



iPhone in Unternehmen

Microsoft Exchange



Exchange ActiveSync-Sicherheitsrichtlinien

- Remote Wipe
- Zwingende Eingabe eines Gerätekenneworts
- Mindestlänge für Kennwörter
- Maximalanzahl fehlgeschlagener Kennworteingaben (vor Local-Wipe)
- Kennwort muss aus Ziffern und Buchstaben bestehen
- Inaktivitätszeit in Minuten (1 bis 60 Minuten)

Zusätzliche Exchange ActiveSync-Richtlinien (nur für 2007)

- Einfaches Kennwort zulassen oder ablehnen
- Kennwortablauf
- Kennwortverlauf
- Richtlinienaktualisierungsvorgabe
- Mindestanzahl komplexer Zeichen in einem Kennwort
- Bei Roaming manuelle Synchronisierung erforderlich
- Kameranutzung zulassen

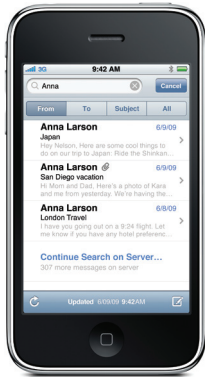
Das iPhone kommuniziert über Microsoft Exchange ActiveSync direkt mit Ihrem Microsoft Exchange Server (EAS) und ermöglicht Push-Dienste für E-Mails, Kalender und Kontakte. Exchange ActiveSync bietet den Benutzern auch Zugang zu Global Address Lookup (GAL) und gewährleistet Administratoren Passcode-Richtlinienzwang und Remote-Wipe-Fähigkeiten.

Das iPhone unterstützt sowohl die grundlegende als auch die zertifikatbasierte Authentifizierung für Exchange ActiveSync. Wenn Ihr Unternehmen derzeit mit Exchange ActiveSync arbeitet, sind die notwendigen Dienste zur Unterstützung des iPhone bereits vorhanden – es ist keine weitere Konfiguration notwendig. Wenn Ihr Unternehmen Erfahrung hat mit Exchange Server 2003 oder 2007, aber noch keine Erfahrung mit Exchange ActiveSync, sollten Sie Folgendes prüfen:

Exchange ActiveSync-Setup

Überblick über die Netzwerkkonfiguration

- Stellen Sie sicher, dass in der Firewall der Port 443 geöffnet ist. Wenn Ihr Unternehmen die Verwendung von Outlook Web Access zulässt, ist Port 443 wahrscheinlich bereits geöffnet.
- Prüfen Sie, ob auf dem Front-End-Server ein Serverzertifikat installiert ist, und aktivieren Sie in IIS SSL für das virtuelle Verzeichnis von Exchange ActiveSync.
- Wenn Sie einen Microsoft Internet Security and Acceleration (ISA) Server verwenden, prüfen Sie, ob ein Serverzertifikat installiert ist, und aktualisieren Sie den öffentliche DNS-Server, damit eingehende Verbindungen abgewickelt werden können.
- Stellen Sie sicher, dass der DNS Ihres Netzwerks eine einzelne, externe routingfähige Adresse für Intranet- und Internetclients an den Exchange ActiveSync-Server zurücksendet. Diese wird benötigt, damit das Gerät dieselbe IP-Adresse für die Kommunikation mit dem Server verwenden kann, wenn beide Verbindungsarten aktiv sind.
- Wenn Sie einen Microsoft ISA-Server verwenden, erstellen Sie einen Web-Listener sowie eine Bereitstellungsrichtlinie für den Zugriff durch Exchange Webclients. Details hierzu entnehmen Sie bitte der Microsoft-Dokumentation.
- Legen Sie für alle Firewalls und Netzwerk-Appliances das Zeitlimit für inaktive Sitzungen auf 30 Minuten fest. In der Dokumentation zu Microsoft Exchange finden Sie Angaben zu alternativen Einstellungen für Takt- und Timeout-Intervalle unter <http://technet.microsoft.com/en-us/library/cc182270.aspx>.
- Konfigurieren Sie mithilfe des Exchange System Managers die Funktionen für mobile Geräte, die Richtlinien und die Einstellungen für die Gerätesicherheit. Unter Exchange Server 2007 können diese Einstellungen über die Exchange-Verwaltungskonsole vorgenommen werden.
- Laden Sie das Microsoft Exchange ActiveSync Mobile Administration-Webtool herunter, und installieren Sie es, da es zum Löschen der Inhalte von mobilen Geräten per Fernzugriff (Remote Wipe) erforderlich ist. Unter Exchange Server 2007 kann Remote Wipe auch mithilfe von Outlook Web Access oder über die Exchange-Verwaltungskonsole gestartet werden.



