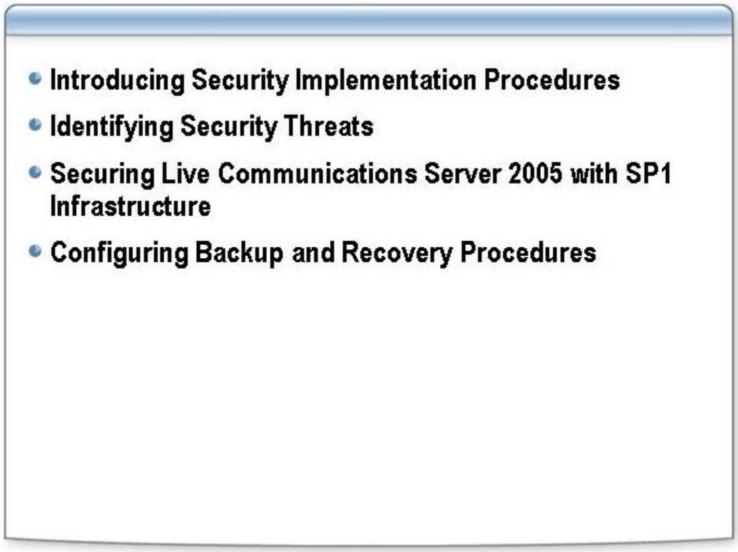
Module 10: Securing Live Communications Server 2005 with Service Pack 1

Contents

Overview



- Introducing Security Implementation Procedures
- Identifying Security Threats
- Securing Live Communications Server 2005 with SP1 Infrastructure
- Configuring Backup and Recovery Procedures

Introduction

After you deploy Microsoft® Live Communications Server 2005 with Service Pack 1 (LCS 2005 with SP1) Standard or Enterprise Edition, you will want to take a proactive approach to security with your LCS 2005 with SP1 implementation.

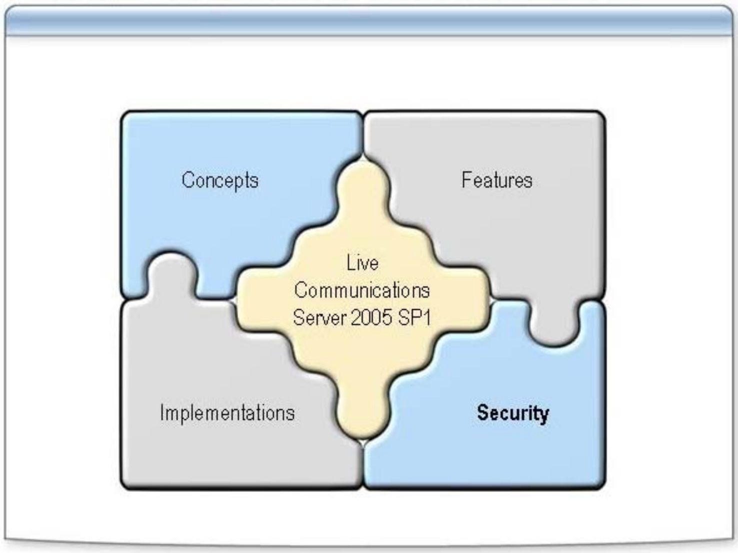
In this module, you will learn how to implement security procedures to defend against threats to your LCS 2005 with SP1 topology. You will also understand the methods used to address the threats to both the server and the client.

Objectives

After completing this module, you will be able to:

- Describe the concepts, features, and methods for implementing securing a LCS 2005 with SP1 infrastructure.
- Identify the potential threats to a LCS 2005 with SP1 implementation.
- Explain how to secure a LCS 2005 with SP1 environment.
- Configure backup and recovery processes.

Lesson: Introducing Security for Live Communications Server 2005 with SP1



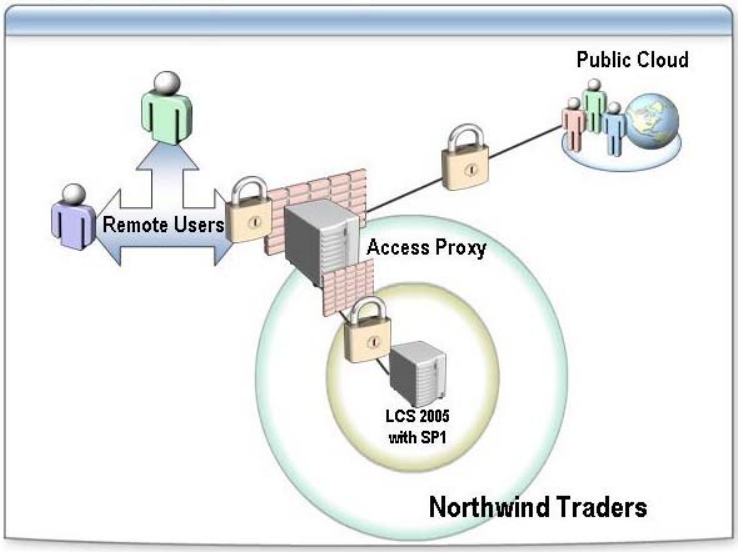
Lesson Objectives

This lesson introduces the security concepts that apply to a LCS 2005 with SP1 Standard or Enterprise Edition environment. Security concepts should be considered during the planning, deployment, and daily operations phase of LCS 2005 with SP1.

After completing this lesson, you will be able to:

- Describe the concepts of securing a LCS 2005 with SP1 implementation.
- List the features of security in a LCS 2005 with SP1 environment.
- Identify different server roles that provide additional security.
- Describe concepts, features, and implementations of securing a Live Communications Server 2005 with SP1 infrastructure.

What Is Security in Live Communications Server 2005 with SP1?



Introduction

Security is a large, complex, and constantly changing challenge for network administrators. Because new threats arise, and existing threats become commonplace, applying security is also a dynamic process. The definition of acceptable risk and the methods used to get to a level of acceptable risk vary among organizations.

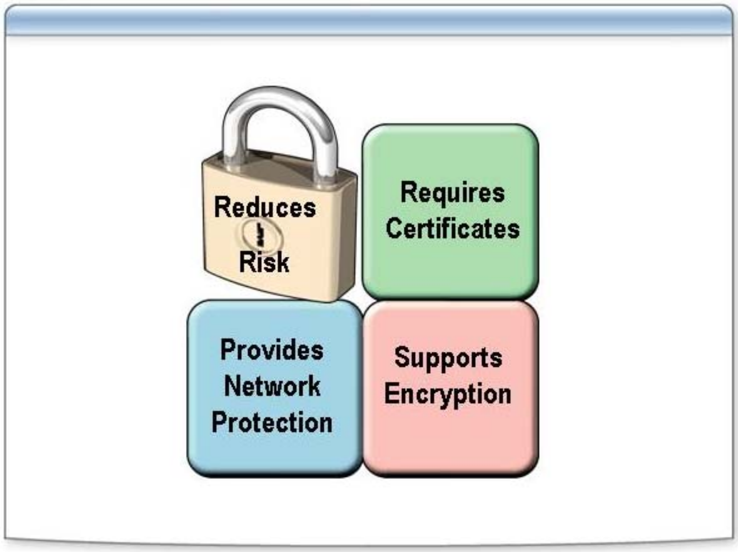
The definition of acceptable security and the methodologies to reach that security level can change over time. An organization's LCS 2005 with SP1 infrastructure and daily operations might change over time, based on security recommendations.

Security Scenarios

In LCS 2005 with SP1, enhanced security features such as the URL blocking filter and spam over instant messaging (SPIM) control helps protect your organization, as well as each enterprise-to-enterprise federated connection, from unsolicited instant messages and IM-based worms. Internal and remote users have security mechanisms in place to help prevent unsolicited communications.

As an administrator, you can disable the ability for your users to click a URL directly. Instead of directly clicking a URL in their Microsoft Office Communicator client, your users will be required to copy and then paste the URL into a browser’s address bar. This procedure is a security benefit, as users can quickly identify and avoid URL extensions that could be a potential security threat, such as .exe extensions.

What Are the Benefits of Securing LCS 2005 with SP1?



Reduces Risk

Requires Certificates

Provides Network Protection

Supports Encryption

Introduction

In the information worker age, individuals can work from home, office, car, or plane, and constant access to up-to-date information is critical. LCS 2005 with SP1 provides encrypted communications between your LCS 2005 with SP1 users and their co-workers or external business partners. This communication facility enables users to converse electronically, without the overhead and formality of e-mail.

Network Protection

When you deploy LCS 2005 with SP1 and implement the security features with this product, security risks to your network are significantly reduced. Specific server roles such as the Access Proxy and Director provide network protection because the internal network does not have a direct entry point.

