprise Edition servers in the pool, the network address and port number for any configured default federation route, the authentication protocol in use, archiving settings, and any configured static routes for outbound connections.

Resources Tab

The Resources tab contains links to various resources related to that selected node. If you select the Forest node and click the Resources tab, for example, it provides links to forest-specific resources in the Resources pane, such as technical documentation and help topics.

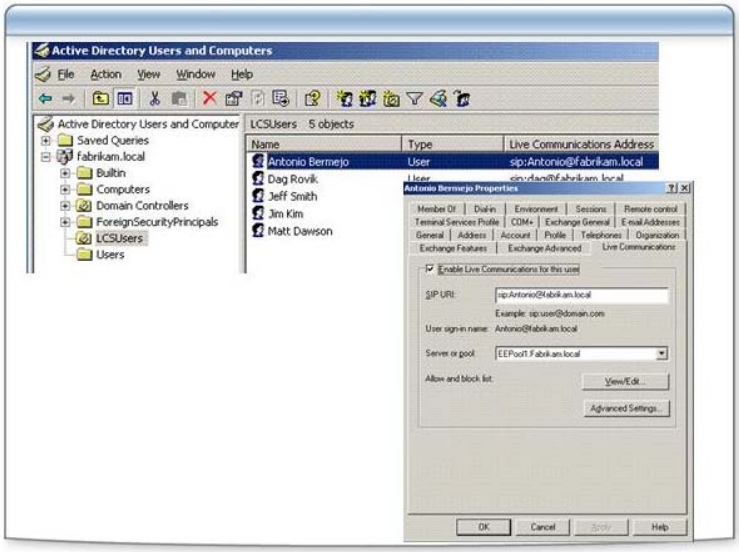
Performance Tab

The Performance tab monitors the performance of the selected server, so if you select a server and then click the Performance tab, it displays a limited and restricted version of the standard Microsoft Windows Server™ 2003 Performance console, which only displays a limited number of counter objects that are relevant and specific to LCS.

Task Pane

All of these console views have a Task pane that shows you the tasks available for the type of object you select. For example, it will allow you to run the Unprep task if you select the forest node, it will allow you to run the Remove Pool task if you select a pool node, and it will allow you to run the Unprep, Domain Add, and Domain Remove tasks if you select a domain node.

Creating and Enabling LCS 2005 Users



Introduction

After deploying your pool and performing the necessary configuration, you need to create and enable the user accounts in Active Directory that will be using the Live Communications Server services.

The following procedures are required to add users to their respective Live Communications Server. The Live Communications Server periodically requests its user information from, and stores its user information in, Active Directory.

Creating User Accounts

You create the user accounts for LCS in Active Directory.

To create user accounts, perform the following steps:

1. Open the **Active Directory Users and Computers** snap-in.
2. Create an organizational unit (OU) that contains all the users you want to create for LCS.
3. Right-click the OU, click **New**, and then click **User**.
4. Complete the New Object-User Wizard.

Enabling User Accounts for LCS

You can enable user accounts for LCS in one of two environments:

- Mail-enabled and mailbox-enabled user accounts
- User accounts that are not mail-enabled or mailbox enabled

To enable mail-enabled or mailbox-enabled user accounts for LCS, perform the following steps:

1. Log on to a server running LCS 2005 with SP1 or a computer with the Live Communications Server Administration tools installed that is also joined to an Active Directory domain. Use an account that has RTCDomainUserAdmins permissions.
2. Open **Active Directory Users and Computers**.
3. Right-click the user that you want to enable for LCS, and then click **Enable users for Live Communications**.

Tip You can enable multiple users for LCS by selecting them all first before right-clicking the selection and clicking Enable users for Live Communications.

---

4. On the **Welcome to Enable Users Wizard** page, click **Next**.
5. In **Select a Pool**, select the pool that will host this user, and then click **Next**.
6. Click **Finish**.

The SIP uniform resource identifier (URI) for this user is automatically populated by using the default e-mail address of the user, which is located in the E-mail field on the General tab of the user's properties in Active Directory Users and Computers.

To enable a user account for LCS that is not mail-enabled or mailbox-enabled, perform the following steps:

1. Log on to a server running LCS 2005 with SP1 or a computer with the Live Communications Server Administration tools installed that is also joined to an Active Directory domain. Use an account that has RTCDomainUserAdmins permissions.
2. Open **Active Directory Users and Computers**.
3. Right-click the user account you want to enable for LCS, and then click **Properties**.
4. Click the **Live Communications** tab, and then click **Enable Live Communications for this user**.

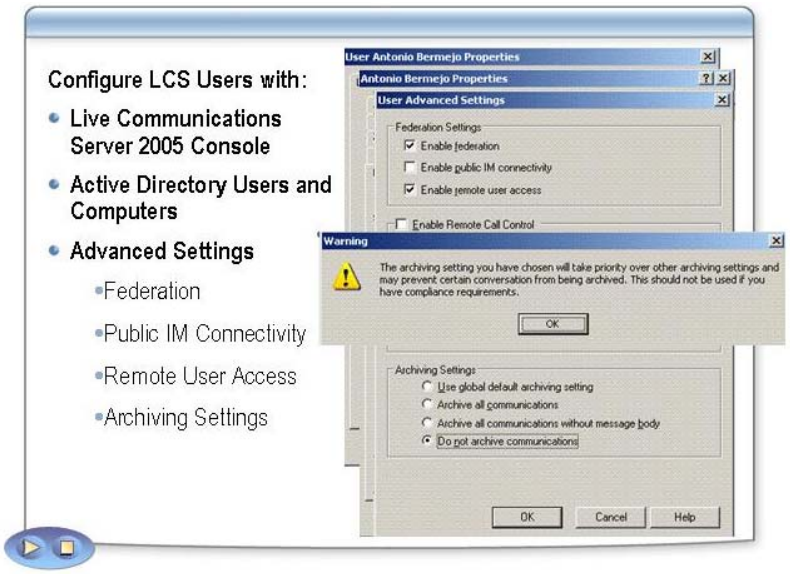
Note The Live Communications tab is only available on a LCS server or a server with the Live Communications Server Administration Tools installed.

---

5. In the SIP URI field, type: sip:*username@dnsrootdomainname*. (For example: sip:user1@fabrikam.local.)
6. Click the drop-down arrow in the **Server or pool** field, and click the pool you want to assign this user account to, keeping in mind that careful planning should take place to determine the number of users per server.
7. Click **OK**.

Important Ensure that the domain portion of the SIP URI used in step 5 is a supported domain. Supported domains are listed on the General tab of the Live Communications Server Global Properties page of the forest node.

Configuring LCS 2005 Users



Introduction

After successfully creating users and enabling them for LCS, you will need to configure your LCS users. The first thing to consider is which server to use for user configuration. There are two options for configuring your LCS users:

- Configure your LCS users from the LCS servers themselves using the Live Communications Server 2005 console.
- Install the LCS 2005 with SP1 Administration Tools on another server in the domain and configure them centrally from there.

Important It is recommended that you do not install LCS 2005 with SP1 on a domain controller, but you can install the LCS 2005 with SP1 Administration Tools on a domain controller for centralized management purposes.

LCS 2005 Administration Tools

The Live Communications Server 2005 with SP1 Administration Tools can be installed from either a Standard Edition or Enterprise Edition CD. You can run the Administration Tools on any of the following platforms:

- Microsoft Windows Server 2003
- Microsoft Windows 2000 Server SP4
- Microsoft Windows XP

Note Running the Administration Tools on Windows 2000 Professional is not supported.

Advanced Settings for LCS Users

Using the Advanced Settings option, you can manually configure your LCS users for federation, remote user access, and public IM connectivity. These user settings will override the global settings configured for LCS. Using this option, you can also specify the required archiving settings for your LCS users.

Note Setting the Archive flag for a user will not archive data if LCS has not enabled Archiving; this would only mark this user for archiving.

Enable Federation Settings for a single LCS User

To enable the different federation settings for a single LCS user using the Live Communications Server 2005 console, perform the following steps:

1. In the Live Communications Server 2005 console, expand the **Forest** node.
2. Expand the **Domains** node, expand the *DomainName* node, and then expand the **Live Communications servers and pools** node.
3. Expand the *PoolName n*ode, and then click **Users**.
4. Double-click the user.
5. Click **Advanced Settings**.
6. On the **User Advanced Settings** page, click **Enable federation** if you want this user to be able to have conversations with users from other companies.
7. Click **Enable public IM connectivity** if you want this user to be able to communicate with users of public IM provider services over the Internet.
8. Click **Enable remote user access** if you want this user to be able to access Live Communications Server 2005 from outside the corporate network.
9. Click **OK**.

Note To configure multiple users' settings, select the users first in the console and then right-click the selection and click **Configure users**. This will start the Configure Users Wizard.

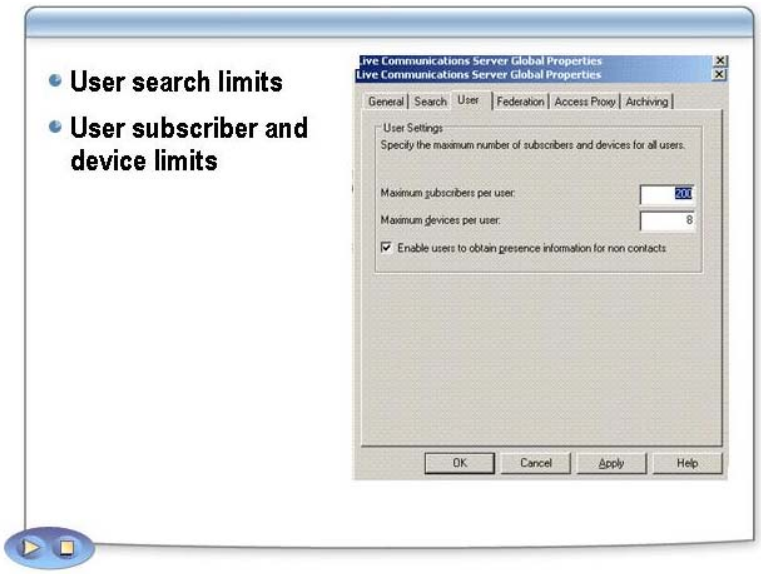
Configure Federation and Archiving Settings for multiple LCS Users

To configure federation and archiving settings for multiple LCS users using the Active Directory Users and Computers console, perform the following steps:

1. In the Active Directory Users and Computers console, select the users you want to configure federation and archiving settings for.
2. Right-click the selected users, and click **Configure Live Communications Users**.
3. On the **Welcome to the Configure Users Wizard** page, click **Next**.
4. On the **Configure User Settings** page, click **Configure Federation** if you want these users to be able to have conversations with users from other companies. (To block this feature, click the **Block Users** radio button).
5. Click **Configure Remote Access** if you want this user to be able to access Live Communications Server 2005 from outside the corporate network. (To block this feature, click the **Block Users** radio button).
6. Click **Configure Public IM Connectivity** if you want these users to be able to communicate with users of public IM provider services over the Internet. (To block this feature, click the **Block Users** radio button).
7. Click **Configure Archiving** if you want these users archiving settings to override the global archiving settings. Click one of the radio buttons to specify the required archiving settings for these users.

