

Microsoft® Official Course



Module 5

Planning and Configuring Messaging Client Connectivity

Microsoft®

Module Overview

- Client Connectivity to the Client Access Server
- Configuring Outlook Web App
- Planning and Configuring Mobile Messaging
- Configuring Secure Internet Access for Client Access Server

Lesson 1: Client Connectivity to the Client Access Server

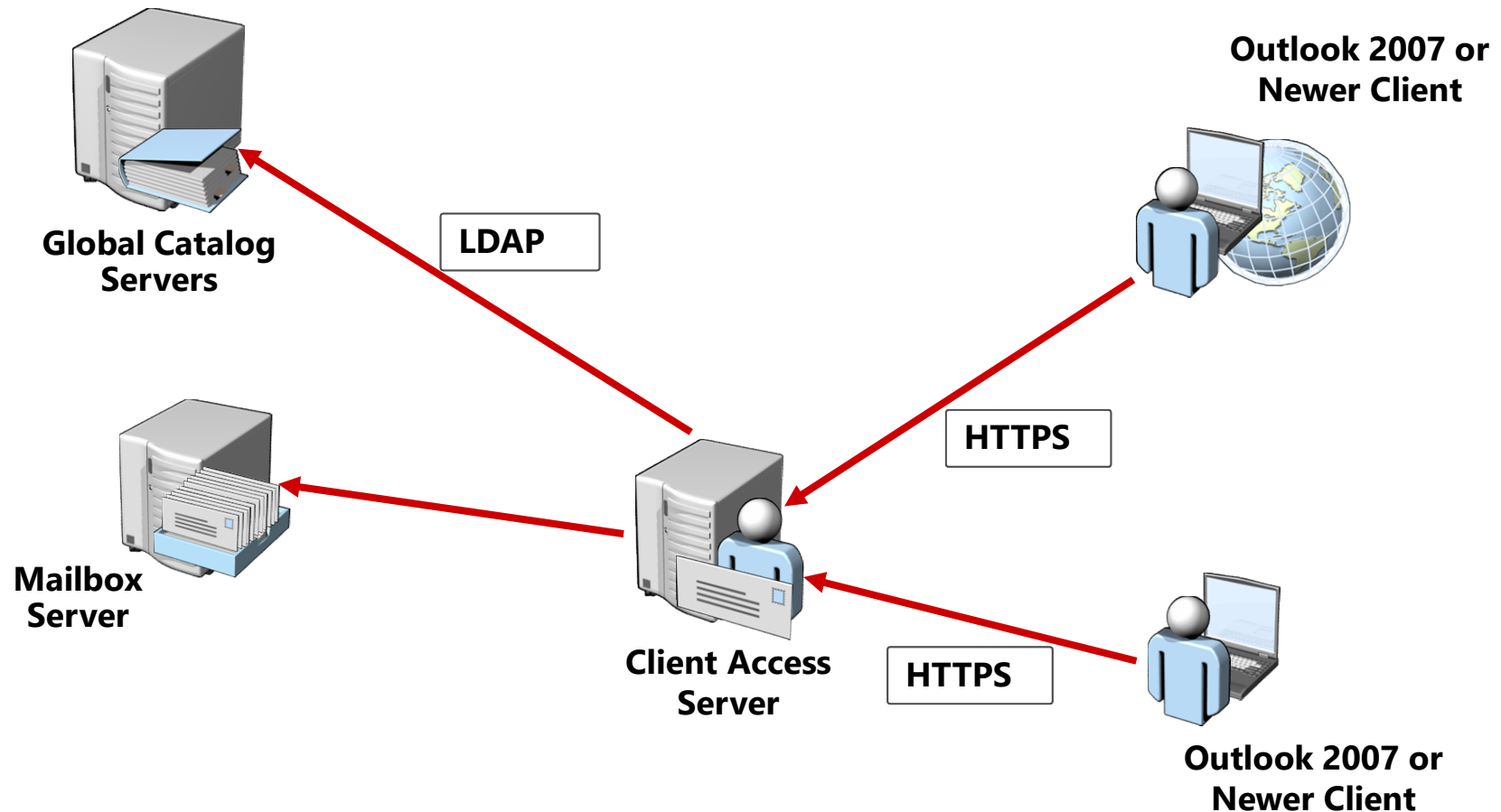
- What Is Outlook Web App?
- What Is Outlook Anywhere?
- What is Exchange ActiveSync?
- What is Outlook Web App Light?
- Connecting Non-Outlook Clients to the Client Access Server

What Is Outlook Web App?