Message Encryption

Server-to-server communication in LCS 2005 with SP1 uses Mutual Transport Layer Security (MTLS) encryption. An example of server-to-server communications is Federation with an external organization. For client-to-server communications, LCS 2005 with SP1 supports Transport Layer Security (TLS). An example of client-to-server communications is Remote User Access from Office Communicator 2005.

Certificates

MTLS and TLS require digital certificates to be installed. All communication traffic is encrypted, and message content is protected while in transit across public networks.

With LCS 2005 with SP1, Web server certificates are sufficient for your Live Communications Server topology. Certificates configured for client authorization are no longer required unless you are interoperating with partner systems or with Live Communications Server 2005 servers without SP1.

If your organization has a mix of Live Communications Servers, some running Live Communications Server 2005 with SP1 and others without SP1, you must use the certificate configuration that is required with Live Communications Server 2005 without SP1, which requires certificates configured for both client and server authorization.

Administrative Control

LCS 2005 with SP1 enhances security through effective administrative control. Administrators can enable or disable the following topologies on a per-user basis:

- Public IM Connectivity
- Remote User Access
- Federation

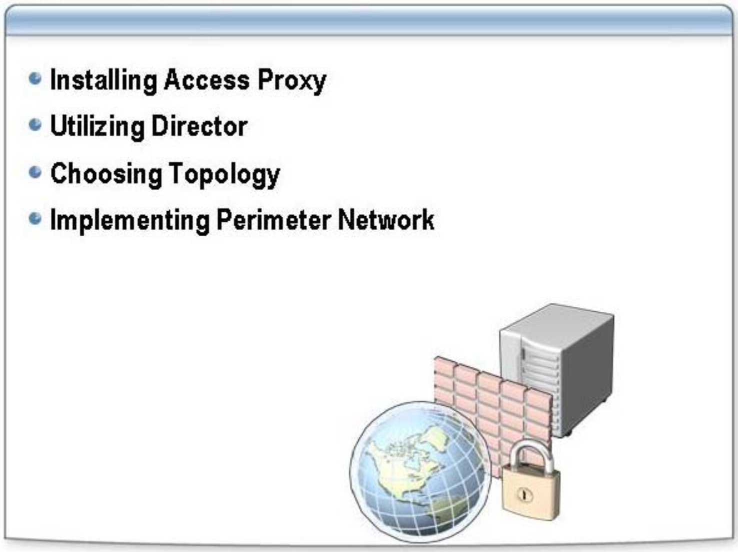
This control enables you to ensure that only authorized employees can use IM to connect to remote users, federated organizations, or users of public IM systems.

Reducing Risk

Deploying an Access Proxy server can also provide filtering of SPIM. This new filtering mechanism has been included to prevent unsolicited communications with users who run the Office Communicator or Microsoft Windows® Messaging clients.

Note To decrease security risks in your infrastructure and take full advantage of the security improvements within Live Communications Server 2005 with SP1, it is recommended that you upgrade your clients to the Office Communicator 2005 client.

Identifying Server Roles to Enhance Security in LCS 2005 with SP1



- Installing Access Proxy
- Utilizing Director
- Choosing Topology
- Implementing Perimeter Network

Introduction

LCS 2005 with SP1 server roles and supported network topologies are designed to help you implement a defense-in-depth strategy. Defense-in-depth is a multilayered, multiple strategy, and security management process used to reduce risk of compromise from internal and external threats.

LCS 2005 with SP1 provides this multilayered approach to security. Specific server roles and topologies have been designed to enhance security while your internal and remote users make use of the features included in LCS 2005 with SP1.

Access Proxy

A central component of this multi-layered security approach is the LCS 2005 with SP1 Access Proxy. The Access Proxy provides a single connection point through which both inbound and outbound Session Initiation Protocol (SIP) traffic can cross Internet firewalls, separating internal and external networks for Federation and Remote User Access traffic. An Access Proxy is required for Federation, Remote User Access, and Public IM Connectivity topologies.

The Access Proxy role was designed to operate in the perimeter network. Access Proxy has restricted routing rules that separate the outside edge of the network from the inside edge. It also provides a central platform to manage and enable cross-organization, domain-based policies.

An Access Proxy does validate inbound message headers, authenticate remote federation servers, and authorize the traffic. However, the Access Proxy does not authenticate client connections.

Note An Access Proxy is an IP-based routing solution and does not imply that a firewall is not needed. Microsoft strongly recommends that you use one or more advanced application-level firewalls, such as Internet Security and Acceleration (ISA) Server 2004.

Director

The Director server is a special configuration mode of either LCS 2005 with SP1 Standard Edition or Enterprise Edition. A Director server does not home any users.

Director servers authenticate and authorize remote clients. Remote clients are your own users connecting from outside the firewall using the Access Proxy. A Director server also routes your users to their home server.

Access Proxies do not communicate to Active Directory®, by design. Enabling a Director server as a Next Hop server can be helpful to provide defense-in-depth against distributed Internet attacks where attackers are posing as remote users.

A Director server role is designed to be the Next Hop server connecting directly with your Access Proxy server. The Director is strongly recommended as your Next Hop server when Remote User Access is supported. As the Next Hop server, a Director server offloads the authentication work and helps to prevent any external attacks from affecting enterprise users.

The Director server is also useful as a central point of logging all Federation and outside user traffic, if this is desired for security auditing. It can also be a single connection point for your Access Proxy server's inbound and outbound traffic to and from your internal network. If you have a firewall between your Access Proxy server and Director server, the changes to your firewall will be minimized if you use a Director server.

Topologies

LCS 2005 with SP1 has several topologies designed to support security enhancements. Topologies include Federation, Remote User Access, and Public IM Connectivity.

You should select a topology based on your business needs. Each topology then makes use of security features such as certificates, authentication procedures, and security auditing.

Network Firewall

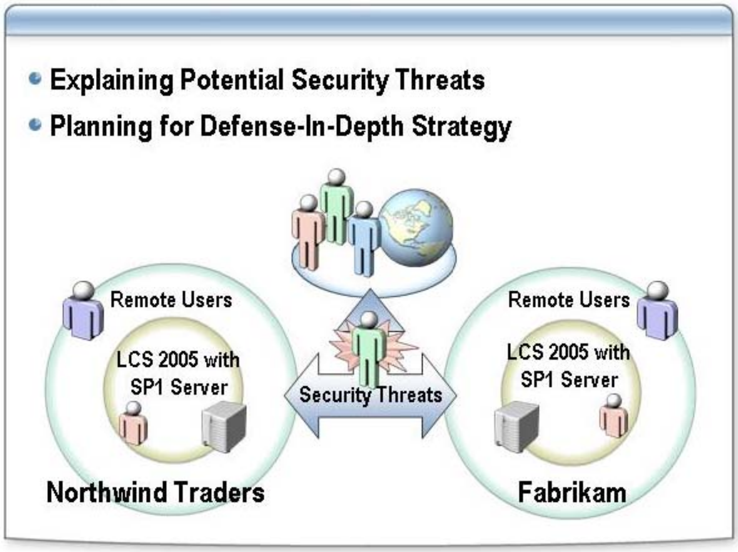
Microsoft ISA Server 2004 can be used as an alternative and in conjunction with a Virtual Private Network (VPN) in a LCS 2005 with SP1 implementation. A computer running ISA Server 2004 can provide advanced firewall services at both the perimeter network and internal network boundaries.

Note When you use a network address translation (NAT) device with Live Communications Server 2005, only presence and instant messaging are enabled for outside users. Scenarios involving audio, video, data collaboration, and file transfer are not supported.

Additional Resources

If you do not have an existing ISA Server 2004 infrastructure, review the Evaluation Guide page on the Microsoft ISA Server Web site, at: http://www.microsoft.com/isaserver/evaluation/newcustomer.mspx.