8. Click **Next**.
9. On the **Configure Operation Status** page, click **Finish**.

Configuring Client Limitations



Introduction

Using the forest node properties in the Live Communications Server 2005 console, you can specify limitations for your LCS users.

Search settings

The client search settings dictate the behavior of the server and the client application when a user searches for a contact. Settings include the maximum number of search result rows returned to the client, the default number of rows requested by the server, and the maximum number of outstanding requests per server.

To specify client search settings, perform the following steps:

1. Open the **Live Communications Server 2005** console, right-click the forest node, and then click **Properties**.
2. On the **Search** tab, configure the following settings:
   a. In **Maximum number of rows returned to the client**, enter the maximum number of search results you want to return to the client. The servers return this number or the number specified in the client request, whichever number is lower. In Windows Messenger, if the search results exceed this number, the user receives a message stating that too many search results were returned. Other clients might handle this situation differently. This value can be a number between 1 and 1000, and the default value is 20.
   b. In **Number of rows requested by the server**, enter the maximum number of rows that the server requests when sending the search to Active Directory. If the search exceeds this limit, Active Directory ignores any additional results and sends only the first *n* results, where *n* is the number requested by the server. This value can be a number between 1 and 3000, and the default value is 200.
   c. In **Maximum number of outstanding requests per server**, enter the maximum number of outstanding search requests permitted by the server. This setting is used to protect the server against possible denial of service attacks and to prevent the server from receiving too many

requests. This value can be a number between 1 and 500, and the default value is 80.

User settings

With the user settings you can specify the maximum number of subscribers and devices that are allowed per user. When a user adds another user to his or her contact list, the user subscribes to this contact's presence information. The maximum number of subscribers is the maximum number of people who can monitor a specific user's presence at a given time.

The maximum number of devices defines the number of devices on which LCS will monitor presence for a user. For example, if a user is logged into eight computers and the device maximum is eight, when the user logs on to a ninth computer, LCS will ignore presence on the ninth computer.

To specify the maximum number of subscribers and devices for each user in the forest, perform the following steps:

1. Open the **Live Communications Server 2005** console, right-click the forest node, and then click **Properties**.
2. On the **User** tab, configure the following settings:
   a. In **Maximum subscribers per user**, enter the maximum subscribers permitted per user. This value can be a number between 10 and 3000, and the default value is 200.
   b. In **Maximum devices per user**, enter the maximum number of devices for which LCS tracks presence information and allows communications for a user. This value can be between 1 and 64, and the default value is 8.

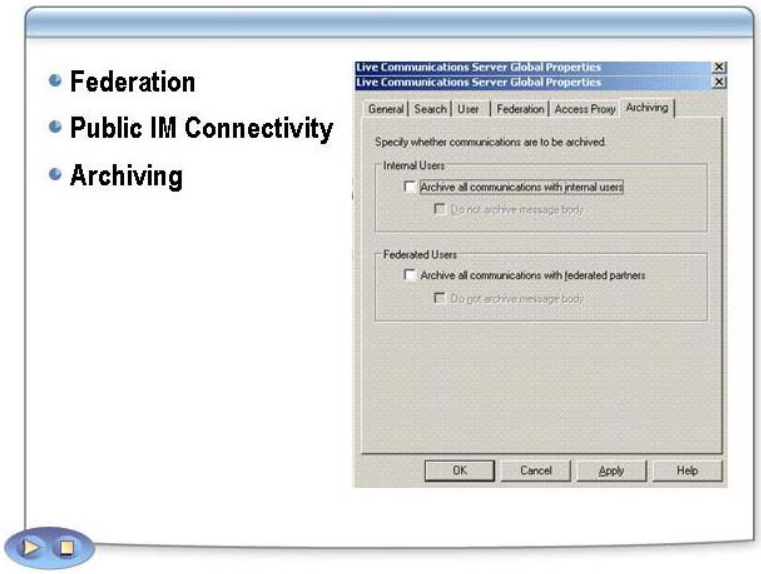
You can also enable users to obtain presence information for non-contact objects. If you want to permit users to obtain presence information for users who are not defined on a contact list, you must configure this setting.

To allow users to obtain presence information, perform the following steps:

1. Open the **Live Communications Server 2005** console, right-click the forest node, and then click **Properties**.
2. On the **User** tab, click the **Enable users to obtain presence information for non contacts** check box.

Note To perform all these tasks, you must be a member of the RTCDomainServerAdmins group.

Configuring Global Settings



Introduction

Using the forest node properties in the Live Communications Server 2005 console, you can specify the following global settings for your LCS forest:

- Federation and public IM connectivity
- Archiving settings for internal and federated communications

Federation and Public IM Connectivity

To support federation and public IM connectivity for your organization, you must enable them for your forest. This process also requires specifying the FQDN of the next hop server through which internal LCS route traffic destined for federated partners is passed.

Important Enabling federation and public IM connectivity does not by itself activate these features. You must also configure each of them on an Access Proxy and for your users. In addition, public IM connectivity requires LCS 2005 with SP1 and the purchase of an additional license.

To enable federation, public IM connectivity, or remote user access, perform the following steps:

1. Open the **Live Communications Server 2005** console, right-click the forest node, and then click **Properties**.
2. On the **Federation** tab, click **Enable Federation and public IM connectivity**.
3. In **Network address**, enter the FQDN of the Director, forwarding Proxy, or Access Proxy through which your internal servers route messages addressed to federated partners.
4. In **Port**, enter the port number to which your internal LCS servers send outbound messages to federated users or remote users. This port number must match the listening port number used by the Director or Access Proxy to which these servers route these messages. By default, the port number is 5061.
5. Click **OK**.

Archiving

At the forest level, you can configure the archiving settings that you want to enable for all users in your forest. You can override these settings for individual users on the User Properties sheet.

To archive all communications sent between internal users, perform the following steps:

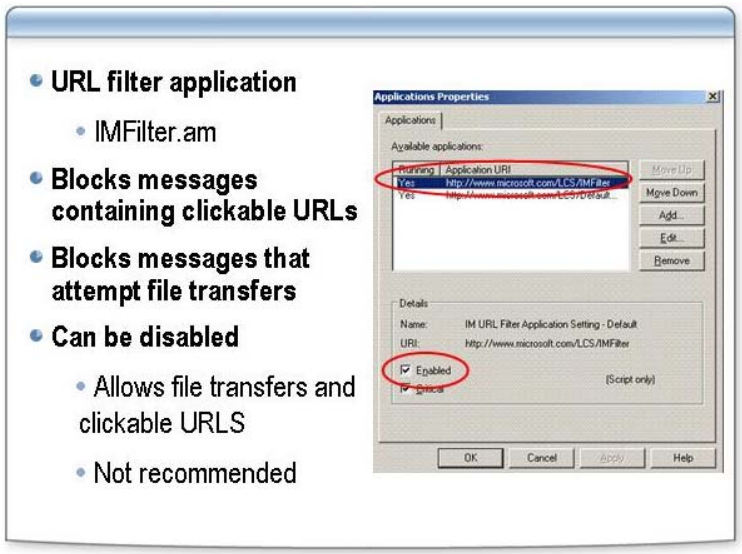
1. Open the **Live Communications Server 2005** console, right-click the forest node, and then click **Properties**.
2. On the **Archiving** tab, click the **Archive all communications with internal users** check box.
3. If you want to archive only usage data, such as the number of messages sent per user, click the **Do not archive message body** check box.

To archive all communications with federated partners, perform the following steps:

1. Open the **Live Communications Server 2005** console, right-click the forest node, and then click **Properties**.
2. On the **Archiving** tab, click the **Archive all communications with federated partners** check box.
3. If you want to archive only usage data, such as the number of messages sent per user, click the **Do not archive message body** check box.

Note To perform all these tasks you must be a member of the RTCDomainServerAdmins group.

Configuring IM Filtering



Introduction

LCS 2005 with SP1 enables you to take advantage of updates and improvements to LCS. Security enhancements in SP1 include a URL blocking filter that helps protect your organization and each enterprise-to-enterprise federated connection from unsolicited instant messages and IM-based worms.

URL Filter Application

The URL filter application, IMFilter.am, provides a way to block messages that contain clickable URLs or that attempt to initiate a file transfer.

IMFilter.am is installed and enabled by default on the following Live Communications Server 2005 SPI server roles:

- Standard Edition
- Enterprise Edition
- Director
- Access Proxy

IMFilter.am is not installed on Live Communications Server 2005 SP1 Proxy, Back-End Database, or Archiving servers.

Important IMFilter.am should always run as the first application on the server.

Blocking URLs

The filter blocks IM that contains clickable URLs by users running Communicator 2005 or Windows Messenger 5.1. Users will still be able to send a URL by pre-pending an underscore character (_) — for example, _contoso.com — but in order to follow the link, recipients will have to copy the URL (minus the underscore character) to their browsers. The time it takes to do this may itself act as a deterrent. An even more reliable deterrent is to educate your users about the danger of activating unknown URLs received through IM and e-mail, and to direct them as a matter of organizational policy not to do so.

Blocking File Transfer Attempts in a Message

The IMFilter.am recognizes any attempt to initiate a file transfer during an IM session and denies these requests. In Communicator, the user is notified that the request was blocked by system policy. In Windows Messenger 5.1, the request is simply blocked without informing the user of why the request was blocked.