- Outlook Web App allows users to access their mailboxes through a Web browser
- Outlook Web App provides:
 - Web-based access to all Exchange mailbox components
 - Secure HTTPS access from the Internet
 - An alternative to deploying a messaging client
 - Access to Exchange Server 2013 features that are not available in earlier versions of Outlook

What Is Outlook Anywhere?

- Outlook Anywhere enables RPC connections over HTTPS to an Exchange Server 2013 Client Access server



What Is Exchange ActiveSync?

- Exchange Active Sync is a protocol that enables mobile devices to access Exchange Server data
- It provides synchronization and management capabilities for mobile platforms
- It is supported on most current mobile platforms with various level of functionality
- Uses HTTPS to connect to Exchange Server

What Is Outlook Web App Light?

- Outlook Web App Light is an application within Outlook Web App that works with older browsers
- Outlook Web App Light provides:
 - Connectivity to user mailbox from mobile browsers
 - Subset of functionalities of Outlook Web App
 - Secure authentication

Connecting Non-Outlook Clients to the Client Access Server

- Non-Outlook clients can connect to Exchange Server by using:
 - POP3 protocol
 - IMAP4 protocol
- Consider using Outlook WebApp as an alternative for a locally installed email client
- Consider using the Windows 8 built-in Mail application that connects to Exchange by using ActiveSync

Lesson 2: Configuring Outlook Web App

- Configuring Options for Outlook Web App
- What Is Outlook Web App Policy?
- Demonstration: Configuring Outlook Web App Options and Policy
- Integrated Applications in Outlook Web App
- Demonstration: Using Apps in Outlook Web App
- What Is Office Web Apps Server Integration?
- Using Outlook Web App in Offline Mode
- Demonstration: Enabling and Using Outlook Web App in Offline Mode

Configuring Options for Outlook Web App

- When using Exchange Admin Center, you can configure following OWA settings:
 - Server certificate
 - Internal and external URL
 - Authentication options
 - Available features
 - File Access settings
- For a full set of OWA options, you should use Exchange Management Shell

What Is Outlook Web App Policy?

- OWA policy allows you to configure set of OWA related options and assign them to one or more mailboxes
- In OWA policy, you can configure following:
 - Policy name
 - Communication management options
 - Information management options
 - Security options
 - User experience options
 - Time management
 - Direct file access and web ready document viewing
 - Offline access

Demonstration: Configuring Outlook Web App Options and Policy

- In this demonstration, you will see how to configure OWA options and policies



Integrated Applications in Outlook Web App

- Integrated Apps in OWA enhance user experience by suggesting tasks based on messages' content
- Preinstalled applications are:
 - Bing
 - Action Items
 - Suggested Apointments
 - Unsubscribe
- You can add apps from the Office Store, a URL or from a file

Demonstration: Using Apps in Outlook Web App

- In this demonstration, you will see how to configure and use applications in OWA

What Is Office Web Apps Server Integration?

- Office Web Apps Server integration provides enhanced user experience when handling office-based email attachments
- Office Web Apps are used to render documents
- Users can modify documents online
- Office Web Apps integrate in OWA interface
- Usage is available to users of Exchange Online or Exchange installed on-premises
- Office Web Apps server is required

Using Outlook Web App in Offline Mode

- Offline Outlook Web App provides users with the ability to access data in their mailboxes even when not connected to Exchange Server
- Offline Outlook Web App:
 - Works only with selected browsers
 - Caches part of the mailbox content
 - Allows users to perform selected tasks
 - Is enabled on per-computer basis
 - Can be controlled by using OWA policies

Demonstration: Enabling and Using Outlook Web App in Offline Mode

- In this demonstration, you will see how to enable and use Offline Outlook Web App



Lesson 3: Planning and Configuring Mobile Messaging

- Discussion: Using Mobile Devices in Business Environments
- How Exchange ActiveSync Works
- Supported Features in Exchange ActiveSync
- What Is Direct Push?
- What Is Remote Wipe?
- What Is Mobile Device Quarantine?
- Securing Mobile Devices with Mobile Device Mailbox Policies
- Demonstration: Reviewing Options for Mobile Device Management in the Exchange Server Administration Center
- Alternatives for Mobile Device Management

Discussion: Using Mobile Devices in Business Environments

- Do you use mobile devices (smartphones and tablets)?
- Which mobile platform do you primarily use in your company?
- What services do you use on mobile devices?
- Are you connecting mobile devices to your company infrastructure?
- Do you have any security policy enforced for mobile devices?
- Do you have any management technology implemented?
- Do you use Active Sync?

