Microsoft Exchange Information Services and Security Policies Supported by Android 2.2 and 2.3

Overview

This document describes the Microsoft Exchange information services and security policies that are supported by Android(TM) mobile technology platform releases 2.2 and 2.3. It is intended for Microsoft Exchange administrators who are planning and then implementing support for Android phones and other devices.

Requirements

To support Android 2.2 and 2.3 phones, you must be running Microsoft Exchange ActiveSync 2003 Service Pack 2, Microsoft Exchange ActiveSync 2007, or Microsoft Exchange ActiveSync 2010.

This document describes the Android 2.2 and 2.3 mobile technology platform, including the Settings, Email, Calendar, Contacts, and related applications, as built by Google. Android is

an open-source platform. If a phone's manufacturer has modified Android with its own versions of these applications, you must contact the manufacturer for information about support for Exchange features.

Supported Information Services

Users can add Microsoft Exchange accounts to their Android 2.2 and 2.3 phones by using the Android Account & Sync settings, which are available in the Settings application or directly from the Email application.

Android 2.2 and 2.3 support the following Exchange information services:

- Adding Exchange user accounts (via an ActiveSync server), and enforcement of some mailbox policies (as described in "Supported Security Policies" in this document)
- Synchronizing email, using the Email application
- Synchronizing calendar events, using the Calendar application
- Synchronizing users' contacts, using the Contacts application and shared system-wide
- Autocompletion of email addresses in Email, from a Global Address List (GAL)

If you are running a Microsoft Exchange ActiveSync 2007 or 2010 server, Android 2.2 and 2.3 also support the automatic discovery of your ActiveSync server using only an email address and password, when adding an account (if you have configured your server to support this feature).

Adding accounts, using the Email, Calendar, and Contacts applications, and other features of Android 2.2 and 2.3 are described in the *Android User's Guide,* available at: http://www.google.com/support/android

Supported Security Policies

Android 2.2 and 2.3 support the Microsoft Exchange ActiveSync mailbox policies described in this section (for more information about Microsoft Exchange ActiveSync mailbox policies, see http://technet.microsoft.com/en-us/library/bb123484(EXCHG.80).aspx).

If you establish a mailbox policy for your ActiveSync server, you can also remotely wipe the contents of any phone that has added an account from your server, as described in this section.

Require password

If you set this ActiveSync mailbox policy, users must secure their phones using a numeric PIN

or alphanumeric password (using the PIN or Password option in the Android Screen Unlock Security settings).

The other ActiveSync mailbox policies have no effect if this policy is not set.

Require alphanumeric password

If you set this ActiveSync mailbox policy, users must secure their phones using a password that includes both letters and numbers (only the Password option is available in the Android Screen Unlock Security settings).

If you don't set this mailbox policy, users may secure their phones with a password or a numeric PIN (both the Password and PIN settings are available).

Number of failed attempts allowed

This ActiveSync mailbox policy sets the maximum number of times a user can enter an incorrect password before the phone resets itself to factory defaults (a local wipe). See the section on performing a remote wipe, in this document, for details about the effects of the factory data reset performed by a local or remote wipe.

Android 2.2 and 2.3 support a maximum of 31 failed password attempts for this setting.

Minimum password length

This ActiveSync mailbox policy sets a minimum number of letters or numbers for an PIN or password.

Android 2.2 and 2.3 support PINs and passwords of up to 16 characters.

Time without user input before password must be re-entered

This ActiveSync mailbox policy sets the maximum number of minutes after a user has last touched the screen or pressed a button before the phone locks itself, requiring the user to unlock the phone with a PIN or password. On Android phones, this restricts the Screen Timeout setting to a duration less than or equal to the value of the policy you set.

Android 2.2 and 2.3 support a maximum of 30 minutes for this setting.

Allow non-provisionable devices

This ActiveSync mailbox policy controls whether devices that support some but not all of your mailbox policies can synchronize information with your Exchange server.

If all of your mailbox policies are supported by Android 2.2 or 2.3 (as described in this section), this policy has no effect on Android phones.

If some of your mailbox policies are not supported by Android and you set this policy, users can add Exchange accounts to their phones, synchronize information, and Android will enforce those of your policies that it does support.

If some of your mailbox policies are not supported by Android and you don't set this policy, users can not add Exchange accounts to their phones and any existing accounts will be prevented from synchronizing information in the future (no existing information is deleted).

Remote wipe

If you establish a mailbox policy on your ActiveSync server, you can perform a remote wipe of any Android 2.2 or 2.3 phone that has added an account from your server. A remote wipe performs the same action as a factory data reset (a feature of the Android Privacy settings): it erases all of the user's personal data from internal phone storage, including information about the user's Exchange accounts, Google Accounts, and any other accounts. It also erases all application settings and any downloaded applications. A remote wipe does not erase any system software updates the user has downloaded or any files on the phone's SD card, such as music or photos.

Conflicting security policies

Android 2.2 and 2.3 phones can add accounts and sync information from multiple Exchange servers; they can also add multiple Google Accounts and other kinds of accounts. Each of these accounts may have security policies that are enforced by Android. If accounts have conflicting security policies, Android enforces the strictest rules set by any account for each kind of policy; in other words, no account policy can relax the degree of security set by another account policy.

Legal

Availability of Google applications, services, and features may vary by country, carrier, phone model, and manufacturer.

Please address questions or comments about this document to: userdocs@android.com

AEW01-23-003