Disabling the IM Filter

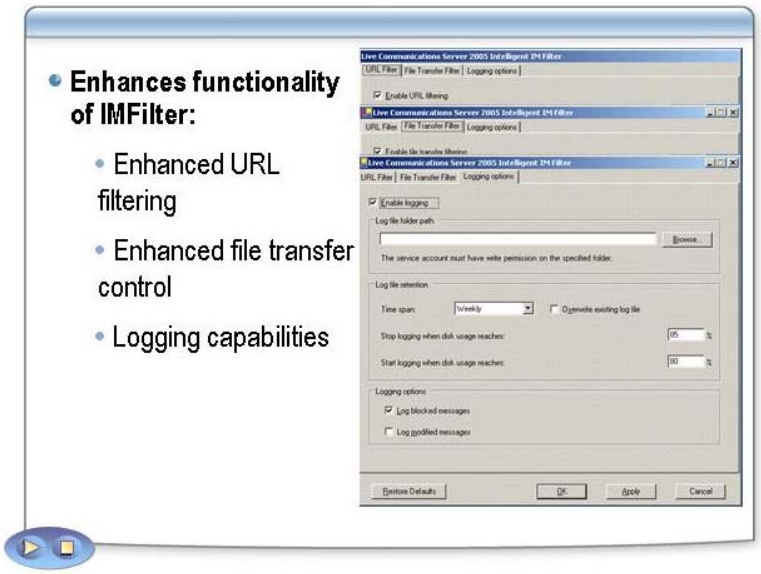
The filter can be disabled on one or more servers, but it is recommended to leave it enabled on all servers. If you must disable a filter on one or more servers, you can expect the following consequences:

- If you disable the filter on one server, IM between clients connected to that server will not be filtered. IM from a client connected to that server but destined for a client connected to another server will be filtered only on arrival at the destination server.
- If you disable the filter on some servers but not others, the results will be similar to those of the preceding case, depending on the origin and destination of the message.
- If you disable the filter on all servers, no IM will be scanned or blocked in your deployment. If a federated partner is running the filter, however, all IM sent to that partner will be blocked unless it too has disabled the filter.
- If you disable the filter on the Access Proxy, filtering will occur only after messages have passed into your internal network.

To disable the IMFilter application, perform the following steps:

1. Click **Start**, point to **All Programs**, **Administrative Tools**, and then click **Live Communications Server 2005**.
2. Expand the pool node and then expand the node of the server you want to disable the filter on.
3. Right click **Applications**, and then click **Properties**.
4. Under **Available applications**, click **http://www.microsoft.com/LCS/IMFilter**.
5. Under **Details**, clear the **Enabled** check box, and then click **OK**.

Filtering with the Intelligent IM Filter



Introduction

The Live Communications Server 2005 Intelligent IM Filter application allows administrators greater flexibility in the protection of their instant message networks than the default IMFilter application that is installed on all LCS 2005 with SP1 servers. The default IMFilter blocks all URLs and file transfers, but the Intelligent IM Filter's enhanced functionality permits several options for configuring how URLs and file transfers are handled. This new enhanced filter also includes configurable logging options and multiple performance counters for tracking network usage and identifying security or performance issues before they cause problems.

The Intelligent Instant Message Filter program helps protect your LCS 2005 with SP1 deployment against the spread of the most common forms of virus with minimal degradation to the user experience.

The Intelligent Instant Message Filter program enhances the functionality of the IMFilter program, which is installed by default on all Live Communications Servers with SP1, by providing the following:

- Enhanced URL filtering
- Enhanced file transfer control
- Logging capabilities

Enhanced URL Filtering

By using the Intelligent IM Filter program, you can configure URL filtering based on the following options available on the URL Filter tab:

- Allow hyperlinks to be sent in any conversation. If this option is selected, the hyperlink is active (clickable) or inactive depending on the client configuration. By default, URLs are sent as inactive in Microsoft Office Communicator 2005. The client behavior can be controlled by a Group Policy Object (GPO) policy.

Note Communicator has a GPO policy that can configure hyperlinks in an instant message as inactive. A security update was released for Window Messenger 5.1 with the same functionality. This server-side option is offered in case GPO is not used in the enterprise or a client that doesn't have the security feature is used.

- **Allow local intranet URLs**. If this option is selected, local intranet URLs are permitted in instant message conversations, regardless of the other settings. Be aware that local intranet URLs are defined on each individual Live Communications Server in the Internet Explorer security tab. This Internet Explore setting on each Live Communications Server determines what types of links the server recognizes as an intranet link.
- **Block all hyperlinks, both intranet and Internet, that contain any of the file extensions defined on the File Transfer Filter tab**. If this option is selected, the Intelligent IM Filter blocks any active intranet or Internet hyperlink that contains a file with an extension listed on the File Transfer Filter tab. When the instant message is blocked, an error message is returned to the sender.
- **Block instant messages that contain hyperlinks**. If this option is selected, Intelligent IM Filter blocks the delivery of any instant message that contains a hyperlink, and an error message is sent back to the client. This is the behavior of the IMFilter program, which is installed by default with Live Communications Server 2005 with SP1.
- **Allow instant messages that contain hyperlinks, but convert the links to plain text**. If this option is selected, the program prefixes the hyperlink with an underscore so that the hyperlink is not functional and the user cannot click it. Instead, the user must copy the URL, remove the underscore, and paste it into a Web browser to access the site. When you select this option, you can also customize a notice that is sent to users at the beginning of each instant message containing a hyperlink.
- **Allow instant messages that contain hyperlinks**. If this option is selected, the Intelligent IM Filter permits instant messages with active hyperlinks. You can also configure a warning that you want to insert at the beginning of each instant message to notify users of the potential danger of clicking on a link.

Enhanced File Transfer Control

The Intelligent IM Filter program controls how file transfers are enabled in a Live Communications Server deployment. The file transfer feature can also be disabled on the client using a GPO policy.

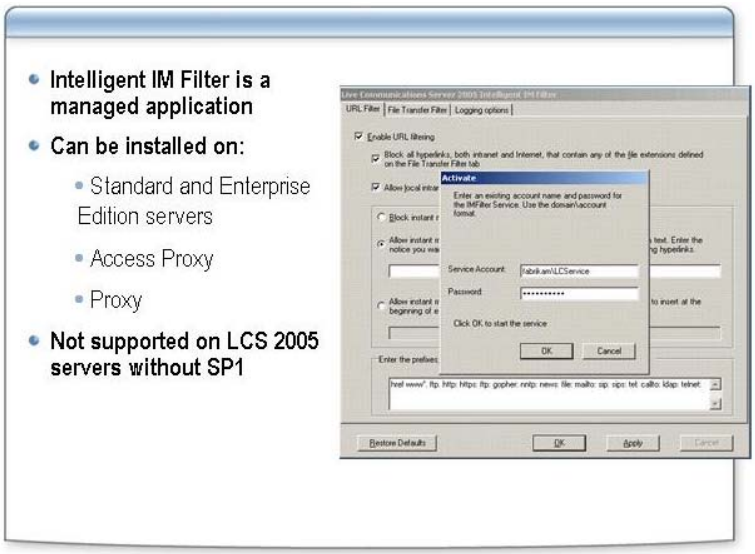
The following options are available on the server side using the Intelligent IM Filter:

- **Allow any file transfer request through the server**. If this option is selected, file transfer filtering is disabled, and any file transfer request going through the server is routed.
- **Block file transfer requests for specific file extensions**. If this option is selected, the administrator can specify file extensions that should be blocked by the server in file transfer requests. File transfer requests that contain defined file extension are blocked by the server, and an error message is returned to the client.
- **Block ALL file transfer requests**. If this option is selected, all file transfer requests are blocked by the server.

Logging Features

The LCS 2005 with SP1 Intelligent IM Filter offers logging capabilities so that you can monitor the SIP messages that were blocked or modified according to the settings you choose.

Installing the Intelligent IM Filter



Installing the Intelligent IM Filter

The Intelligent Instant Message (IM) Filter program is a managed application that can be installed on the following LCS roles:

- LCS 2005 with SP1, Standard and Enterprise Editions
- LCS 2005 with SP1, Access Proxy
- LCS 2005 with SP1, Proxy

The Intelligent IM Filter is not supported on LCS 2005 servers without SP1.

To install the Intelligent IM Filter, perform the following steps:

1. Log on to your LCS server.

   On an Access Proxy or Proxy in a workgroup, you must be logged on as a member of the local Adminstrators group. For any other server role, you must be logged on as a member of the RTCDomainServerAdmins group.
2. Download IIMFilterInstall.msi from the Microsoft Web site at http://r.office.microsoft.com/r/rlidLCS?clid=1033&p1=2&p2=iimfilterexe.
3. Double-click **IIMFilterInstall.msi**.
4. On the welcome page, click **Next**.
5. On the **License Agreement** page, click **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Ready to install the program** page, click **Install** to start the installation.
7. On the **Application successfully installed** page, click **Finish**.

Important Before installing the Intelligent IM Filter, please read the *Deploying Intelligent Instant Message Filter* guide in the **Additional Reading** folder. If you do not configure Intelligent IM Filter correctly, your messaging environment can be negatively affected.

Configuring the Intelligent IM Filter

To configure the Intelligent IM Filter program, you can use the program console that runs after you install the Intelligent IM Filter. The user interface of the program console is not integrated with the Live Communications Server administrative snap-in.

To start the Intelligent IM Filter console at a later time, click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005 Intelligent Instant Message Filter**.

Disabling the Intelligent IM Filter

You can disable the Intelligent IM Filter by stopping the service.

To disable the Intelligent IM Filter, perform the following steps:

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Services**.
2. Right-click **Live Communications Server 2005 Intelligent IM Filter**, and then click **Stop**.

Remove the Intelligent IM Filter

Use the following steps to remove the Intelligent IM Filter from a LCS server. When you remove Intelligent IM Filter, the default LCS filter program, IMFilter.am, is automatically re-enabled.

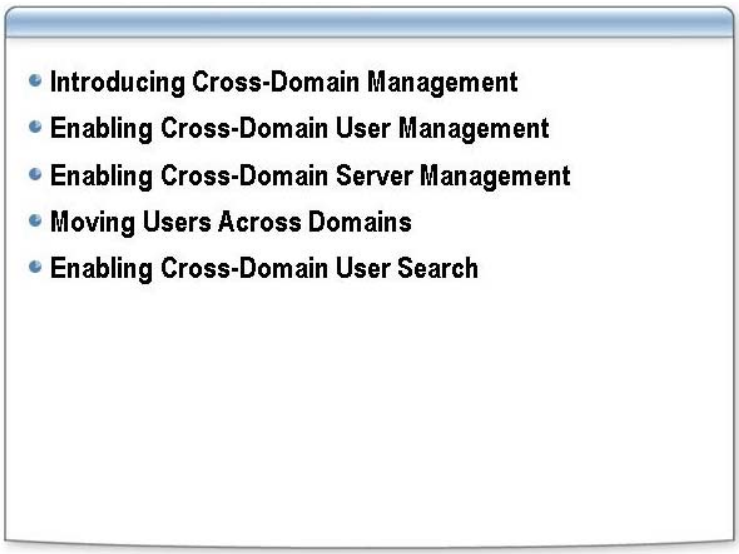
Refer to the "Deployment Considerations" section of the *Deploying Intelligent Instant Message Filter* guide in the **Additional Reading** folder for details on how the removal of the Intelligent IM Filter impacts the default program IMFilter.am.