How Exchange ActiveSync Works

- ActiveSync enables users to synchronize data from Exchange to the mobile device
- It uses HTTPS to connect to Client Access server
- Autodiscover is used to configure settings on the device
- You can selectively sync data to the mobile device
- Synchronized data stay on the mobile device even when offline

Supported Features in Exchange ActiveSync

- Some of the features implemented in Exchange Server 2013 ActiveSync are:
 - Support for HTML formatted messages
 - Conversation grouping of email messages
 - Ability to synchronize or not sync conversation
 - Support for fast message retrieval
 - Enhanced Exchange Search
 - Autodiscover for over-the-air provisioning
 - Direct Push
 - Support for availability information
 - GAL photos
 - Information Rights Management

What Is Direct Push?

- DirectPush:
 - Is an ActiveSync protocol feature that keeps the mailbox content on your device up to date
 - Works over data or WiFi connection
 - Notifies mobile device whenever change in mailbox happens
 - Uses port 443
- Time-out values on firewall should be modified

What Is Remote Wipe?

- Remote Wipe allows you to remotely delete all data on your mobile device in case it is lost or stolen
- Remote Wipe:
 - Can be issued by device owner or administrator
 - Can delete all data from an internal and removable memory
 - Can be issued from Outlook Web App, Exchange admin center or Exchange Management Shell
 - Requires connection to Exchange Server

What Is Mobile Device Quarantine?

- Each mobile device that connects to Exchange has its access state defined
- Access state for mobile device can be:
 - Allowed
 - Blocked
 - Quarantined
- You can define rules for device access based on the device family and device type

Securing Mobile Devices with Mobile Device Mailbox Policies

- Mobile Device Mailbox Policy allows you to enforce security settings for mobile devices on a per -base
- In Mobile Device Mailbox Policy you can configure:
 - Device password requirements
 - Encryption requirements
 - Local wipe options
 - Device inactivity settings
 - Password lifecycle settings

Demonstration: Reviewing Options for Mobile Device Management in the Exchange Server Administration Center

- In this demonstration, you will see how to configure available options for mobile devices in Exchange Server 2013

Alternatives for Mobile Device Management

- Managing mobile devices allows you to:
 - Preconfigure mobile devices
 - Deploy configuration profiles over the air
 - Deploy applications over the air
 - Control hardware and software behavior on mobile devices
 - Deploy updates to mobile
 - Enforce security options for mobile devices
- No unique solution for management exists
- Third-party tools
- Windows Intune and Configuration Manager can be considered for mobile device management

Lesson 4: Configuring Secure Internet Access for Client Access Server

- Exchange Server Security Guidelines
- Secure Internet Access Components
- Deploying Exchange Server 2013 for Internet Access
- Securing Client Access Traffic from the Internet
- Securing SMTP Connections from the Internet
- Benefits of using a Reverse Proxy