Andere Microsoft Exchange ActiveSync-Dienste

- Mail-Suche in Exchange Server 2007
- Kalendereinladungen akzeptieren und erstellen
- Suche in der globalen Adressliste
- Zertifikatbasierte Authentifizierung
- E-Mail-Push-Funktion in ausgewählte Ordner
- Autodiscovery

Standardauthentifizierung (Benutzername und Kennwort)

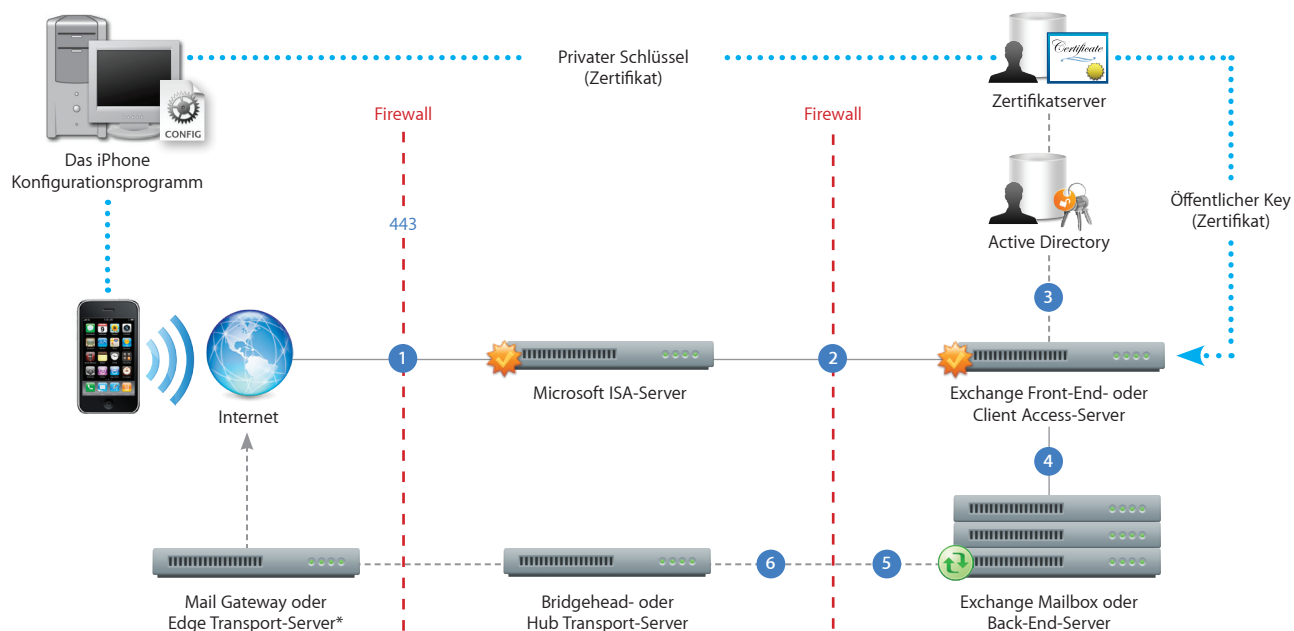
- Aktivieren Sie über den Active Directory-Dienst Exchange ActiveSync für spezielle Benutzer oder Gruppen. Diese sind in Exchange Server 2003 und Exchange Server 2007 standardmäßig für alle Mobilgeräte auf dem Unternehmensniveau aktiviert. Näheres hierzu finden Sie in Exchange Server 2007 unter "Empfängerkonfiguration" der Exchange-Verwaltungskonsole.
- Standardmäßig ist in Exchange ActiveSync die Standardbenutzerauthentifizierung aktiviert. Es wird empfohlen, SSL für die Standardauthentifizierung zu aktivieren, um sicherzustellen, dass Zertifikate während der Authentifizierung verschlüsselt werden.