Note If you uninstall LCS 2005 with SP1, the Intelligent IM Filter is not automatically removed. You must uninstall this program separately.

To remove the Intelligent IM Filter, perform the following steps:

1. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
2. Select **Microsoft Office Live Communications Server 2005 Intelligent Instant Message Filter**, and then click **Remove**.
3. Close **Add or Remove Programs**.

Lesson: Enabling Cross-Domain Management of LCS 2005 with SP1



Introduction

LCS 2005 allows administrators to manage LCS servers running in other domains. Users in one domain can also be authorized to search for users in other domains. This lesson explains the steps involved in enabling cross domain management and user search capabilities.

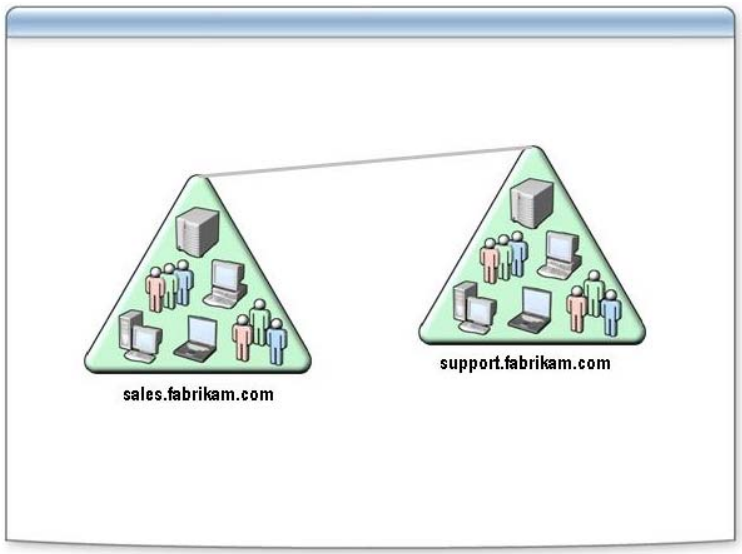
Cross domain management is necessary in a scenario where LCS domain administrator groups (RTCDomainUserAdmins or RTCDomainServerAdmins) from one domain need to manage users and servers, running LCS 2005 with SP1, in another domain.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the basic cross-domain management scenarios.
- Enable cross-domain user management.
- Enable cross-domain server management.
- Move users across domains.
- Enable cross-domain user searching capabilities.

Introducing Cross-Domain Administration



Introduction

There are four basic scenarios for cross-domain management with each one requiring different procedures to enable it.

- Management of LCS Active Directory objects in another domain, where administrators in one domain manage LCS 2005 users in another domain. To enable this scenario, you need to run the Domain Add command on another domain. Domain Add requires that the user running this procedure must have Domain Administrator credentials for the domain that is granting permissions.
- Management of settings and data on the pools or servers in another domain, where administrators in one domain manage servers running LCS 2005. To enable this scenario, you need to add the LCS 2005 administrative groups directly to the local LCS 2005 administrative groups on the relevant pool or servers. This requires that the user running this procedure must have Local Administrator credentials on the machine.
- Movement of users between domains. Another scenario where cross-domain administration permissions are necessary is to enable an administrator to move users between pools, where the pools and the users are in different domains. In this case, the administrator needs to be a member of the LCS 2005 domain administrator groups (RTCDomainServerAdmins or RTCDomainUserAdmins) for the domain(s) where the users are being moved from, and also needs to be a member of the LCS 2005 local administrative groups on the two pools.
- Enabling cross-domain user searching. This scenario is required only if your deployment has LCS deployed in more than one domain. If your topology has only LCS deployed in a single domain, then the single server domain search is enabled within this domain when you run the Prep Domain routine. To enable this scenario, you run the DomainAdd routine with the users-only option.

How to Use DomainAdd

The DomainAdd task is used to enable various cross-domain scenarios. The DomainAdd task grants an added domain, permissions on the generic LCS objects in the source domain. This task is similar to DomainAdd to Forest Root; however, DomainAdd grants permission in the source domain rather than the forest root.

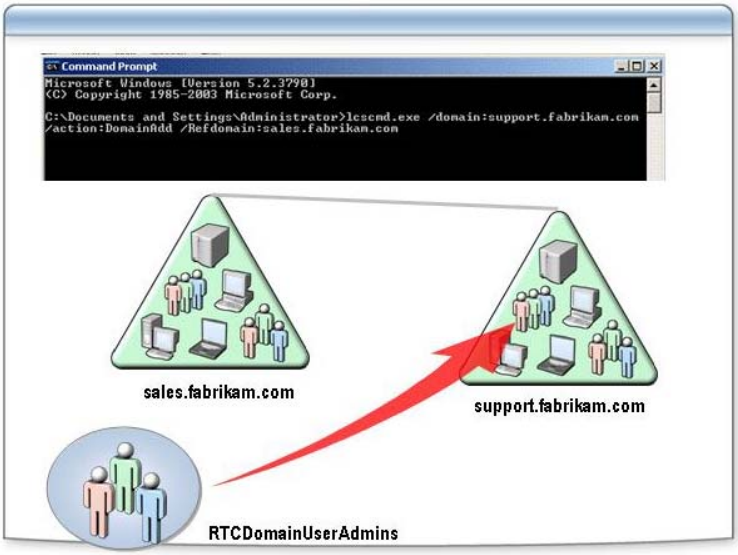
You can run DomainAdd in one of two ways to enable slightly different scenarios.

- DomainAdd with its default options gives permissions to the added domain on all the generic LCS objects in the source domain.
- DomainAdd with the users-only option gives the added domain permissions on a limited subset of the generic LCS objects in the source domain.

A high-level list of the Access Control Entries (ACEs) and specific capabilities enabled by DomainAdd is included in the following table.

DomainAdd Type	**Permissions Granted**
DomainAdd in default mode	■ ACEs for every user's RTC User property set, RTC User Search property, including authenticated user ACE for every user's RTC User Search property ■ Direct ACE for replicating directory changes, enabling the Live Communications Servers to synchronize user data from Active Directory ■ Direct ACEs to allow access on well-known containers such as the Systems, Users, and Computers containers ■ ACEs on the Microsoft container and RTC Server object, under the computer objects that are created during deployment of a Live Communications Server
DomainAdd with users-only switch	■ Authenticated user ACE for every user's RTC User Search property ■ ACE for replicating directory changes

Enabling Cross-Domain User Administration



Introduction

The slide figure illustrates how enabling cross-domain administration is achieved. The fictitious company Fabrikam hosts user and LCS servers in two separate domains.

In this scenario, administrators from the sales.fabrikam.com domain need to manage users in the support.fabrikam.com domain. Administrators in sales.fabrikam.com will configure and enable users in support.fabrikam.com for LCS. To achieve this, perform the following steps:

1. Verify that Prep Domain has been successfully run in support.fabrikam.com.
2. Run DomainAdd with its default parameters to add permissions to the sales.fabrikam.com administrator groups for the user domain, support.fabrikam.com.

Enable cross-domain user administration

To enable cross-domain user administration where administrators in the sales.fabrikam.com domain can manage users in the support.fabrikam.com domain, run DomainAdd with default parameters in the support.fabrikam.com users domain to grant permissions to administrators in the sales.fabrikam.com. The RTCDomainUserAdmins in sales.fabrikam.com can now enable and manage users in support.fabrikam.com for LCS 2005. However, the administrators from sales.fabrikam.com cannot manage any user data for users in support.fabrikam.com because this data is stored on the LCS server in support.fabrikam.com. This functionality requires cross-domain server administration permissions.

To grant one domain, permission to administer users in another domain, perform the following steps:

1. Log on to a computer joined to a domain with Domain Admins credentials in the users domain (the domain that needs to be managed by administrators in another domain).
2. Run the following LcsCmd.exe command:

```
LcsCmd.exe /domain[:<FQDN for users domain, to be managed>]
/action:DomainAdd /RefDomain:<FQDN for domain of the user
administrators>
```

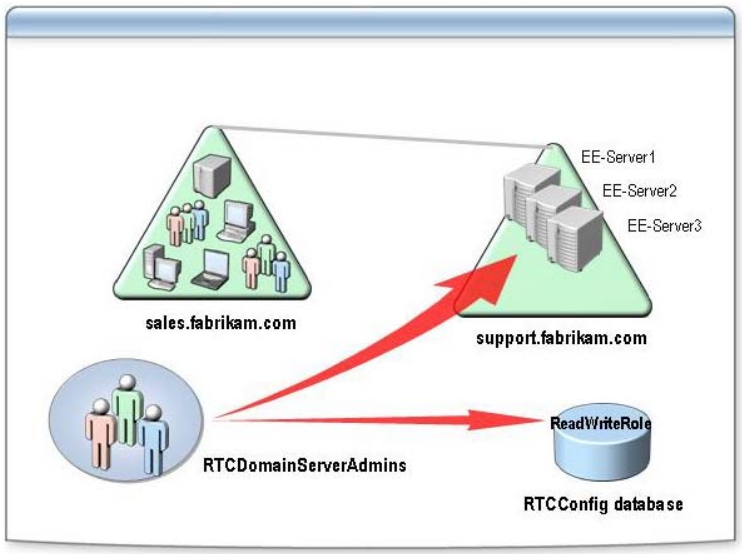
   For example:

```
LcsCmd.exe /domain:support.fabrikam.com /action:DomainAdd
/Refdomain:sales.fabrikam.com
```

3. Verify that the DomainAdd procedure succeeded by checking that the LcsCmd log file indicates “Success” and has no errors. You can also run the following verification command:

```
LcsCmd.exe /domain[:<FQDN for users domain, to be managed>]
/action:CheckDomainAddState /Refdomain:<FQDN for domain of
the user administrators>
```

Enabling Cross-Domain Server Administration



Introduction

The previous scenario does not allow the administrators in sales.fabrikam.com to manage the data of the support.fabrikam.com domain users stored on the LCS servers. This data includes contacts and ACEs for users and the user data that is imported when users are moved. To allow administrators in sales.fabrikam.com to manage this data for users in support.fabrikam.com, you must enable cross-domain server management.