Lesson: Identifying and Planning for Security Threats



- Explaining Potential Security Threats
- Planning for Defense-In-Depth Strategy

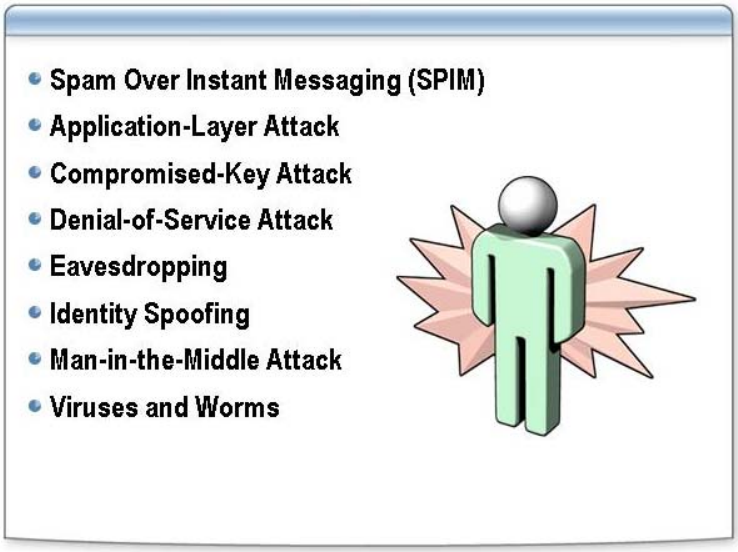
Lesson Objectives

This lesson introduces the potential security threats your infrastructure and users might face. You should understand the potential security threats to be able to configure your LCS 2005 with SP1 settings to reduce those threats to an acceptable level.

After completing this lesson, you will be able to:

- Explain the potential security threats to your LCS 2003 with SP1 infrastructure.
- Plan for a defense-in-depth strategy.
- Identify the potential threats to a LCS 2005 with SP1 implementation.

Explaining Potential Threats



- Spam Over Instant Messaging (SPIM)
- Application-Layer Attack
- Compromised-Key Attack
- Denial-of-Service Attack
- Eavesdropping
- Identity Spoofing
- Man-in-the-Middle Attack
- Viruses and Worms

Introduction

This lesson identifies and describes some of the common threats to the security of your Live Communications Server deployment.

An installation of LCS 2005 with SP1 could possibly be exposed to the following threats:

- Spam over instant messaging (SPIM)
- Application-layer attack
- Compromised-key attack
- Denial-of-service attack
- Eavesdropping
- Identity spoofing
- Man-in-the-middle attack
- Viruses and worms

SPIM

Spam over instant messaging (SPIM) is unsolicited commercial instant messages, or presence subscription requests. While not by itself a compromise of the network, it can reduce resource availability, and could eventually lead to a compromise of the network. If Federation is enabled and a coordinated spam attack is established, this can be difficult to overcome. A Microsoft SIP Header extension has been added to reduce the risk of this kind of attack in Federation scenarios.

Application Layer Attack

The application-layer attack occurs when the attacker takes advantage of a fault in a server's operating system or one or more of the server's applications. A successful attack results in the attacker bypassing normal operation and control. An attacker could gain read/write access to operating system or application, inject viruses or worms, install a sniffer program for later attacks, or install a custom application programming interface (API) extension program.

Compromised Key Attack

A compromised-key attack occurs when the attacker determines the key to an encrypted conversation or file. A key is a secret code or number used to encrypt, decrypt, or validate secret information. This key corresponds to the certificate associated with the server. This is a time-consuming and sophisticated process, but not impossible. Once the attacker is successful in determining the key, the attacker uses the key to decrypt encrypted data without the knowledge of the sender of the data.

Denial of Service Attack

The Denial of Service (DOS) attack occurs when the attacker prevents normal network use and function by valid users. When the attacker successfully gains access to the network by using a denial-of-service, the attacker can hide evidence of the attack and prevent users from accessing network resources.

Eavesdropping

Eavesdropping can occur when an attacker gains access to the data path in a network and has the ability to monitor and read the traffic. This is also called sniffing. If the traffic is in plain text, the attacker is able to read the traffic after the attacker gains access to the path. An example is when the attacker is able to install their own server API extension program.

Additionally, if you enable Public IM Connectivity, be aware that communications between the LCS 2005 with SP1 server to the public IM server communications are encrypted. However, communications from the public IM server to the public IM client may not be encrypted.

Generally, communications from a Live Communications Server to the client is encrypted. While federated enterprises may choose to disable this encryption to the client, these communications usually take place within an intranet protected by firewalls and other safeguards.

Identity Spoofing

Spoofing occurs when the attacker determines and uses an IP address of a network, computer, or network component when not authorized to do so. A successful attack allows the attacker to operate as if the attacker were the entity normally identified by the IP address. The only time this comes into play for LCS 2005 with SP1 is when the administrator has configured gateways that only support TCP and the administrator has had to mark their IP addresses as a trusted host. Using TLS (Transport Layer Security) or working with a gateway over a trusted network is a way to stop identity spoofing.

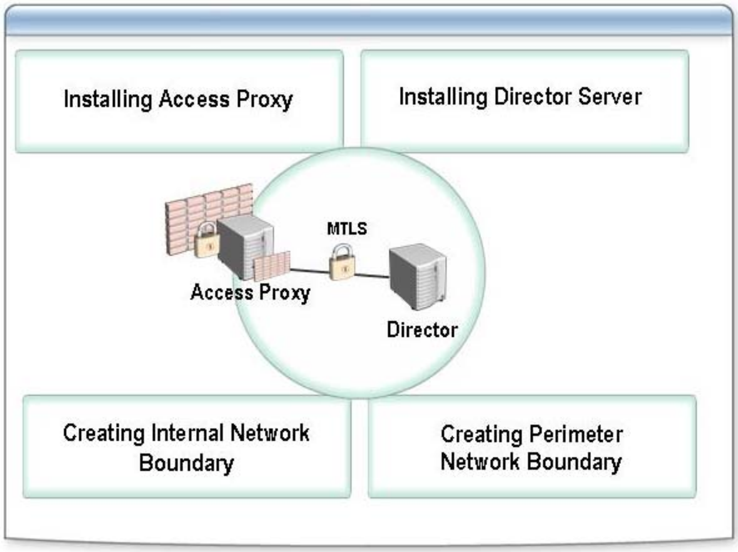
Man-in-the-Middle Attack

A man-in-the-middle attack occurs when an attacker reroutes communication between two users through the attacker's computer without the knowledge of the two communicating users. The attacker can monitor and read the traffic before sending it on to the intended recipient. This can happen if an attacker can modify the Active Directory directory service to add a server as a trusted server, or if they can modify DNS to get clients to connect through them on their way to the server.

Viruses and Worms

A virus is a unit of code that is designed to reproduce additional, similar code units. Viruses need hosts, and a host can be a file, an e-mail message, or a program. A worm is a unit of code that is coded to reproduce additional, similar code units, but does not require a host. Viruses and worms primarily appear during file transfers between clients, or when URLs are sent from other users. A virus on your computer could use your identity and send instant messages on your behalf.

Planning for a Defense-in-Depth Strategy


Installing Access Proxy
Installing Director Server
MTLS
Access Proxy
Director
Creating Internal Network Boundary
Creating Perimeter Network Boundary

Introduction

It is important to plan for a defense-in-depth strategy against potential security threats. Planning helps to reduce risk of a compromised LCS 2005 with SP1 infrastructure, an infrastructure that not only includes the servers but the internal or remote clients as well.

Defense-in-depth

You can implement a defense-in-depth strategy for LCS 2005 with SP1 by planning to complete the following steps:

- Create an internal network boundary.
- Create a perimeter network boundary.
- Install an Access Proxy.
- Locate the Access Proxy in the perimeter network.
- Separate network traffic depending on topology.
- Install a Director server for authentication.

Internal Network Boundary

You can use ISA Server 2004 or another firewall product to create an internal, protected network. You can protect your internal network further by specifying a Next Hop server to which your Access Proxy forwards incoming traffic.

Perimeter Network Boundary

You can use ISA Server 2004 or another firewall product to create a perimeter network. A perimeter network is where you place computers that handle external connections, such as the Access Proxy or the Microsoft Office Communicator Web Access server.

Note Computers in the perimeter network should not be members of a domain. Domain membership requires opening of additional ports in the internal firewall, which may create an unacceptable security risk.

Server Roles

It is recommended to use an Access Proxy with a Director server role to isolate external traffic. You must use an Access Proxy for Remote User Access, Federation, and Public IM Connectivity. A Director is strongly recommended as the first internal LCS 2005 with SP1 for Remote User Access and federated traffic.

Access Proxy

Locate the Access Proxy in the perimeter network. Plan to complete the following Access Proxy recommendations listed below:

- Use a dedicated server for the Access Proxy.
- Do not use the enterprise namespace for the Access Proxy. Use a workgroup namespace instead.
- Use different DNS names on the internal and external edges of the Access Proxy.
- Use a certificate issued by a public CA for the external edge when implementing Remote User Access and for Federation.