Zertifikatbasierte Authentifizierung

- Installieren Sie die Zertifikatdienste für Unternehmen auf einem Mitgliedsserver oder Domänencontroller in Ihrer Domäne (dieser dient als Authentifizierungsserver). Weitere Informationen zu den Zertifikatdiensten finden Sie in den von Microsoft erhältlichen Ressourcen.
- Konfigurieren Sie IIS auf Ihrem Exchange-Front-End-Server oder Client-Access Server so, dass die zertifikatbasierte Authentifizierung im Virtuellen Verzeichnis von Exchange ActiveSync akzeptiert wird.
- Deaktivieren Sie "Standardauthentifizierung", und wählen Sie entweder "Clientzertifikate akzeptieren" oder "Clientzertifikate anfordern", um Zertifikate zu akzeptieren oder von allen Benutzern anzufordern.."
- Erstellen Sie mit Ihrem Zertifizierungsserver Clientzertifikate. Exportieren Sie den öffentlichen Schlüssel, und konfigurieren Sie IIS für die Benutzung dieses Schlüssels. Exportieren Sie den privaten Schlüssel, und verwenden Sie das Konfigurationsprogramm des iPhone oder die kabellose Registrierung und Konfiguration, um diesen Schlüssel an das iPhone zu senden.

Exchange ActiveSync-Bereitstellungsszenario

Dieses Beispiel zeigt, wie eine Verbindung zwischen dem iPhone und einer typischen Implementierung von Microsoft Exchange Server 2003 oder 2007 hergestellt wird.



*Je nach deiner Netzwerkkonfiguration bleibt der Mail Gateway oder Edge Transport Server innerhalb des Perimeternetzwerks (DMZ).

- 1 Das iPhone fordert den Zugriff auf Exchange ActiveSync-Dienste über den Port 443 (HTTPS) an. (Dieser Port wird auch für Outlook Web Access und andere sichere Web-Dienste verwendet, daher ist dieser Port in vielen Implementierungen bereits geöffnet und für den SSL-verschlüsselten HTTPS-Verkehr konfiguriert.)
- 2 ISA bietet Zugriff auf den Exchange Front-End- oder Client Access-Server. ISA ist als Proxy konfiguriert oder in vielen Fällen als Reverse-Proxy, um den Verkehr zum Exchange Server abzuwickeln.
- 3 Exchange Server authentifiziert den einwählenden Benutzer über den Active Directory-Dienst und den Zertifikatserver (wenn die zertifikatbasierte Authentifizierung aktiviert ist).
- 4 Wenn der Benutzer das richtige Zertifikat bereitstellt und Zugriff auf die Exchange ActiveSync-Dienste hat, stellt der Front-End-Server eine Verbindung zur zugehörigen Mailbox auf dem Back-End-Server (über den globalen Katalog von Active Directory) her.
- 5 Die Verbindung zu Exchange ActiveSync ist aufgebaut. Aktualisierungen/Änderungen werden kabellos auf das iPhone übertragen, und Änderungen auf dem iPhone werden auf dem Exchange-Server nachvollzogen.
- 6 Gesendete Mail-Elemente auf dem iPhone werden auch mit dem Exchange Server über Exchange ActiveSync synchronisiert (Schritt 5). Um ausgehende E-Mails an externe Empfänger weiterzuleiten, werden E-Mails normalerweise per SMTP über einen Bridgehead- (oder Hub Transport-)Server an einen externen Mail-Gateway (oder Edge Transport Server) weitergeleitet. Je nach der Netzwerkkonfiguration kann der Mail-Gateway oder Edge Transport Server innerhalb des Perimeternetzwerks oder außerhalb der Firewall angesiedelt sein.