Cross-domain server management involves administrators from one domain managing LCS servers in another domain. It can also include administrators in one domain managing server-based user data stored on LCS servers in another domain.

To allow administrators in one domain the ability to manage LCS servers and data in another domain, grant the administrators or the administrative groups such as RTCDomainServerAdmins of one domain, the following permissions:

- Permissions on the relevant LCS servers in the source domain.

  To grant permissions to a LCS server, the administrative group in the target domain must be given membership of the RTC Local Administrators domain local group and the local administrators group on the relevant LCS servers in the source domain.

- Permissions on the configuration database (RTCConfig), which stores pool-level settings.

  To grant permissions to the configuration database the administrative group in the target domain must be granted ReadWriteRole permissions on the configuration database of the relevant Standard Edition server or Enterprise pool in the source domain. On Standard Edition servers, the RTC Local Administrators group already has this permission, so this step is not required. For an Enterprise pool, the target domain administrative group (RTCDomainServerAdmin) must be added to the RTCConfig database ReadWriteRole.

Enable cross-domain server administration

To enable cross-domain server administration and allow administrators in one domain the ability to manage a pool or server in another domain, perform the following steps:

- Add the RTCDomainServerAdmins group from sales.fabrikam.com to the RTC Local Administrators group on the three Enterprise Edition servers of the same Enterprise pool in the support.fabrikam.com domain (EE-Server1, EE-Server2, and EE-Server3).
- Grant the RTCDomainServerAdmins group from sales.fabrikam.com, group access and database permissions on the configuration database (RTCConfig) of the Enterprise pool, which is stored on the back-end database. Both Standard Edition servers and Enterprise pools use the RTCConfig database to store pool-level settings.

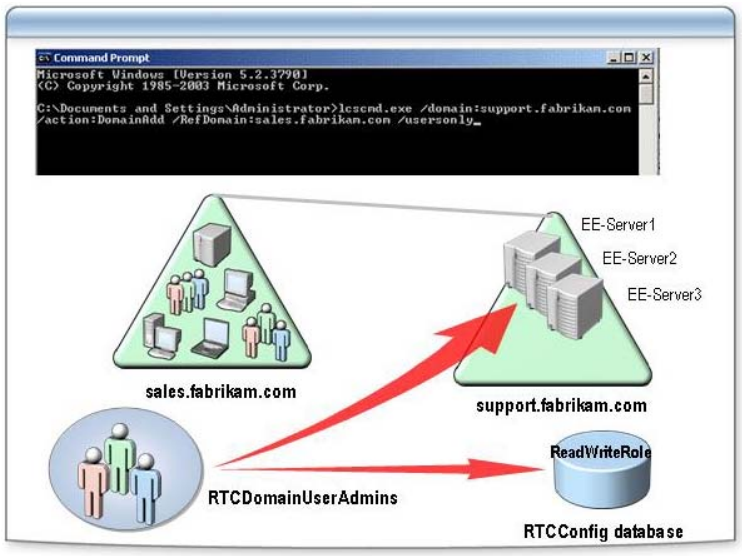
To add an administrative group to the local server administration group, perform the following steps:

1. Log on to the target server running LCS 2005 with SP1 as a user with at least local administrator credentials for the server.
2. To grant this group permission to manage this server, add the other domain's RTCDomainServerAdmins groups as members of the RTC Local Administrators group.

To grant access permissions to the administrative group for the RTCConfig database, perform the following steps:

1. Do one of the following:
   c. For an Enterprise pool, log on to the LCS 2005 with SP1 back-end database server.
   d. For a Standard Edition server, log on to the server itself.
2. Open the SQL Enterprise Manager snap-in.
3. Connect to the instance used by the LCS 2005 with SP1 server. For an Enterprise pool, specify the SQL back-end server and instance used by the pool. For a Standard Edition Server, the instance is (local)\rtc.
4. Add a new login to the Security node, using the RTCDomainServerAdmins group as the new login.
5. On the Database Access tab for the new login, on the RTCConfig database, permit the ReadWriteRole database role.

Moving Users Across Domains



Introduction

Moving users from one domain to another can require similar steps as those involved in configuring cross-domain user or server administration. Use the following guidelines:

- If the users being moved reside in multiple domains and the servers involved are in a single domain, run DomainAdd and add the server domain with the users-only option to the domain hosting the users.

Note The optional /usersonly switch specifies whether the DomainAdd action is to be performed using restricted permissions (only the Active Directory permissions relevant to a users-only domain should be included in the action). Omitting the /usersonly switch defaults to giving the target domain's groups the full set of LCS server permissions, including Active Directory permissions.

An RTCDomainUserAdmins administrator from the server domain should run this procedure.

- If the servers to and from which you want to move users are located in multiple domains, then the administrator from each domain, a member of RTCDomainUserAdmins, requires administrative permissions on the relevant LCS servers in each of the other server domains.

Use the following steps to grant the necessary permissions:

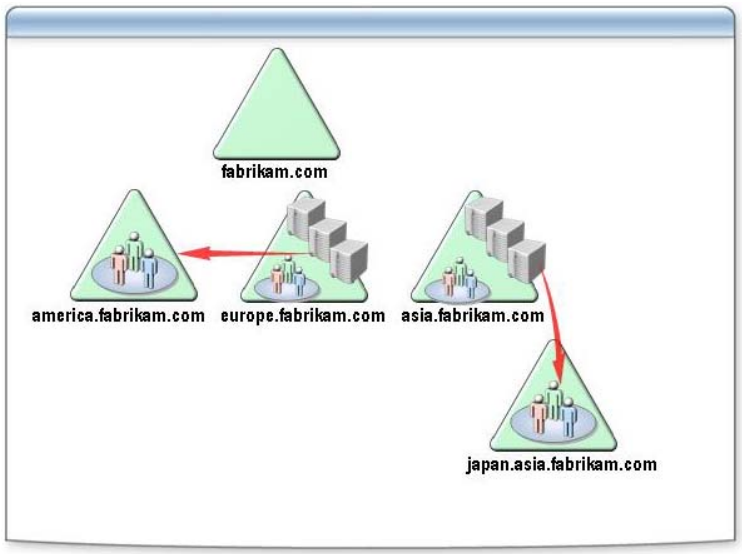
- **Grant permissions on the relevant LCS servers in the source domain**. To grant permissions to a LCS server, the administrative group in the target domain must be given membership in the RTC Local Administrators groups on the relevant LCS server in the source domain.
- **Grant permissions to the Configuration Database (RTCConfig), which stores pool-level settings**. To grant permissions to the configuration database, the administrative group in the target domain must be granted ReadWriteRole permissions on the configuration database (RTCConfig) of the relevant Standard Edition server or Enterprise pool in the source domain.

- If the users and servers involved in the move users operation are both in multiple domains, then use the following guidelines.

  An RTCDomainUserAdmins administrator from the server domain should run this procedure.

  - Run DomainAdd and add the server domain with the users-only option to the domain hosting the users.
  - Grant the RTCDomainUserAdmins in the target domain membership of the RTC Local User Administrators groups on the relevant LCS server in the source domains to and from which users are being moved.
  - Grant the RTCDomainUserAdmins in the target domain the ReadWriteRole database role permissions on the configuration database (RTCConfig) of the relevant Standard Edition server or Enterprise pool in the source domains to and from which users are being moved.

Enabling Cross-Domain User Search



Introduction

This procedure is necessary only in a scenario where there are multiple domains of LCS server 2005 users, and users in at least one domain need to be able to search users in other domains. Through this procedure, you can get domain permissions on another domain so that authenticated users in one domain will have permissions to search users in the other domain.

To enable cross-domain user search in topologies with multiple LCS domains, you must ensure that each LCS domain has permissions to search users on every user domain. You enable cross-domain search by running DomainAdd with the users-only option to grant the added domain permissions to search in the source domain.

If you have two domains (Domain A and Domain B) that are each hosting LCS servers and users in their specific domains only, and you want to enable search between these domains, you must:

- Run DomainAdd with the users-only option to add Domain B to Domain A. This step allows servers in Domain B to search for users in Domain A.
- Run DomainAdd with the users-only option in Domain B and add Domain A. This step allows servers in Domain A to search for users in Domain B.

Cross-Domain User Search in a Complex Environment

To understand how cross-domain user search is enabled in a more complex environment, consider the fictitious company Fabrikam.com in the slide figure. The company has two domains with LCS servers deployed (europe.fabrikam.com and asia.fabrikam.com), and two users-only domains (japan.asia.fabrkam.com, hosted by asia.fabrikam.com and america.fabrikam.com, hosted by europe.fabrikam.com).

In the Fabrikam environment, the necessary Active Directory preparation steps have been performed in each server domain and the required steps have also been taken to enable the server domains to host and administer the users in their respective users-only domains. At this point the following search capabilities exist:

- LCS servers in europe.fabrikam.com can search only for users in its own domain and in america.fabrikam.com.
- LCS servers in asia.fabrikam.com can search only for users in its own domain and in japan.asia.fabrikam.com.

To enable complete cross-domain user search, administrators at Fabrikam need to run DomainAdd with the users-only option for every user domain to add any domain with servers that does not currently have permissions. This requires the following steps:

- Run DomainAdd with the users-only option on america.fabrikam.com to add asia.fabrikam.com, to allow LCS servers in asia.fabrikam.com to search users in america.fabrikam.com.
- Run DomainAdd with the users-only option on europe.fabrikam.com to add asia.fabrikam.com, to allow LCS servers in asia.fabrikam.com to search users in europe.fabrikam.com.
- Run DomainAdd with the users-only option on asia.fabrikam.com to add europe.fabrikam.com, to allow LCS servers in europe.fabrikam.com to search users in asia.fabrikam.com.
- Run DomainAdd with the users-only option on japan.asia.fabrikam.com to add europe.fabrikam.com, to allow LCS servers in europe.fabrikam.com to search users in japan.asia.fabrikam.com.

Steps to Enable Cross-Domain User Search

Use the following procedure to enable cross-domain search. This procedure requires a user with Domain Admins credentials in the relevant user domain that is giving permissions to the server domain.