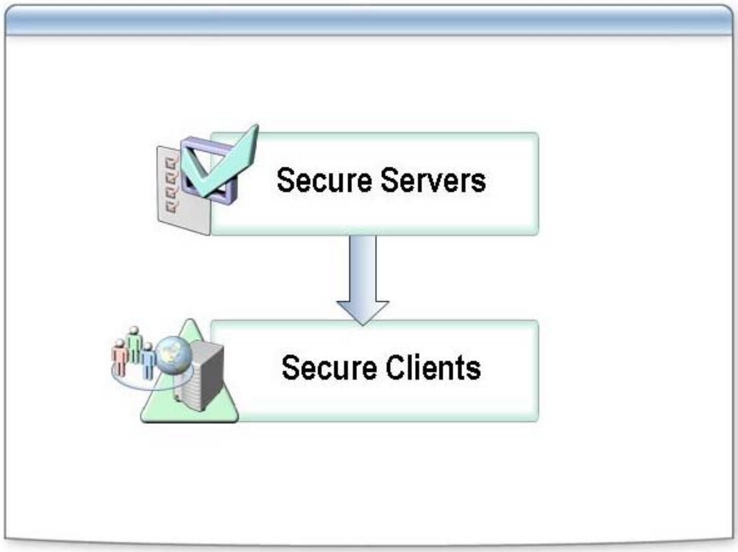
Director

It is recommended to use a dedicated server to run LCS 2005 with SP1 Director server role. It is also recommended to use a separate Director server for Remote User Access and a separate Director server for Federation traffic. This configuration also requires separate Access Proxies.

Separate Network Traffic

It is recommended that you separate Remote User Access and Federation network traffic. Use one or more Access Proxies for Federation and one or more Access Proxies for Remote User Access only.

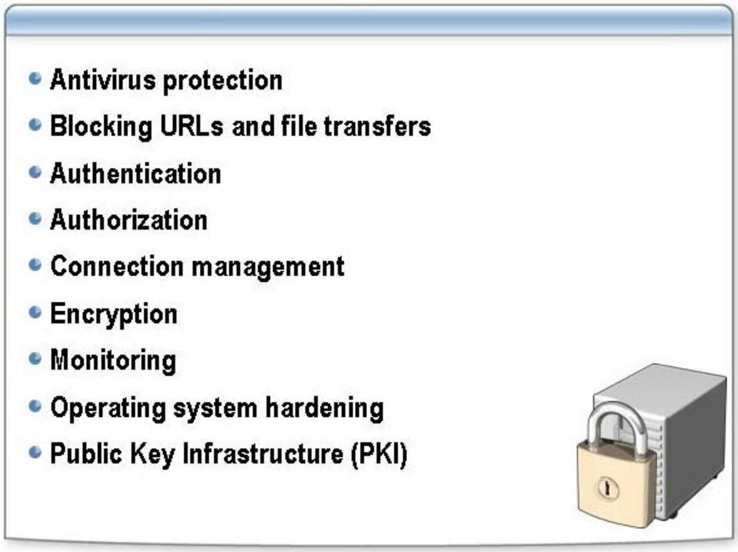
Lesson: Securing LCS 2005 with SP1



This lesson introduces how to protect your LCS 2005 with SP1 environment from potential security threats. You will learn how to implement security methods on your servers and client. After completing this lesson, you will be able to:

- List the security methods to protect your LCS 2005 with SP1 servers.
- List the security methods to protect your LCS 2005 with SP1 clients.
- Configure Group Policy for LCS 2005 with SP1.
- Configure message filter controls.
- Explain how to increase security in a LCS 2005 with SP1 environment.

Protecting LCS 2005 with SP1 Servers



- Antivirus protection
- Blocking URLs and file transfers
- Authentication
- Authorization
- Connection management
- Encryption
- Monitoring
- Operating system hardening
- Public Key Infrastructure (PKI)

Introduction

A secure installation of LCS 2005 with SP1 addresses potential security threats. It also helps to reduce the risk of a successful attack by using one or more of the following solutions:

- Antivirus protection
- Blocking URLs and file transfers
- Authentication
- Authorization
- Connection management
- Encryption
- Monitoring
- Operating system hardening
- Public Key Infrastructure (PKI)

Antivirus Protection

Use antivirus software to reduce risk of attack by viruses and worms. Keep the antivirus dynamic files up-to-date to help prevent viruses from taking control of LCS 2005 with SP1 functionality, operating system, and the functionality of other applications.

Blocking URLs

LCS 2005 with SP1 introduces a new IM filter application, IMFilter.am, which blocks messages that contain URLs or attempt to initiate a file transfer. IMFilter.am is installed and enabled by default on the following LCS 2005 with SP1 server roles:

- Standard Edition
- Enterprise Edition
- Director
- Access Proxy

Server Authentication

Server authentication is used to prevent unauthorized access to resources. Review the following list of server authentication methods:

- **Clients and servers authenticate to other servers using certificates**. You configure the certificate on the server during setup.
- **Servers require MTLS**. If no certificate is presented, the peer is treated as a client, resulting in reduced bandwidth availability.

Authorization

Users can control which other users can see their presence and which users can successfully communicate with them in real time. This access control list is maintained on the server in the user's behalf. It can be edited by the Administrator from the Live Communications Server Microsoft Management Console (MMC). Authorization in LCS 2005 with SP1 is not tied to Windows security groups

Connection Management

Network connections can be managed by configuring a number of different network components and methods on firewalls, TCP/IP, and LCS 2005 with SP1. Server-to-server network connections use MTLS on port 5061 by default.

Encryption

Encryption reduces the impact of eavesdropping. TLS and MTLS are used by LCS 2005 with SP1 to provide encryption. Server-to-server traffic is required to be MTLS, both inside and outside of the internal network perimeter. Client-to-server traffic inside the internal network perimeter can be TCP or TLS. Client-to-client traffic that is outside or crosses the internal network perimeter can be TCP from the enterprise client to its internal home server, but all other links are TLS. TLS and MTLS both require certificates, whereas TCP does not require certificates.

Monitoring

The following event-types, sources, and methods can be used for event monitoring:

- Event Viewer
- LCS 2005 with SP1 MOM Management Pack
- Enabling flat file logging level one
- Enabling archiving
- LCSMonitor.exe

Operating System Hardening

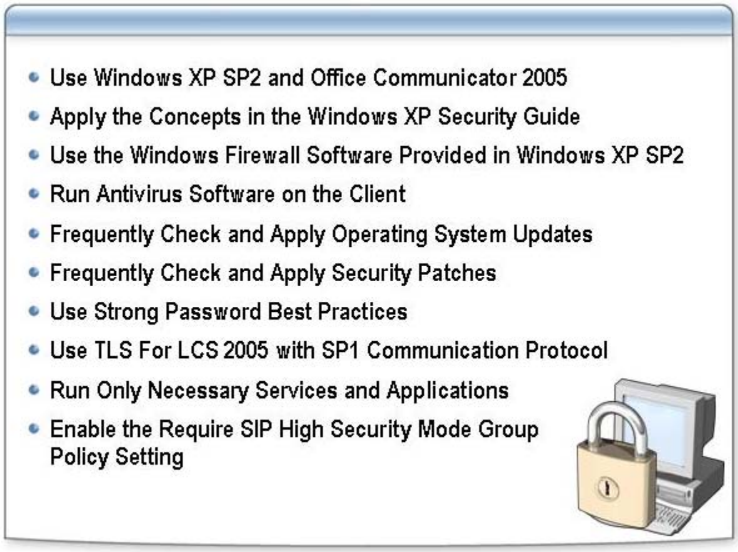
LCS 2005 with SP1 requires Windows Server® 2003. You should harden your operating system according to best practices for that specific component.

Public Key Infrastructure

LCS 2005 with SP1 uses certificates from your existing Public Key Infrastructure. LCS 2005 with SP1 supports the following CAs:

- Internal (private) CAs
  - Microsoft Windows Server 2003 Enterprise CA
  - Windows Server 2003 Standalone CA
  - Windows 2000 Standalone CA
- External (public) CAs

Protecting LCS 2005 with SP1 Clients



- Use Windows XP SP2 and Office Communicator 2005
- Apply the Concepts in the Windows XP Security Guide
- Use the Windows Firewall Software Provided in Windows XP SP2
- Run Antivirus Software on the Client
- Frequently Check and Apply Operating System Updates
- Frequently Check and Apply Security Patches
- Use Strong Password Best Practices
- Use TLS For LCS 2005 with SP1 Communication Protocol
- Run Only Necessary Services and Applications
- Enable the Require SIP High Security Mode Group Policy Setting

Introduction

While the majority of LCS 2005 with SP1 security configuration is performed on the server, you can take steps to increase security on the client as well. Review the following steps to increase security on your LCS 2005 with SP1 clients:

- Use Windows XP SP2 and Office Communicator 2005.
- Apply the concepts in the “Windows XP Security Guide” on the Microsoft Web site at: http://www.microsoft.com/technet/security/prodtech/winclnt/secwinxp/xpsgch01.mspx.
- Use the Windows Firewall software provided in Windows XP SP2.
- Run antivirus software on the client.
- Frequently check and apply operating system updates.
- Frequently check and apply security patches.
- Use strong password best practices.
- Use TLS for LCS 2005 with SP1 communication protocol.
- Run only necessary services and applications.
- Enable the **Require SIP high security mode** Group Policy setting for the user’s Group Policy Object (GPO).

