



Video 13

Configuring the Client Access Server

© Train Signal, Inc., 2002-2007

Where we're going



- CAS Role overview
- IIS virtual directories for Exchange
- Outlook Anywhere Architecture
- Setting up Outlook Anywhere
- Active-Sync Architecture
- New Active-Sync features
- Active-Sync configuration
- Best Practices

© Train Signal, Inc., 2002-2007

CAS Role



- **What the Client Access Role is responsible for:**
 - Autodiscover & Availability services
 - Outlook Web Access
 - POP and IMAP services
 - Outlook Anywhere (RPC-over-HTTPS)
 - Exchange Active-Sync
 - Offline Address Book

Notes:

- Why is CAS not in the DMZ?

© Train Signal, Inc., 2002-2007

IIS Virtual Directories – Part 1



- **Most of the CAS functionality is based in IIS:**
 - These virtual directories in the default web Site run CAS services:
 - OWA (connects to Exchange 2007 mailbox servers)
 - RPC
 - RPCwithCerts
 - Microsoft-Server-ActiveSync
 - OAB
 - EWS
 - Autodiscover
 - UnifiedMessaging

© Train Signal, Inc., 2002-2007

IIS Virtual Directories – Part 2



- For OWA connections to Exchange 2003/2000 servers:
 - Exchange
 - Public (used for both legacy and 2007 PF access)
 - Exadmin
 - Exchweb
- All these directories are encrypted with the cert installed on the root site
- To create a new CAS website, you'd use the New-OWAVirtualDirectory cmdlet to create the requisite virtual directories

© Train Signal, Inc., 2002-2007

Outlook Anywhere Architecture



- **How Outlook Anywhere works:**
 - HTTPS tunnel created between client and CAS
 - Standard MAPI/RPC traffic passed through tunnel to appropriate Mailbox server
 - Traffic is encrypted with cert installed on Default Web site
 - Connection from client can be made from anywhere that HTTPS is allowed
 - Allows use of all "fat" client features that can be used internally
 - .ost file caches data, keeping an offline copy of server-side mailbox

© Train Signal, Inc., 2002-2007

Setting up Outlook Anywhere



- **Configuring Outlook Anywhere**
 - Install certificate
 - Make sure SSL is enabled on default web site (it is by default)
 - Add the RPC over HTTP Proxy via Add/Remove Windows Components
 - Enable Outlook Anywhere via the EMC (or EMS with Enable-OutlookAnywhere)
 - Set URL
 - Set Authentication method (NTLM if you have ISA proxy, or Basic if not)
 - Configure Outlook Anywhere on Outlook 2007
 - Accounts -> profile properties -> More Settings -> Connection Tab
 - URL: same URL you configured above (ex: cowmail.cashcowcapitalgroup.com)
 - Principal name: "msstd:cowmail.cashcowcapitalgroup.com"
 - Auth: needs to match what was set on server

© Train Signal, Inc., 2002-2007

Active-Sync Architecture



- **How Exchange Active Sync works:**
 - Client sends an HTTPS "heartbeat" with info about folders to sync, leaving an open session with the server.
 - Server holds that message data until a certain timeout
 - Default timeout (minimum) is 15 minutes. Max is 30 minutes
 - When timeout arrives, server responds that nothing was there, client resends heartbeat request
 - If folders are updated in the interval, server notifies device immediately
 - If notified of changes, device contacts server for download, then resends heartbeat

© Train Signal, Inc., 2002-2007

New Features



- **What's been added:**
 - SharePoint and UNC access
 - Follow-up flags
 - HTML message support
 - Autodiscover support
 - Enhanced Exchange Search
 - Fast message retrieval
 - Device password policy enforcement
 - Out of Office message setting
 - Meeting requests and attendee availability

© Train Signal, Inc., 2002-2007

Setting up Active-Sync



- **Configuration**

On the server:

- Determine the external URL
- Determine the auth method
- Determine which file resources should be made available
- Set up a policy if desired

On the mobile device:

- Setting up the device
- Managing the device
- Managing devices via OWA

© Train Signal, Inc., 2002-2007

Best Practices



- **Recommendations**

- Use a cert with Subject Alternative Names (SAN) and stick with the default site
- For Outlook Anywhere, use NTLM authentication if possible
- To use NTLM, you will need an advanced firewall like ISA 2006
- Use cached-mode with Outlook Anywhere
- Watch the HTTP timeout interval on your firewalls for the sake of ActiveSync
- Only allow SSL connections for ActiveSync
- Create and deploy a Windows Mobile password policy

© Train Signal, Inc., 2002-2007

Wrap-up



- **Where we've been:**

- The whole CAS
- How IIS fits in
- Outlook Anywhere
- Exchange ActiveSync
- Best Practices

© Train Signal, Inc., 2002-2007
