iPhone in Business
Microsoft Exchange

Exchange ActiveSync security policies

- Remote wipe
- Enforce password on device
- Minimum password length
- Maximum failed password attempts (before local wipe)
- Require both numbers and letters
- Inactivity time in minutes (1 to 60 minutes)

Additional Exchange ActiveSync policies (for 2007 only)

- Allow or prohibit simple password
- Password expiration
- Password history
- Policy refresh interval
- Minimum number of complex characters in password
- Require manual syncing while roaming
- Allow camera

iPhone communicates directly with your Microsoft Exchange Server via Microsoft Exchange ActiveSync (EAS), enabling push email, calendar, and contacts. Exchange ActiveSync also provides users with access to the Global Address Lookup (GAL), and provides administrators with passcode policy enforcement and remote wipe capabilities. iPhone supports both basic and certificate-based authentication for Exchange ActiveSync. If your company currently enables Exchange ActiveSync, you have the necessary services in place to support iPhone—no additional configuration is required. If you have Exchange Server 2003 or 2007 but your company is new to Exchange ActiveSync, review the following steps.

Exchange ActiveSync Setup

Network configuration overview

- Check to ensure port 443 is open on the firewall. If your company allows Outlook Web Access, port 443 is most likely already open.
- On the Front-End Server, verify that a server certificate is installed and enable SSL for the Exchange ActiveSync virtual directory in IIS.
- If you're using a Microsoft Internet Security and Acceleration (ISA) Server, verify that a server certificate is installed and update the public DNS to resolve incoming connections.
- Make sure the DNS for your network returns a single, externally-routable address to the Exchange ActiveSync server for both intranet and Internet clients. This is required so the device can use the same IP address for communicating with the server when both types of connections are active.
- If you're using a Microsoft ISA Server, create a web listener as well as an Exchange web client access publishing rule. See Microsoft's documentation for details.
- For all firewalls and network appliances, set the Idle Session Timeout to 30 minutes. For information about heartbeat and timeout intervals, refer to the Microsoft Exchange documentation at http://technet.microsoft.com/en-us/library/cc182270.aspx.
- Configure mobile features, policies, and device security settings using the Exchange System Manager. For Exchange Server 2007, this is done in the Exchange Management Console.
- Download and install the Microsoft Exchange ActiveSync Mobile Administration Web Tool, which is necessary to initiate a remote wipe. For Exchange Server 2007, remote wipe can also be initiated using Outlook Web Access or the Exchange Management Console.

Other Exchange ActiveSync services

- Mail search on Exchange Server 2007
- Accept and create calendar invitations
- Global Address List lookup
- Certificate-based authentication
- Email push to selected folders
- Autodiscovery

Basic Authentication (username and password)