Client Connection Management

Client connections are handled differently from server connections. The following list describes the differences:

- A limit on the number of outstanding transactions is established.
- Throttling on client connections is established.
- Throttling on message rate is established.
- Isolation of users (per-user throttling) is established.

Windows Messenger 5.1 Clients

It is recommended that you upgrade your Windows Messenger 5.1 clients to the Microsoft Office Communicator client. If you cannot upgrade, the recommendation is to use TLS both inside and outside the internal network perimeter.

Communicator Clients

Connection management on the Microsoft Office Communicator client is available from the **Action** menu. To access connection management, click **Actions**, and then click **Options**.

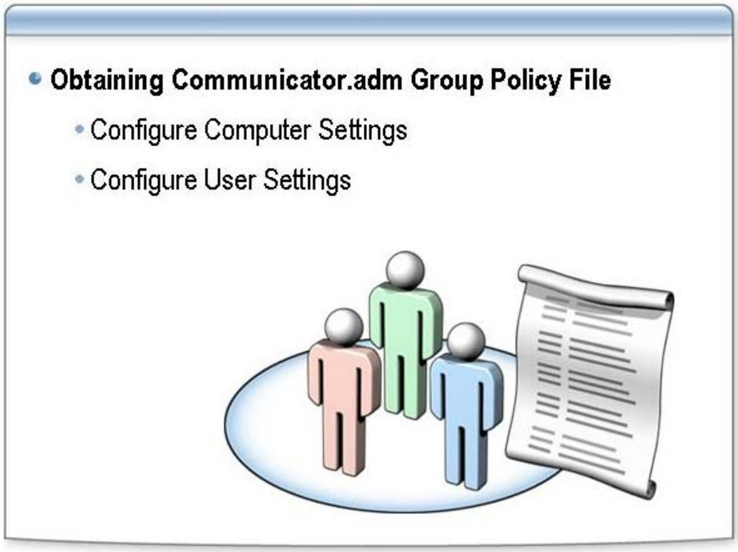
Click the **Accounts** tab to configure an account. When the user enables his or her LCS 2005 with SP1 account, you can configure the connection configuration as automatic or manual by clicking **Advanced**. The recommendation is to use TLS both inside and outside the internal network perimeter.

Best Practices

A brief best practices list is provided below that describes how to secure your LCS 2005 with SP1 clients:

- Use the Communicator client.
- Use Windows XP SP2.
- Use TLS.

Configuring Group Policy Settings



- **Obtaining Communicator.adm Group Policy File**
  - Configure Computer Settings
  - Configure User Settings

Introduction

Group Policy provides directory-based desktop configuration management. You can use Group Policy to implement security lockdowns, by defining Computer and User settings within a GPO for the following:

- Registry-based policies
- Security
- Software installation

Communicator.adm

The Communicator.adm file is provided with Office Communicator, and when loaded in the GPO Editor (Gpedit.dll), provides the Computer settings found at:

- Computer Config\Administrative Templates\Windows Messenger Policy Settings\
- \Windows Messenger Feature Policies
- \SIP Communications Service Policies
- \RTC Client API Service Policies

The Communicator.adm file also provides the User settings found at:

- User Config\Administrative Templates\Windows Messenger Policy Settings\
- \Windows Messenger Feature Policies
- \SIP Communications Service Policies

Group Policy Configuration

Group Policy configuration for LCS 2005 with SP1 depends on the needs of the business as well as the level of security you decide to enforce. The following is a list of LCS 2005 with SP1 Group Policy option:

- Prevent users from running Windows Messenger
- Prevent initial, automatic start of Windows Messenger
- Prevent connection to .NET Messaging Service

- Prevent connection to SIP Communications Service
- Prevent connection to Exchange Messaging Service
- Prevent video calls
- Prevent computer-to-computer audio calls
- Prevent computer-to-phone audio calls
- Allow computer-to-phone calls
- Prevent file transfer
- Prevent collaboration features
- Prevent Microsoft NetMeeting®
- Specify Instrumentation
- Prevent automatic update from Microsoft .NET Messaging Service
- Prevent Ink in instant messages
- Require logon credentials
- Allow additional server DNS names
- Specify encryption for collaboration features
- Specify encryption for computer-to-computer audio and video calls
- Require SIP high security mode
- Allow storage of passwords
- Specify transport and server
- Limit bandwidth for audio and video calls
- Specify dynamic port ranges
- Enable certificate revocation list checking

For more information about configuring group policies for Office Communicator 2005, see "Module 5: Deploying Microsoft Office Communicator 2005".

Additional Resources

For more information about obtaining and using the Group Policy Management Console, review the “Enterprise Management with the Group Policy Management Console” on the Microsoft Web site at: http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

For more information about Group Policies, visit the Group Policy Home on the Microsoft Web site at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/default.mspx.

Configuring Message Filtering Settings

- **Configuring Message Filter Controls**
  - Using Recipient’s Contact List
  - Verifying Providers
  - Verifying Federated Partners
  - Allowing All Communications

Introduction

Message filter controls determine how the Access Proxy will mark incoming messages, depending on whether they are verified by the sender. Message filter controls are another part of this multilayered approach to security.

Message Filter Configuration

You can implement the message filter controls when you configure Federation to your federated partners. You can also configure message filter controls when enabling Public IM Connectivity. The following message filter controls are available when you configure Federation:

- Allow communications only from users on recipient’s contact list.
- Allow communications only from users verified by this federated provider.
- Allow all communications from this federated provider.

You also have the following options for Public IM Connectivity configuration:

- Allow communications only from users on recipient’s contact list.
- Allow communications only from users verified by this provider.
- Allow all communications from this provider.

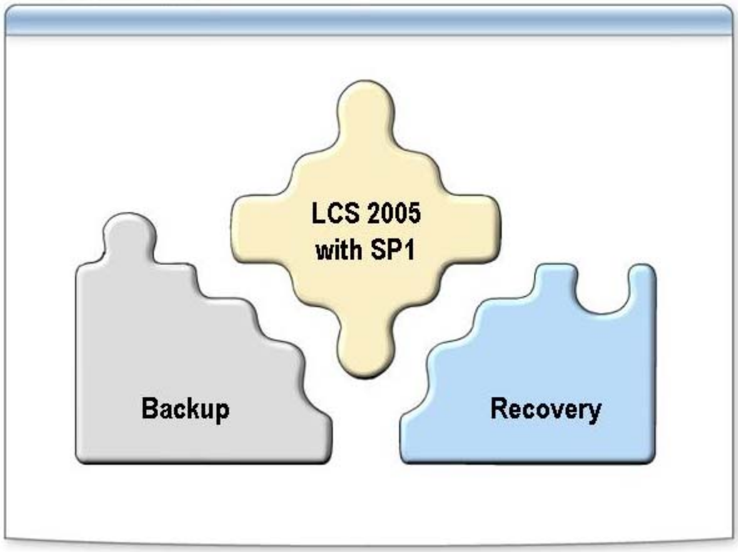
Selecting **Allow communications only from users on recipient’s contact list** means that you do not trust verification levels asserted by the federated partner. If you choose this option, the Access Proxy marks all incoming presence subscription requests as unverified. If the sender is already on the recipient’s allow list, the internal server will respond to that request; otherwise, the request is rejected. Similarly, requests for an instant messaging session that are marked as unverified are rejected by the client.

When you enable Federation or Public IM Connectivity, the default message filter control is **Allow communications only from users verified by this (federated) provider**. It means you trust the federated or provider verification level and you handle incoming messages accordingly.

The **Allow all communications from this (federated) provider** setting means that you accept all messages, whether they are verified or not. If you choose this option, the Access Proxy marks all messages as verified. The recipient’s home pool or server notifies the client, and all messages are handled according to settings on the client. In the case of presence subscription requests, the following settings determine how the message is handled:

- **Allow**: The sender’s request is accepted and the sender will be able to see the recipient’s presence information.
- **Block**: The request is rejected.
- **Prompt**: The recipient is asked whether to allow the sender to see presence information.