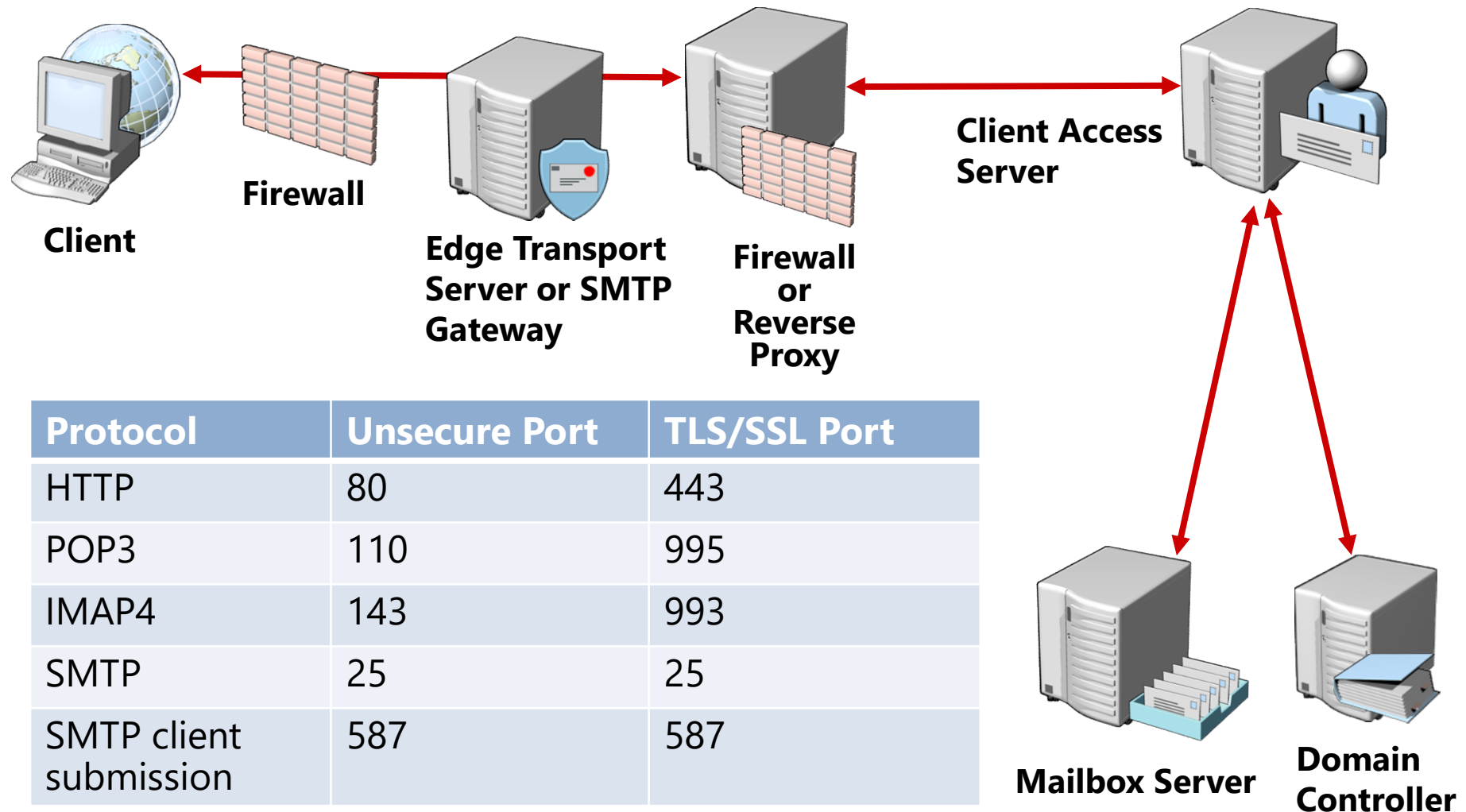
Exchange Server Security Guidelines

- To keep your Exchange Server secure, follow these guidelines:
 - Apply security and software updates
 - Avoid running additional software on Exchange Servers
 - Install and maintain anti-virus software
 - Enforce strong passwords in your organization

Secure Internet Access Components

- Providing Internet access for Exchange Server may include:
 - Enabling messaging clients to connect to the Client Access server
 - Enabling IMAP4/POP3 clients to send SMTP email
- Enabling secure access to the Exchange servers may require:
 - VPN
 - Firewall configuration
 - Reverse proxy configuration

Deploying Exchange Server 2013 for Internet Access



Securing Client Access Traffic from the Internet

- To provide secure CA from the Internet:
 - Create and configure a server certificate
 - Require SSL for all virtual directories
 - Enable only required client access methods
 - Require secure authentication
 - Enforce remote client security
 - Require TLS/SSL for IMAP4 and POP3 access
 - Implement an application layer firewall or reverse proxy

Securing SMTP Connections from the Internet

- SMTP connections from the Internet may be required for IMAP4 or POP3 clients
- To secure the SMTP connections:
 - Enable TLS/SSL for SMTP client connections
 - Use the Client Receive Connector (Port 587)
 - Ensure that anonymous relay is disabled
 - Enable IMAP4 and POP3 selectively

Benefits of Using a Reverse Proxy

- Reverse proxy provides:
 - Security: Internet client connections are terminated on the reverse proxy
 - Application-layer filtering: Inspect the contents of network traffic
 - SSL bridging: All connections to the reverse proxy and to the Client Access server are encrypted
 - Load balancing: Arrays of reverse proxy servers can distribute network traffic for a single URL
 - SSL offloading: SSL requests can be terminated on the reverse proxy

Lab: Planning and Configuring Messaging Client Connectivity

- Planning Client Connectivity
- Configuring Outlook Web App and Outlook Anywhere
- Configuring Exchange ActiveSync
- Publishing Exchange Server 2013 through TMG 2010

Logon Information

20341A-LON-DC1, 20341A-LON-CAS1

20341A-LON-MBX1, 20341A-LON-TMG

20341A-LON-CL1

User name: Adatum\Administrator

Password: Pa\$\$w0rd

Estimated Time: 75 minutes





Lab Scenario

A. Datum is planning its client connectivity solution for Exchange Server 2013. The company has several different types of clients, and it needs to find an appropriate solution for each, while staying compliant with the organization's security policy.

As A. Datum's Exchange administrator, you need to propose and implement a solution for client connectivity. You also must ensure that connections from the Internet are as secure as possible.

Lab Review

- What is the main purpose of Outlook Web App policies?
- What is the prerequisite for using Offline Outlook Web App?

Module Review and Takeaways

- Review Question
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