To enable a server domain to search a user domain, perform the following steps:

1. Log on to a computer joined to a domain with an account that has Domain Admins credentials for the user domain (the domain with the users that you want to search).
2. Run the following LcsCmd.exe command:

```
LcsCmd.exe /domain[:<FQDN of the user domain the server
domain want to search users from>] /action:DomainAdd
/RefDomain:<FQDN of the server domain > /usersonly
```

For example:

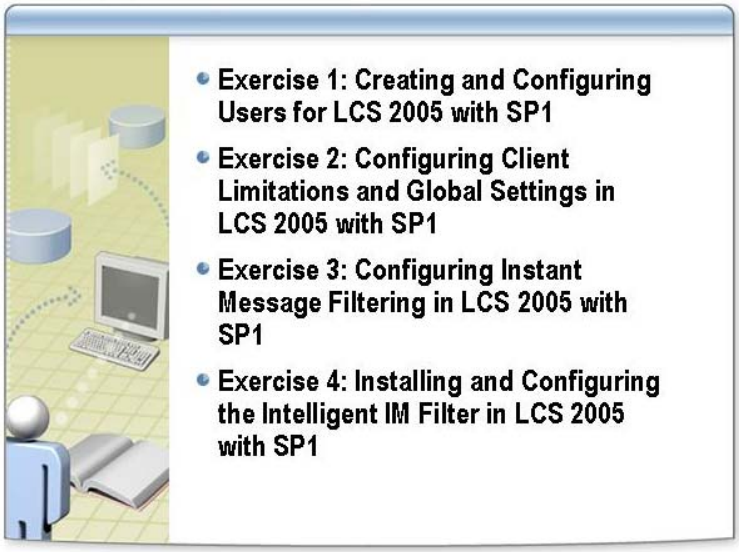
```
LcsCmd.exe /domain:japan.asia.fabrikam.com
/action:DomainAdd /Refdomain:europe.fabrikam.com /usersonly
```

3. Verify that the DomainAdd procedure succeeded, either by checking that the LcsCmd log file indicates “Success” and has no errors, or by running the following LcsCmd.exe command:

```
LcsCmd.exe /domain[:<FQDN for user domain>]
/action:CheckDomainAddState /Refdomain:<FQDN of server
domain> /usersonly
```

Note If DomainAdd has already been run for some reason, such as for cross-domain administration, then DomainAdd does not need to be run again, and the cross-domain user search permissions have already been granted.

Lab 4: Administering and Configuring LCS 2005 with SP1



Objectives

After completing this lab, you will be able to:

- Create, enable and configure users for LCS 2005 with SP1.
- Configure client limitations and global settings in LCS 2005 with SP1.
- Configure instant message filtering in LCS 2005 with SP1.
- Configure the Intelligent IM Filter application in LCS 2005 with SP1.

Estimated time to complete this lab: **45 minutes**

Important: At the end of this lab, close down the VPC images and delete changes.

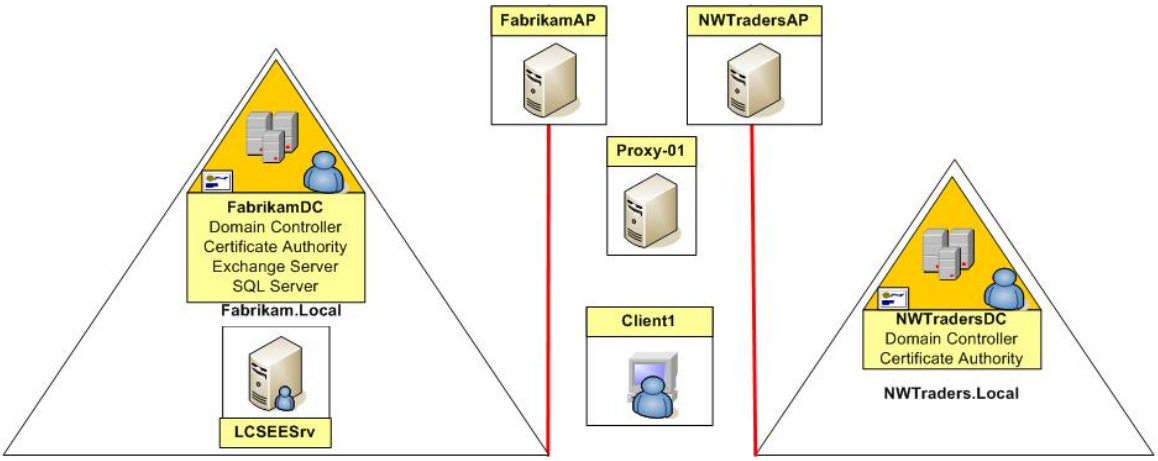
Introduction

Matt Dawson, the Fabrikam network administrator, wants to implement numerous administrative controls on the Fabrikam network. However, he is keen to see how these controls apply in a pilot environment before he rolls applies the changes to all his users. Hence, he is going to create some pilot user accounts, and then check how the policies apply to those accounts.

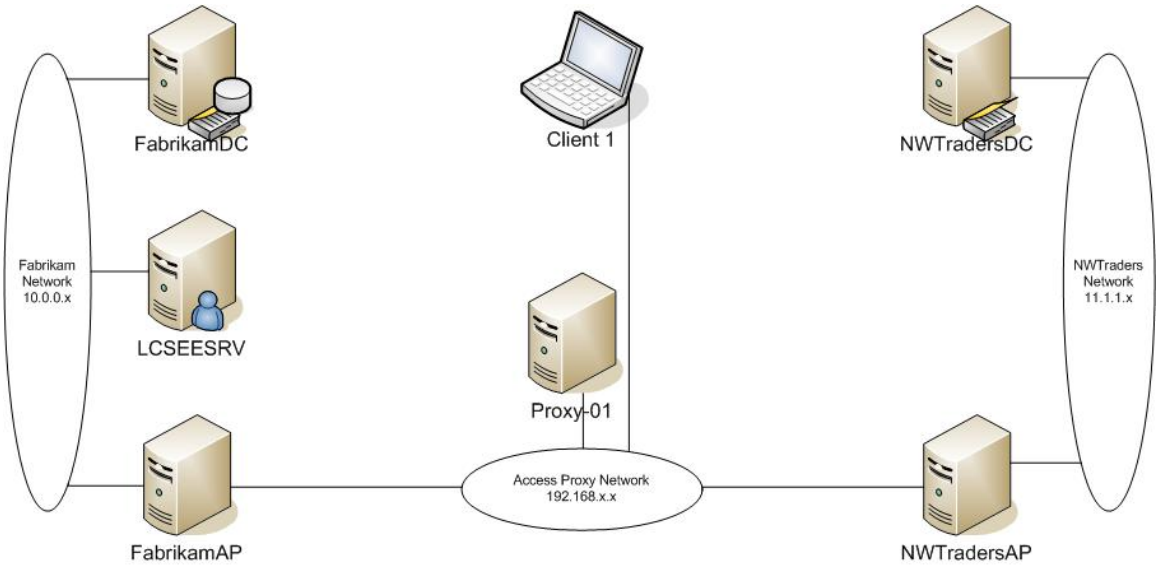
In this lab, you will use Active Directory Users and Computers to create and enable some users for LCS 2005 with SP1. Then you will use the Live Communications Server 2005 console to configure the users for LCS 2005 with SP1. Next, you will configure and test some client limitation settings for LCS users in the forest and view the global federation settings for LCS, and then you will use the default IMFilter.am application to configure and test the URL filtering and file transfer blocking capabilities. Finally, you will use the downloadable Intelligent IM Filter application to configure and test its enhanced URL filtering and file-transfer-blocking features.

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 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-LCSEESRV-B	LCSEESRV

Important: You should start these virtual PC images prior to commencing the labs in this module.

On 7034A-FabrikamDC-B, a Service Control Manager message box may appear, with the following message: At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details. If this message appears, click OK, and continue. The message refers to the Kerberos Key Distribution Center service. However, this service starts properly.

On 7034A-LCSEESRV-B, the Live Communications Server service may fail to start if FabrikamDC has not completely booted before starting LCSEESRV. Before you start the lab, check that the Live Communications Server service on LCSEESRV is running.

At the end of the lab, close down these virtual PC images without saving changes.

Exercise 1
Creating and Configuring Users for LCS 2005 with SP1

Scenario
As part of the pilot project, Matt wants to create some users and enable them for LCS.

Description
In this exercise, you will use create some users and then enable those users to use LCS 2005 with SP1. Then you will configure the users' settings for LCS.

Tasks	Detailed Steps
 **Important:** Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
1. Create users for LCS 2005 with SP1.	**a.** Log on to **7034A-FabrikamDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. **c.** Right-click the **LCSUsers** OU, point to **New**, and then click **User**. **d.** On the **New Object - User** page, in the **First name** box, type **Max**. **e.** In the **Last name** box, type **Stevens**. **f.** In the **User logon name** box, type **max**. Note that the field after the User logon name shows **@fabrikam.local**. **g.** Click **Next**. **h.** In the **Password** and **Confirm password** boxes, type **pass@word1**. **i.** Clear the **User must change password at next logon** check box. **j.** Click **Next**. **k.** Accept the default Exchange mailbox parameters, and then click **Next**. **l.** Click **Finish**. **m.** Repeat steps **c** to **l** to create four more users as follows: User 1 • First name: **Rebecca** • Last name: **Laszlo** • User logon name: **rebecca** • Password: **pass@word1** User 2 • First name: **Kim** • Last name: **Akers** • User logon name: **kimak** • Password: **pass@word1**

	User 3 • First name: **Kim** • Last name: **Abercrombie** • User logon name: **kimab** • Password: **pass@word1** User 4 • First name: **Kim** • Last name: **Ralls** • User logon name: **kimra** • Password: **pass@word1** **n.** Leave the Active Directory Users and Computers console open.
2. Enable users for LCS 2005 with SP1.	**a.** Using the CTRL key, select all five of the new users you just created. **b.** Right-click the selection, and then click **Enable users for Live Communications**. **c.** On the **Welcome to Enable Users Wizard** page, click **Next**. **d.** On the **Select a Pool** page, from the drop-down list, ensure that the **EEPool1.Fabrikam.local** pool is selected, and then click **Next**. **e.** On the **Enable Operation Status** page, note that there should be five successful operations listed, and then click **Finish**. **f.** Right-click in a blank area of the details pane, and then click **Refresh**. *Note that the Live Communications Address column now contains an entry for the new users.* **g.** Double-click **Kim Akers**. **h.** On the **Kim Akers Properties** page, click the **Live Communications** tab. *Note that the SIP URI for a mailbox-enabled user is automatically populated by using the user's default e-mail address.* **i.** Click **Advanced Settings** . *Note that by default new LCS-enabled users do not have their federation or archiving settings configured.* **j.** In the **User Advanced Setting** dialog box, click **OK**. **k.** On the **Kim Akers Properties** page, click **OK**. **l.** Close Active Directory Users and Computers.
3. Configure users for LCS 2005 with SP1.	**a.** Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Live Communications Server 2005**. **b.** In the **Microsoft Office Live Communications Server 2005** console, expand the **Forest – fabrikam.local** node, and then expand the **Domains** node. **c.** Expand the **fabrikam.local** node, and then expand the **Live Communications servers and pools** node. **d.** Expand the **eepool1** node, and then click **Users**. **e.** Using the CTRL key, select all five of the new users you created in the earlier task.

	f. Right-click the selection, and then click **Configure users**. **g.** On the **Welcome to the Configure Users Wizard** page, click **Next**. **h.** On the **Configure User Settings** page, click **Configure Federation**, click **Configure Remote Access**, and then click **Configure Archiving**. **i.** Click **Next**. **j.** On the **Configure Operation Status** page, note that there should be five successful operations listed, and then click **Finish**. **k.** Leave the Live Communications Server 2005 console open.