Lesson: Configuring Backup and Recovery Procedures



Introduction

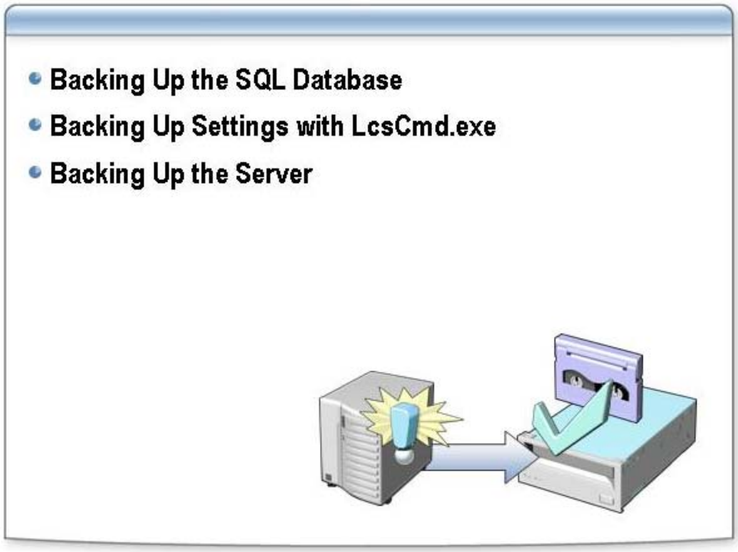
Backup and recovery procedures are an essential part of any disaster recovery plan. LCS 2005 with SP1 assets need to be included in an organization's backup and recovery procedures so that if a disaster occurs, the organization can reinstate its IM facilities with minimum disruption.

Lesson Objectives

This lesson introduces the backup and recovery concepts for LCS 2005 with SP1. After completing this lesson, you will be able to:

- Describe how to back up a LCS 2005 with SP1 server.
- Explain the process of restoring a LCS 2005 with SP1 server.
- Configure backup and recovery for LCS 2005 with SP1.

Backing Up LCS 2005 with SP1



- Backing Up the SQL Database
- Backing Up Settings with LcsCmd.exe
- Backing Up the Server

Introduction

Backing up LCS takes place in three main ways:

- SQL database backup
- Configuration setting backup
- Server backup

Backing Up the SQL Database

LCS 2005 with SP1 uses two SQL databases: RTC and RTCConfig. To back up a SQL database, perform the following steps

1. Log on to SQL Server™ and open **Enterprise Manager**.
2. Expand a server group, and then expand your server.
3. Expand **Databases**, right-click the database, point to **All Tasks**, and then click **Backup Database**.
4. In the **Name** box, type the backup set name. Optionally, in **Description**, type a description of the backup set.
5. Under **Backup**, click **Database - complete**.
6. Under **Destination**, click **Tape or Disk**, and then specify a backup destination.
7. If no backup destinations appear, click **Add** to add an existing destination or to create a new one.
8. Under **Overwrite**, do one of the following:
   a. Click **Append to media** to append the backup to any existing backups on the backup device.
   b. Click **Overwrite existing media** to overwrite any existing backups on the backup device.
9. Optionally, click the **Schedule** check box to schedule the backup operation to run later or periodically.
10. Optionally, click the **Options** tab and do one or more of the following:

a. Click the **Verify backup upon completion** check box to verify the backup.

b. Click the **Eject tape after backup** check box to eject the tape when the backup operation is complete. This is available only with tape devices.

c. Click the **Check media set name and backup set expiration** check box to prevent accidental overwrites. In **Media set name**, type the name of the media to be used for the backup operation. Leave this blank when specifying only the backup set expiration.

d. If it is the first use of the backup media, or you want to change an existing media label, under **Media set labels**, click the **Initialize and label media** check box and type the media set name and media set description. The media can be initialized and labeled only when overwriting the media.

Backing up Settings

The LcsCmd.exe command-line tool provides a way to export the pool and server level settings as a group. LcsCmd.exe is installed by default to **%ProgramFiles%\Common Files\Microsoft LC 2005**, and provides many useful command line abilities.

For backup purposes, you can use the following commands:

- ExportPoolConfig
- ExportServerConfig

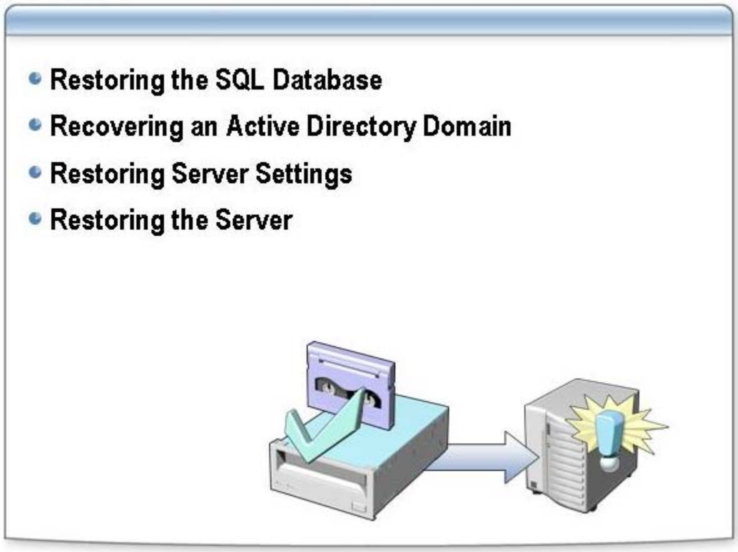
The export settings ensure uniform configuration among servers or pools in your environment or to back up a configuration for recovery purposes. You can back up an existing configuration before making any changes so you can restore the existing settings if a problem arises.

Backing up the Server

Computers within your LCS 2005 with SP1 environment also require server-level and system-state backups on a regular basis. Server-level backups help to ensure that you can restore your entire LCS 2005 with SP1 environment speedily in case of a server failure. Server level backups should be managed alongside your existing server backup routines.

For more information about how to use Veritas Backup Exec software to backup LCS 2005 with SP1, see "Protecting Live Communications Server 2005 with VERITAS Backup Exec Software", available from: http://office.microsoft.com/en-us/FX011526591033.aspx#Veritas

Describing a LCS 2005 with SP1 Restore Process



- **Restoring the SQL Database**
- **Recovering an Active Directory Domain**
- **Restoring Server Settings**
- **Restoring the Server**

Introduction

Backing up is only part of the recovery operation; it is vital to be able to restore the database, settings, or server. LCS 2005 with SP1 provides processes to restore the LCS environment.

Restoring the Database

To restore the LCS SQL database, perform the following steps:

1. Log on to the SQL Server.
2. In **Enterprise Administrator**, expand a server group, and then expand a server.
3. Expand **Databases**, right-click the database, point to **All Tasks**, and then click **Restore Database**.
4. In the **Restore as database** box, type or select the name of the database to restore, if different from the default. To restore the database with a new name, type the new name of the database.
5. Click **Database**.
6. In the **First backup to restore** list, click the backup set to restore.
7. In the **Restore** list, click the database backup to restore.
8. Optionally, click the **Options** tab and do the following:
   a. In **Restore as**, type the new name or location for each database file comprising the database backup. Specifying a new name for the database determines automatically the new names for the database files restored from the database backup.
   b. Click **Leave database operational. No additional transaction logs can be restored** if no further transaction log or differential database backups are to be applied.
   c. Click **Leave database non operational, but able to restore additional transaction logs** if another transaction log or differential database backup is to be applied.

Recovering an Active Directory Domain

The user database on LCS 2005 with SP1 Back-End Database retains a mapping of Active Directory user globally unique identifiers (GUIDs) and security identifiers (SIDs) to the user and SIP uniform resource identifier (URI). As a result, backups taken of the SQL database contain these mappings.

If Active Directory encountered a problem and was not restored as part of the disaster recovery procedure, a database restoration of the RTC database can restore LCS 2005 with SP1.

If you must restore the Active Directory domain, these mappings will change and you will need to export user data using the LCS 2005 with SP1 database (RTC), rebuild your Active Directory domain, and import user data back into the database. If you rebuild a domain, you cannot simply restore the database backup, because it now contains obsolete mappings to the previous domain.

Restoring Server Settings

The LcsCmd.exe command-line tool provides a way to import the pool and server level settings as a group. You can use the following commands:

- ImportPoolConfig
- ImportServerConfig

The import settings ensure uniform configuration among servers or pools in your environment or to restore a configuration for recovery purposes. You can back up an existing configuration before making any changes, so you can restore the existing settings if a problem arises.