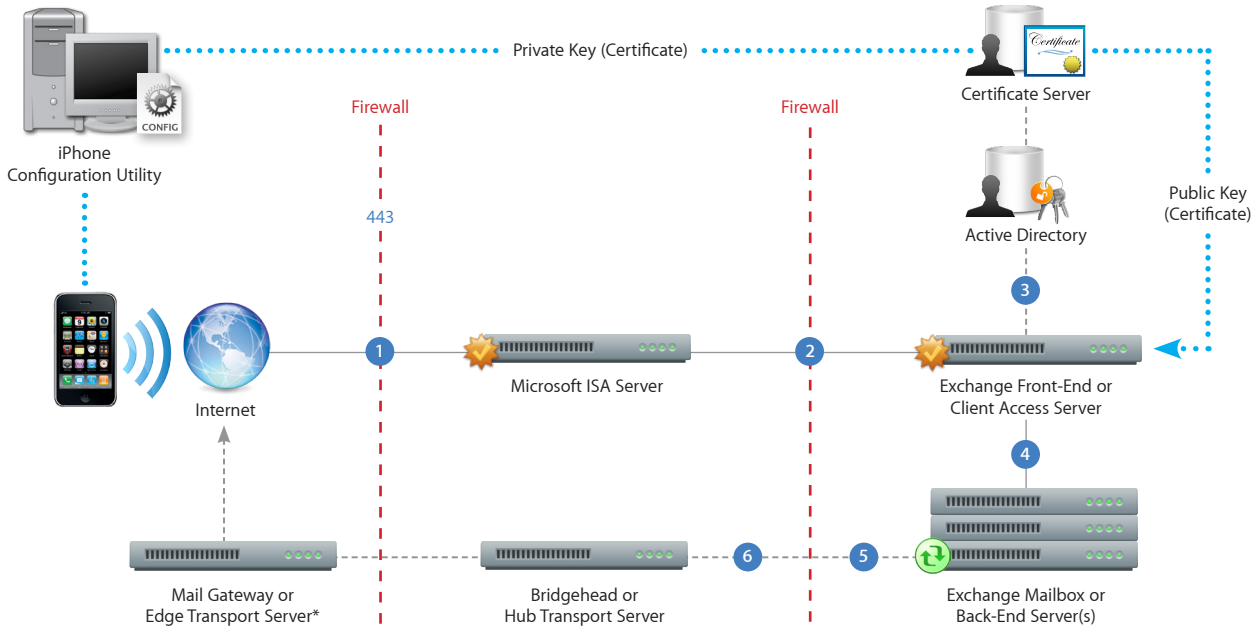
- Enable Exchange ActiveSync for specific users or groups using the Active Directory service. These are enabled by default for all mobile devices at the organizational level in Exchange Server 2003 and Exchange Server 2007. For Exchange Server 2007, see Recipient Configuration in the Exchange Management Console.
- By default, Exchange ActiveSync is configured for basic user authentication. It's recommended that you enable SSL for basic authentication to ensure credentials are encrypted during authentication.

Certificate-based Authentication

- Install enterprise certificate services on a member server or domain controller in your domain (this will be your certificate authority server). For more information on certificate services, please refer to resources available from Microsoft.
- Configure IIS on your Exchange front-end server or Client Access Server to accept certificate-based authentication for the Exchange ActiveSync virtual directory.
- To allow or require certificates for all users, turn off "Basic authentication" and select either "Accept client certificates" or "Require client certificates."
- Generate client certificates using your certificate authority server. Export the public key and configure IIS to use this key. Export the private key and use the iPhone Configuration Utility or Over-the-Air Enrollment and Configuration to deliver this key to iPhone.

Exchange ActiveSync Deployment Scenario

This example shows how iPhone connects to a typical Microsoft Exchange Server 2003 or 2007 deployment.



*Depending on your network configuration, the Mail Gateway or Edge Transport Server may reside within the perimeter network (DMZ).

1. iPhone requests access to Exchange ActiveSync services over port 443 (HTTPS). (This is the same port used for Outlook Web Access and other secure web services, so in many deployments this port is already open and configured to allow SSL encrypted HTTPS traffic.)
2. ISA provides access to the Exchange Front-End or Client Access Server. ISA is configured as a proxy, or in many cases a reverse proxy, to route traffic to the Exchange Server.
3. Exchange Server authenticates the incoming user via the Active Directory service and the certificate server (if using certificate-based authentication).
4. If the user provides the proper credentials and has access to Exchange ActiveSync services, the Front-End Server establishes a connection to the appropriate mailbox on the Back-End Server (via the Active Directory Global Catalog).
5. The Exchange ActiveSync connection is established. Updates/changes are pushed to iPhone over the air, and any changes made on iPhone are reflected on the Exchange Server.
6. Sent mail items on iPhone are also synchronized with the Exchange Server via Exchange ActiveSync (step 5). To route outbound email to external recipients, mail is typically sent through a Bridgehead (or Hub Transport) Server to an external Mail Gateway (or Edge Transport Server) via SMTP. Depending on your network configuration, the external Mail Gateway or Edge Transport Server could reside within the perimeter network or outside the firewall.

© 2009 Apple Inc. All rights reserved. Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries. iPhone is a trademark of Apple Inc. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. June 2009 L372756C