Exercise 2
Configuring Client Limitations and Global Settings in LCS 2005 with SP1

Scenario

Now that he has enabled and configured his users for LCS 2005, Matt wants to verify the global federation settings and test some client limitation settings on his LCS 2005 with SP1 servers.

Description

In this exercise, you will use the Live Communications 2005 console to configure some limitations on the LCS clients in the forest, and then view the global federation settings in LCS for the forest.

Tasks	Detailed Steps
Important: Perform this part of the exercise on the 7034A-FabrikamDC-B virtual machine.	
1. Configure client limitations for LCS 2005 with SP1.	**a.** On **7034A-FabrikamDC-B**, in the **Microsoft Office Live Communications Server 2005** console, right-click the **Forest – fabrikam.local** node, and then click **Properties**. **b.** In the **Live Communications Server Global Properties** dialog box, click the **Search** tab. **c.** Under **Search Settings**, in **Maximum number of rows returned to the client**, type **1**. **d.** Click the **User** tab. **e.** Under **User Settings**, in **Maximum subscribers per user**, type **10**. **f.** In **Maximum devices per user**, type **2**. **g.** Click the **Federation** tab. *Note that, by default, federation and public IM connectivity is not enabled on your LCS servers in the forest.* **h.** Click the **Archiving** tab. *Note that, by default, communications are not archived on your LCS servers in the forest.* **i.** Click **OK**. **j.** Right-click **fabrikamdc.fabrikam.local**, and then click **Stop**. **k.** Wait for a moment until the server stops, right-click **fabrikamdc.fabrikam.local**, and then click **Start**.
2. Sign in to Windows Messenger on FabrikamDC.	**a.** Click **Start**, point to **All Programs**, and then click **Windows Messenger**. **b.** In the **Sign In to a SIP Communications Service** dialog box, in the **Sign-in name** and **User name** boxes, type **max@fabrikam.local**. **c.** In the **Password** box, type **pass@word1**. **d.** Click **OK**.

Important: Perform this part of the exercise on the 7034A-LCSEESRV-B virtual machine.	
3. Sign in to Windows Messenger on LCSEESRV.	**a.** On **7034A-LCSEESRV-B**, click **Start**, point to **All Programs**, and then click **Windows Messenger**. **b.** On the **Tools** menu, click **Options**. **c.** In the **Options** dialog box, click the **Accounts** tab. **d.** Click **My contacts include users of a SIP Communications Service**. **e.** Click **Advanced**. **f.** In the **SIP Communications Service Connection Configuration** dialog box, click **Configure settings**. **g.** In the **Server name or IP address** box, type **eepool1.fabrikam.local**. **h.** Under **Connect using**, click the **TLS** option. **i.** Click **OK**, and then click **OK** again. **j.** Click **Click here to sign in**. **k.** In the **Connect to Messaging Services** dialog box, ensure that **SIP Communications Service** is selected, and then click **OK**. **l.** In the **Sign In to a SIP Communications Service** dialog box, in the **Sign-in name** box, type **Rebecca@fabrikam.local**. **m.** Click **OK**. **n.** In the **Sign In to a SIP Communications Service** dialog box, in the **User name** box, type **rebecca@fabrikam.local**. **o.** In the **Password** box, type **pass@word1**. **p.** Click **OK**.
4. Add a contact for Max Stevens on LCSEESRV.	**a.** In **Windows Messenger**, click the **Tools** menu, and then click **Add a Contact**. **b.** On the **Add a Contact** page, click **Search for a contact**, and then click **Next**. **c.** On the next **Add a Contact** page, in the **First Name** box, type **max**, and then click **Next**. **d.** On the **Search results** page, click **Max Stevens**, and then click **Next**. **e.** On the **Success** page, click **Finish**. **f.** **Max Stevens** should now appear in the **All Contacts** list.
Important: Perform this part of the exercise on the 7034A-FabrikamDC-B virtual machine.	
5. Allow the contact to view your presence and add them to your contact list on FabrikamDC.	**a.** Switch back to the **7034A-FabrikamDC-B** virtual machine. A **Windows Messenger** dialog box appears, informing you that rebecca@fabrikam.local has added you to her contact list. **b.** Ensure that **Allow this person to see when you are online and contact you** is selected.

	c. Ensure that **Add this person to my contact list** is checked, and then click **OK**. *Note that Rebecca Laszlo is now in your All Contacts list, and is online.*
6. Add Kim Abercrombie to your contacts on FabrikamDC.	**a.** In **Windows Messenger**, click the **Tools** menu, and then click **Add a Contact**. **b.** On the **Add a Contact** page, click **Search for a contact**, and then click **Next**. **c.** On the next **Add a Contact** page, in the **First Name** box, type **kim** and then click **Next**. The message **Too many matches were found** will appear. **d.** Click **Cancel**.
7. Modify the client limitation setting for LCS 2005 with SP1.	**a.** Switch back to the **Live Communications Server 2005** console. **b.** Right-click the **Forest – fabrikam.local** node, and then click **Properties**. **c.** Click the **Search** tab. **d.** Under **Search Settings**, in the **Maximum number of rows returned to the client** box, type **5**. **e.** Click **OK**. **f.** Right-click **fabrikamdc.fabrikam.local**, and then click **Stop**. **g.** Wait for a moment until the server stops, right-click **fabrikamdc.fabrikam.local**, and then click **Start**.
8. Add Kim Abercrombie to your contacts on FabrikamDC.	**a.** Switch back to **Windows Messenger**. **b.** Click the **Tools** menu, and then click **Add a Contact**. **c.** On the **Add a Contact** page, click **Search for a contact**, and then click **Next**. **d.** On the next **Add a Contact** page, in the **First Name** box, type **kim**, and then click **Next**. **e.** On the **Search results** page, click **Kim Abercrombie**, and then click **Next**. **f.** On the **Success** page, click **Finish**. Kim Abercrombie should now appear in the All Contacts list. **g.** Close the Windows Messenger window. **h.** In the system tray, right-click the Windows Messenger icon, and then click **Exit**.
Important: Perform this part of the exercise on the 7034A-LCSEESRV-B virtual machine.	
9. Close down Windows Messenger on LCSEESRV.	**a.** Close the Windows Messenger window. **b.** In the system tray, right-click the Windows Messenger icon and click **Exit**.

Exercise 3
Configuring Instant Message Filtering in LCS 2005 with SP1

Scenario

For pilot testing purposes, the Fabrikam administrator wants to temporarily configure the LCS 2005 with SP1 server to allow URLs in instant messages.

Description

In this exercise, you will attempt to send an instant message with a URL in it. This will be blocked by the IMFilter application initially. Next, you will disable the IMFilter and send another instant message with a URL in it, which will succeed.

Tasks	Detailed Steps
Important: Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
1. Sign in to Office Communicator 2005 on FabrikamDC.	**a.** On **7034A-FabrikamDC-B**, click **Start**, point to **All Programs**, and then click **Microsoft Office Communicator 2005**. **b.** In the system tray, right-click the Communicator icon, and then click **Open**. **c.** Click **Actions**, and then click **Options**. **d.** In the **Options** dialog box, on the **Accounts** tab, click **Advanced**. **e.** In the **Advanced Connection Settings** dialog box, click **Configure settings**. **f.** In the **Server name or IP address** box, type **eepool1.fabrikam.local**. **g.** Click the **TLS** option. **h.** Click **OK**, and then click **OK** again. **i.** Click **Sign In**. **j.** In the **Sign-In Account** dialog box, in the **Sign-in name** box, type **max@fabrikam.local**. **k.** Click **OK**. **l.** In the **Sign-In Account** dialog box, in the **User name** box, type **max@fabrikam.local**, and in the **Password** box, type **pass@word1**. **m.** Click **OK**.
Important: Perform this exercise on the 7034A-LCSEESRV-B virtual machine.	
2. Sign in to Office Communicator 2005 on LCSEESRV.	**a.** On **7034A-LCSEESRV-B**, click **Start**, point to **All Programs**, and then click **Microsoft Office Communicator 2005**. **b.** Close the Microsoft Internet Explorer® window that opens. **c.** On the **Microsoft Office Communicator** page, click **Actions**, and then click **Options**.