Restoring the Server

If a server experiences a severe failure, such as hard disk failure, deliberate tampering, or a virus attack, then it may be necessary to carry out a full server restore. This restore process will depend on your backup environment. After carrying out a server restore, it will be necessary to restore the SQL database.

Lab 10: Securing Live Communications Server 2005 with SP1

- Exercise 1: Setting Filtering on Federated Communications
- Exercise 2: Configuring Office Communicator Group Policy
- Exercise 3: Using LcsCmd.exe to Export Server Settings

Objectives

After completing this lab, you will be able to:

- Set filtering on incoming federated communications.
- Configure Group Policy for Live Communications Server 2005 with SP1.
- Use LcsCmd.exe to export your LCS 2005 with SP1 settings.

Estimated time to complete this lab: **30 minutes**

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

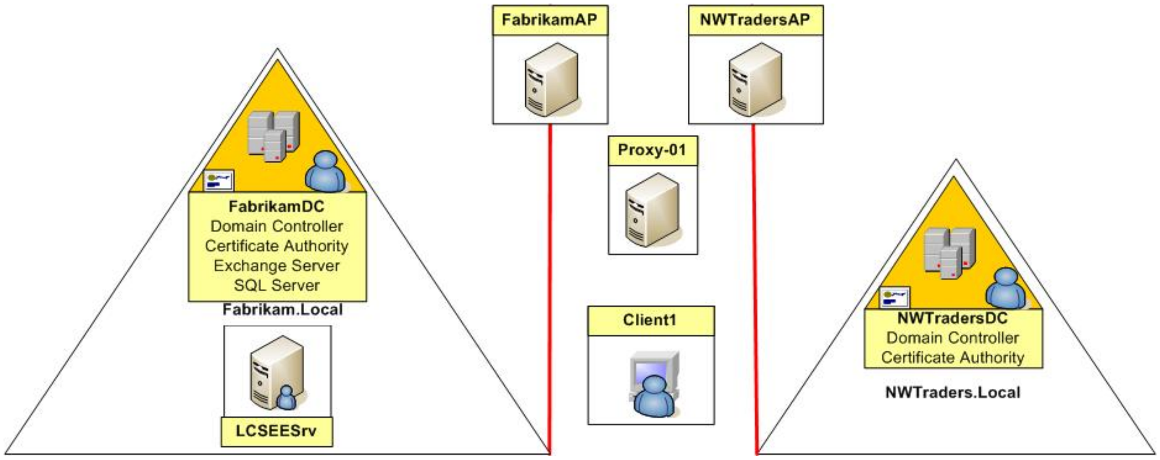
Introduction

Matt Dawson, the network administrator of Fabrikam, is concerned that the company's new implementation of LCS 2005 with SP1 could be open to exploitation by attackers. He wants to enhance security throughout the Fabrikam domain, and to prevent users from being subjected to SPIM.

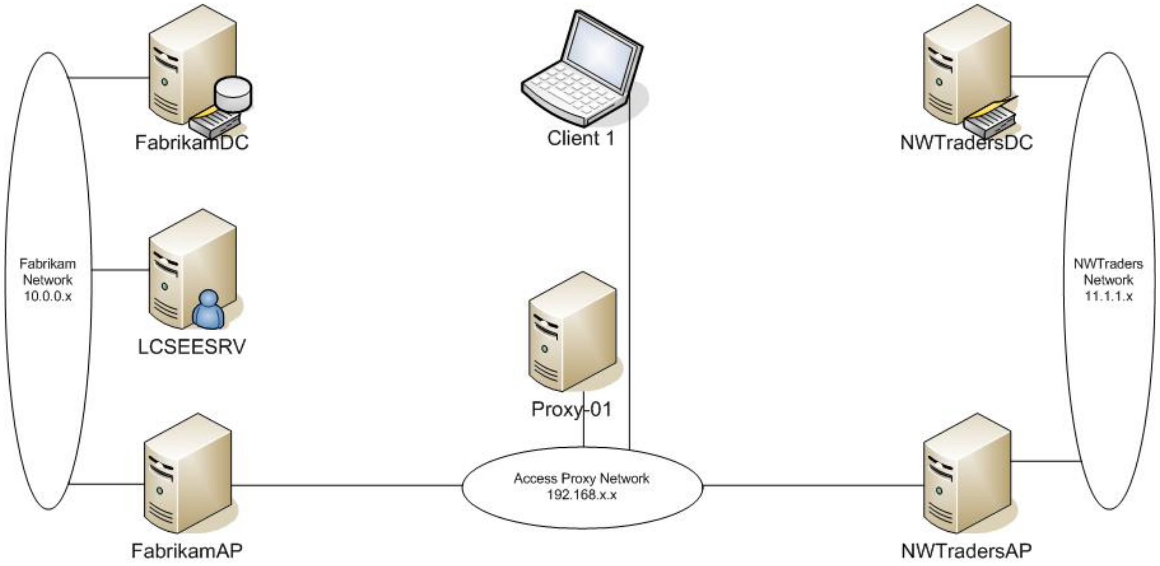
In this lab you secure the LCS 2005 with SP1 environment. You will set up filters for incoming federated communications, configure group policy settings, and export your LCS 2005 with SP1 settings.

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


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

Virtual PC Image to Computer NetBIOS Name Mappings

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

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

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

Close down the VPC images at the end of this lab and delete changes.

Exercise 1
Set Filtering on Incoming Federated Communications

Scenario

The first security change Matt can implement is to filter incoming communications from federated partners and public IM service providers. This setting helps to control SPIM. This capability is especially useful in blocking unsolicited messages from users of public IM services, but it also provides an additional layer of control over communications from other federated partners and clearinghouses.

Description

In this lab, you will restrict the federated connection with NWTraders by changing the default “Allow Communications Only From Users Verified by this Federated Provider” to “Allow communications only from users on recipient’s contact list.”

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-FabrikamAP-B virtual machine.	
1. Set the filters on incoming Federation communications.	**a.** Log on to the **7034A-FabrikamAP-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Computer Management**. **c.** In the **Computer Management** console, expand **Services and Applications**. **d.** Right-click **Microsoft Office Live Communications Server 2005**, and then click **Properties**. **e.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, click the **Allow** tab. **f.** In the **Allowed federated domains** list, click **NWTradersAP.NWTraders.local**, and then click **Edit**. **g.** In the **Edit Federated Partner** dialog box, in the **Select an option for filtering incoming communications** section, click **Allow communications only from users on recipient’s contact list**. **h.** On the **Edit Federated Partner** dialog box, click **OK**. **i.** In the **Microsoft Office Live Communications Server 2005 Properties** dialog box, click **OK**. **j.** Close the Computer Management console.

Exercise 2
Configuring Office Communicator Group Policy

Scenario

Matt wants to use Group Policy to enforce security options as well as disable certain features on the Office Communicator 2005 client. To do this, he is can use the Communicator.adm template that is provided with LCS 2005 with SP1 to modify group policy. He can then enforce this new group policy on this LCSUsers organizational unit.

Description

In this exercise, you use group policy to disable certain features in Microsoft Office Communicator 2005.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-FabrikamDC-B virtual machine.	
1. Configure Group Policy for LCS 2005 with SP1.	**a.** Log on to the **7034A-FabrikamDC-B** as **Administrator** with a password of **pass@word1**. **b.** Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**. **c.** In the Active Directory Users and Computers console, expand the **Fabrikam.local** domain, right-click the **LCSUsers** organizational unit, and then click **Properties**. **d.** In the **LCSUsers Properties** dialog box, click the **Group Policy** tab. **e.** Click **New**, and then type **LCSGP**. **f.** Click **LCSGP**, and then click **Edit**. **g.** On the **Group Policy Object Editor** console, under **Computer Configuration**, right-click **Administrative Templates**. **h.** Point to **All Tasks**, and then click **Add/Remove Templates**. **i.** In the **Add/Remove Templates** dialog box, click **Add**. **j.** In the **Policy Template** dialog box, in the **File name** box, type **E:\Demo Files\Communicator ADM File\Communicator.adm**, and click **Open**. **k.** In the **Add/Remove Templates** dialog box, click **Close**. **l.** In the **Group Policy Object Editor** console, expand **User Configuration**, expand **Administrative Templates**, and then expand **Microsoft Office Communicator Policy Settings**. **m.** Click **Microsoft Office Communicator Feature Policies**. **n.** In the right pane, right-click **Prevent file transfer**, and then click **Properties**. **o.** On the **Prevent file transfer Properties** page, click **Enabled**, and then click **OK**. **p.** Right-click **Prevent users from saving instant messages**, and then click **Properties**.