	d. In the **Options** dialog box, on the **Accounts** tab, click **Advanced**. **e.** In the **Advanced Connections Settings** dialog box, click **Configure settings**. **f.** In the **Server name or IP address** box, type **eepool1.fabrikam.local**. **g.** Click the **TLS** option button. **h.** Click **OK**, and then click **OK** again. **i.** On the **Microsoft Office Communicator** page, click **Sign In**. **j.** In the **Sign-In Account** dialog box, in the **Sign-in name** box, type **rebecca@fabrikam.local** and in the **Password** box, type pass@word1. **k.** Click **OK**. **l.** In the **Sign-In Account** dialog box, in the **User name** box, type **rebecca@fabrikam.local**, and in the **Password** box, type **pass@word1**. **m.** Click **OK**.
Important: Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
3. Send an instant message containing a URL in Office Communicator 2005.	**a.** Switch back to the **7034A-FabrikamDC-B** virtual machine. **b.** In **Office Communicator 2005**, double-click **Rebecca Laszlo**. **c.** In the conversation window, type the following: **Click the following link for more information on LCS: http://www.microsoft.com/office/livecomm/prodinfo/default.mspx** **d.** Click **Send**. **e.** Read the system message in the top of the conversation window. *The message indicates that the message was not delivered and that the possible reason for this is that the message may contain a hyperlink or some other content that has been blocked.* **f.** Close the Rebecca Laszlo – Conversation window.
4. Disable the IMFilter on FabrikamDC and LCSEESRV.	**a.** Switch back to the **Live Communications Server 2005** console. **b.** Expand the **eeppol1** node, and then expand the **fabrikamdc.fabrikam.local** server node. **c.** Right-click **Applications**, and then click **Properties**. **d.** In the **Applications Properties** dialog box, under **Available applications**, click **http://www.microsoft.com/LCS/IMFilter**. **e.** Under **Details**, clear the **Enabled** check box, and then click **OK**. **f.** Expand the **lcseesrv.fabrikam.local** server node. **g.** Right-click **Applications**, and then click **Properties**. **h.** In the **Applications Properties** dialog box, under **Available applications**, click **http://www.microsoft.com/LCS/IMFilter**. **i.** Under **Details**, clear the **Enabled** check box, and then click **OK**. **j.** In the **Live Communications Server 2005** console, right-click

	fabrikamdc.fabrikam.local, and then click **Stop**. **k.** Wait for a moment until the server stops, right-click **fabrikamdc.fabrikam.local**, and then click **Start**. **l.** Right-click **lcseesrv.fabrikam.local**, and then click **Stop**. **m.** Wait for a moment until the server stops, right-click **lcseesrv.fabrikam.local**, and then click **Start**. **n.** Wait for two minutes before continuing the next task.
5. Send an instant message containing a URL in Office Communicator 2005.	**a.** Switch back to Office Communicator 2005. **b.** Double-click **Rebecca Laszlo**. **c.** In the **Rebecca Laszlo - Conversation** window, type the following: **Click the following link for more information on LCS: http://www.microsoft.com/office/livecomm/prodinfo/default.mspx** **d.** Click **Send**. *This time the message is allowed to be sent because the IMFilter application has been disabled on the LCS server.* **e.** Close the Rebecca Laszlo - Conversation window.
Important: Perform this part of the exercise on the 7034A-LCSEESRV-B virtual machine.	
6. Read the instant message on LCSEESRV.	**a.** Switch back to the **7034A-LCSEESRV-B** virtual machine. **b.** Click the **Max Stevens – Conversation** button in the taskbar to open it. *Note that the message containing the URL link has been received.* **c.** Close the Max Stevens - Conversation window.
Important: Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
7. Enable the IMFilter on FabrikamDC and LCSEESRV.	**a.** Switch back to the **7034A-FabrikamDC-B** virtual machine. **b.** Switch back to the **Live Communications Server 2005** console. **c.** Expand the **fabrikamdc.fabrikam.local** server node. **d.** Right-click **Applications**, and then click **Properties**. **e.** In the **Applications Properties** dialog box, under **Available applications**, click **http://www.microsoft.com/LCS/IMFilter**. **f.** Under **Details**, select the **Enabled** check box, and then click **OK**. **g.** Expand the **lcseesrv.fabrikam.local** server node. **h.** Right-click **Applications**, and then click **Properties**. **i.** In the **Applications Properties** dialog box, under **Available applications**, click **http://www.microsoft.com/LCS/IMFilter**. **j.** Under **Details**, select the **Enabled** check box, and then click **OK**.

	k. In the **Live Communications Server 2005** console, right-click **fabrikamdc.fabrikam.local**, and then click **Stop**. **l.** Wait for a moment until the server stops, right-click **fabrikamdc.fabrikam.local**, and then click **Start**. **m.** Right-click **lcseesrv.fabrikam.local**, and then click **Stop**. **n.** Wait for a moment until the server stops, right-click **lcseesrv.fabrikam.local**, and then click **Start**. **o.** Wait for two minutes before continuing the next task.

Exercise 4
Installing and Configuring the Intelligent IM Filter in LCS 2005 with SP1

Scenario

The default IMFilter in LCS 2005 with SP1 can block all URLs and file transfers, but Matt would like to use the enhanced functionality of the Intelligent IM Filter, which permits several options for configuring how URLs and file transfers are handled in LCS 2005 with SP1, and therefore provides greater flexibility than the default filter.

Description

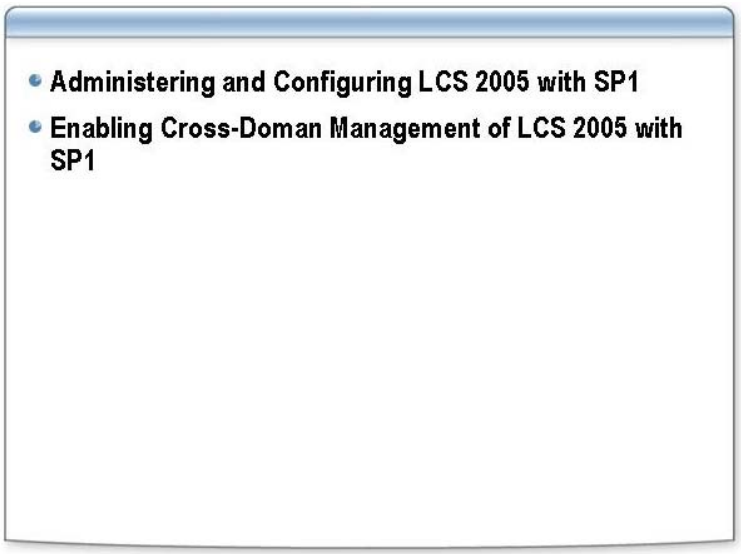
In this exercise, you will install the Intelligent IM Filter application and then configure and test its settings.

Tasks	Detailed Steps
Important: Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
1. Install the Intelligent IM Filter on FabrikamDC.	**a.** On **7034A-FabrikamDC-B**, click **Start**, and then click **My Computer**. **b.** Navigate to **E:\Demo Files\IIM Filter**, and then double-click **IIMFilterInstall.msi**. **c.** On the **Welcome** page, click **Next**. **d.** On the **License Agreement** page, click **I accept the terms in the license agreement**, and then click **Next**. **e.** On the **Ready to install the program** page, click **Install** to start the installation. **f.** On the **Application successfully installed** page, click **Finish**. *The Intelligent IM Filter application launches automatically after the wizard completes.*
2. Configure the Intelligent IM Filter on FabrikamDC.	**a.** In the **Live Communications Server 2005 Intelligent IM Filter** dialog box, click **Allow instant messages that contain hyperlinks. Enter the warning you want to insert at the beginning of each instant message containing hyperlinks**, then under that type: **"Warning: you should not click any unknown links in instant messages. Refer to the company's URL policy documentation for more details."** **b.** Click the **File Transfer Filter** tab. **c.** Click **Block only file extensions in the list below**. (Note that .txt extensions will be allowed, but .exe extensions will be blocked.) **d.** Click the **Logging options** tab. **e.** Click **Enable logging**. **f.** In the **Log file folder path**, type **C:\IIMFilter_Logs**. **g.** Click **OK**.

	h. In the **Folder does not exist** message box, click **OK**. **i.** In the **Activate** dialog box, in the **Service Account** box, type **fabrikam\administrator**, and in the **Password** box, type **pass@word1**. **j.** Click **OK** to start the service and activate the filter.
3. Send an instant message containing a URL in Office Communicator 2005 on FabrikamDC.	**a.** Switch back to Microsoft Office Communicator. **b.** Double-click **Rebecca Laszlo**. **c.** In the conversation window, type the following: **Click the following link for more information on LCS: http://www.microsoft.com/office/livecomm/prodinfo/default.mspx** **d.** Click Send. *The message is allowed to be sent because the Intelligent IM Filter application has allowed URLs to be sent in instant messages, but with an accompanying warning message.*
Important: Perform this part of the exercise on the 7034A-LCSEESRV-B virtual machine.	
4. Read the instant message on LCSEESRV.	**a.** Switch back to the **7034A-LCSEESRV-B** virtual machine. **b.** Click the **Max Stevens – Conversation** button in the taskbar to open it. *Note that the message containing the URL link has been received, but that the message has been pre-pended with the corporate warning message.*
Important: Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
5. Transfer a file in Office Communicator 2005 on FabrikamDC.	**a.** On **7034A-FabrikamDC-B**, switch back to Office Communicator 2005. **b.** In the conversation window, click **Actions**, and then click **Send a File**. **c.** Double-click the **WINDOWS** folder. **d.** Scroll across and select the **setuplog** text document, and then click **Open**. *This file is transferred because the file extension is allowed in the Intelligent IM Filter.* **e.** Click **Actions**, and then click **Send a File**. **f.** In the **WINDOWS** folder, scroll across and select **NOTEPAD**, and then click **Open**. *This file is not delivered, because the file extension has been blocked by the Intelligent IM Filter.*
Important: Perform this part of the exercise on the 7034A-LCSEESRV-B virtual machine.	
6. Accept the file transfer on LCSEESRV.	**a.** On **7034A-LCSEESRV-B**, in the **Max Stevens – Conversation** window, under **setuplog.txt**, click **Accept (ALT+C)**.

	b. In the Microsoft Office Communicator warning message, click **OK**. *Note that the setuplog text file has now been transferred successfully to Rebecca Laszlo.* **c.** Close the Max Stevens - Conversation window.
7. Close all virtual machines and do not save changes.	**a.** In the **7034A-LCSEESRV-B** virtual computer window, click the **Action** menu, and then click **Close**. **b.** In the **Close** dialog box, click **Turn off and delete changes**, and then click **OK**. **c.** Repeat these steps for all remaining VPC images.

Review



There are several methods for administering Microsoft® Live Communications Server 2005 with SP1 (LCS 2005 with SP1). There are also several post-installation tasks required to enable and configure your users and servers to use LCS 2005 with SP1. This module looked at the tools and consoles used to administer users and servers in LCS 2005 with SP1, and showed you how to configure global, user, and server settings for LCS 2005 with SP1. You also learnt how to enable several cross-domain management scenarios for LCS 2005 with SP1.

In the next module, you will look at the features of the Office Communicator 2005 client for LCS 2005 with SP1.