	q. In the **Prevent users from saving instant messages Properties** dialog box, click **Enabled**, and then click **OK**. **r.** Right-click **Configure SIP Security Mode**, and then click **Properties**. **s.** In the **Configure SIP Security Mode Properties** dialog box, click **Enabled**. **t.** In the **Configure SIP Security Mode** dialog box, click the down arrow on the list, click **High Security Mode**, and then click **OK**. **u.** On the **Group Policy Object Editor** page, right-click **Warning Text**, and then click **Properties**. **v.** In the **Warning Text Properties** dialog box, click **Enabled**. **w.** In the **Warning Text** box, type **Warning, instant messaging conversations cannot be saved**, and then click **OK**. **x.** Close the Group Policy Object Editor console. **y.** In the **LCSUsers Properties** dialog box, click **Close**, and then close the Active Directory Users and Computers console.
⚠ **Important:** Perform this exercise on the 7034A-LCSEESRV-B virtual machine.	
2. Refresh Group Policy.	**a.** Log on to **7034A-LCSEESRV-B** as **Jeff** with a password of **pass@word1**. **b.** Click **Start**, and then click **Run**. **c.** In the **Open** box, type **cmd**, and then click **OK**. **d.** At the command prompt, type **GPUPDATE /FORCE**, and press ENTER. A message appears, indicating that group policy has refreshed. **e.** Close the command prompt.
3. Test Group Policy.	**a.** Click **Start**, point to **All Programs**, and click **Microsoft Office Communicator 2005**. **b.** If a Microsoft Internet Explorer® Web page appears, close it. **c.** In the **Microsoft Office Communicator** dialog box, click the **Actions** menu, and then click **Options**. **d.** In the **Options** dialog box, in the **Sign-in name** box, type **jeff@fabrikam.local**, and then click **Advanced**. **e.** In the **Advanced Connection Settings** dialog box, click **Configure settings**, and in the **Server name or IP address** box, type **EEPool1.fabrikam.local**. **f.** Under **Connect using**, click **TLS**, and then click **OK**. **g.** On the **Options** dialog box, click **OK**. **h.** In the Microsoft Office Communicator window, click **Sign In**. **i.** On the **Sign-In Account** dialog box, click **OK**. If a **Communicator** dialog box from **matt@fabrikam.local** appears, click **OK** to accept communications from Matt. **j.** If there are users in Jeff's contact list, go to Step o. **k.** If there are no users in Jeff's contact list, click the **Contacts** menu, and then click **Add a Contact**. **l.** On the **How do you want to add a contact** page, click **Search for a**

	contact, and then click **Next**. **m.** In the **Add a Contact** wizard, in the **First Name** box, type **Jim**, and then click **Next**. **n.** On the **Search results** page, click **Jim Kim**, and then click **Next**. **o.** On the **Success!** page, click **Finish**. **p.** Right-click a contact, and then click **Send an Instant Message**. **q.** Verify that the warning text appears. **r.** Verify the **Save As** button is not visible. **s.** On the **File** menu, ensure that the **Save**, **Save As**, and **Save as e-mail** options are not available. **t.** Log off 7034A-LCSEESRV-B.

Exercise 3
Use LcsCmd.exe to Export Server Settings

Scenario

Finally, Matt wants to use LCS the ExportGlobalConfig and ExportServerConfig actions to save the Live Communications Server global settings, which can then be used as a backup for restoration in the event you have to recover data or roll back to the last known valid configuration.

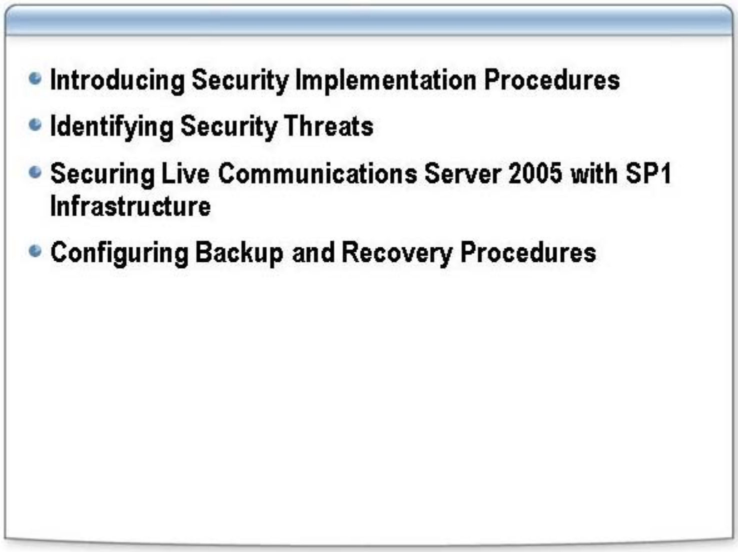
Description

Use the LcsCmd.exe to export your LCS 2005 with SP1 settings. This export can be later used for recovery purposes.

Tasks	Detailed Steps
⚠ **Important:** Perform this exercise on the 7034A-LCSEESRV-B virtual machine.	
1. Use LcsCmd.exe to export global and server settings.	**a.** Log on to **7034A-LCSEESRV-B** as **Administrator** with a password of **pass@word1**. **b.** If a **Sign-In Account** dialog box appears, click **Cancel**, and close Microsoft Office Communicator. **c.** Click **Start**, and then click **Run**. **d.** On the **Open** box, type **cmd**, and then click **OK**. **e.** At the command prompt, type **CD C:\Program Files\Common Files\Microsoft LC 2005**, and then press ENTER. **f.** At the command prompt, type **LcsCmd.exe /forest /action:ExportGlobalConfig /configFile:c:\LCSGlobalExport.xml**, and then press ENTER. **g.** Check that the **Action completed successfully** message appears. **h.** At the command prompt, type **LcsCmd.exe /server /action:ExportServerConfig /role:EE /configfile:c:\EEServerExport.xml**, and then press ENTER. **i.** Check that the **Action completed successfully** message appears. **j.** Do not close the command prompt.
2. Review the exported file.	**a.** Click **Start**, and then click **My Computer**. **b.** Navigate to **C:\**, and then double-click the **LCSGlobalExport.xml** file. **c.** If an **Information Bar** appears, click **Do not show this message again**, and then click **OK**. **d.** Click the yellow bar at the top of the Internet Explorer window, and then click **Allow Blocked Content**. **e.** In the **Security Warning** message box, click **Yes**. **f.** Search for **property name="RouteToEnterpriseEdge"**, and note the current value of **FabrikamAP.Fabrikam.local**.

3. Delete a configuration setting.	**a.** Click **Start**, point to **Administrative Tools**, and then click **Live Communications Server 2005**. **b.** In the **Microsoft Office Live Communications Server 2005** console, right-click **Forest – fabrikam.local**, and then click **Properties**. **c.** In the **Live Communications Server Global Properties** dialog box, click the **Access Proxy** tab. **d.** Under **Network address**, click **FabrikamAP.Fabrikam.local**, and then click **Remove**. **e.** In the **Live Communications Server Global Properties** dialog box, click **OK**. **f.** Right-click **Forest – fabrikam.local**, and then click **Refresh**. **g.** Note that in the right-hand pane, the **Trusted Access Proxy** value changes from **FabrikamAP.Fabrikam.local** to **<Empty>**.
4. Use LcsCmd.exe to restore the original setting from the exported file.	**a.** Switch back to the command prompt. **b.** At the command prompt, type **lcscmd.exe /forest /action:ImportGlobalConfig /configfile:c:\LCSGlobalExport.xml**, and then press ENTER. **c.** Check that the **Action completed successfully** message appears. **d.** Switch back to the Microsoft Office Live Communications Server 2005 console. **e.** Right-click **Forest – fabrikam.local**, and then click **Refresh**. **f.** Note that in the right pane, the **Trusted Access Proxy** value changes back from **<Empty>** to **FabrikamAP.Fabrikam.local**.
5. 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



- Introducing Security Implementation Procedures
- Identifying Security Threats
- Securing Live Communications Server 2005 with SP1 Infrastructure
- Configuring Backup and Recovery Procedures

In this module, you learned about the different security threats that could affect your LCS 2005 with SP1 environment. You also learned how to configure your LCS 2005 with SP1 servers and clients to prevent unauthorized access.

It is recommended that you maintain a defense-in-depth by implementing an Access Proxy, Director server, and perimeter network. A perimeter network provides an extra layer of network security between your internal network and external attackers.

In the next Module, you will look at how to implement the LCS 2005 with SP1 Address Book server role.