Android 4.0.4 Support on Galaxy Nexus, Nexus S, and Motorola Xoom for Microsoft Exchange Policies

Overview

This document describes the Microsoft Exchange information services and security policies supported by the Android™ mobile technology platform 4.0.4, codenamed Ice Cream Sandwich, running on Galaxy Nexus and Nexus S phones and the Motorola Xoom tablet. These three devices are referred to in this document as "pure Google" devices. The information presented here is intended for Microsoft Exchange administrators who are planning and implementing support for any of these pure Google devices running Ice Cream Sandwich.

Requirements

To support Android 4.0 running on pure Google devices, you must be running one of the following versions of Microsoft Exchange:

- Exchange Server 2010 SP1 with Exchange ActiveSync 14.1
- Exchange Server 2010 with Exchange ActiveSync 14.0
- Exchange Server 2007 SP1 with Exchange ActiveSync 12.1
- Exchange Server 2007 with Exchange ActiveSync 12.0
- Exchange Server 2003 SP2 with Exchange ActiveSync 2.5

This document describes the Android 4.0.4 platform, including the Settings, Email, Calendar, People, and related apps as built by Google. If a device manufacturer has modified these apps on its own devices, you must contact the manufacturer for information about support for Exchange features.

Supported Information Services

Users can add Microsoft Exchange accounts to their pure Google devices by using the Account & Sync settings available from the Settings or Email app.

Android 4.0 supports 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
- Searching email, using the Email application
- For Exchange 2010 only, synchronizing information about messages that have been forwarded or replied to.
- Synchronizing calendar events, using the Calendar application
- Synchronizing users' contacts, using the People application and shared system-wide
- Auto-completion from a Global Address List (GAL) when searching for email addresses and other contact info in Email, Gmail, People, Phone, and Calendar.

If you are running a Microsoft Exchange 2007 or 2010 server, Android 4.0.4 also supports the automatic discovery of your Exchange 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 People applications, and other features of Android 4.0 running on pure Google devices are described at http://support.google.com/ics/nexus.

Supported Security Policies

Pure Google devices 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.aspx).

If you establish a mailbox policy for your Exchange server, you can also remotely wipe the contents of any device that has added an account from your server. For details, see Remote Wipe policy described below.

Require password

If you set this ActiveSync mailbox policy, users must secure their devices using a PIN or alphanumeric password (using the PIN or Password options in **Settings > Security > Screen lock**).

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 devices using a password that includes both letters and numbers (only the Password option is available in **Settings > Security > Screen lock**).

If you don’t set this mailbox policy, users may secure their devices 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 device resets itself to factory defaults (a local wipe). See Remote Wipe policy below for details about the effects of the factory data reset performed by a local or remote wipe.

Pure Google devices 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.

Pure Google devices support PINs and passwords of up to 16 characters.

Minimum password complex characters

This ActiveSync mailbox policy sets a minimum number of non-letter characters in the password.

Restrict password history

This ActiveSync mailbox policy prevents users from reusing the last *n* unique passwords.

Password expiration timeout

This ActiveSync mailbox policy specifies the password expiration timeout. Email will not synchronize until the user specifies a new password.

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 device locks itself, requiring the user to unlock the device with a PIN or password. On pure Google devices, this restricts the **Settings > Display > Sleep** setting to a duration less than or equal to the value of the policy you set.

Allow non-provisionable devices

This ActiveSync mailbox policy controls whether pure Google 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 (as described in this section), this policy has no effect.

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

Allow attachment download

This policy controls whether email attachments can be downloaded to devices.

Maximum attachment size

This policy limits the maximum size of email attachments that are automatically downloaded.

Disable camera

This policy controls whether the device camera can be used.

Require device encryption

If you set this ActiveSync mailbox policy, users must secure their devices with encryption. Emails will cease to synchronize if the device is not encrypted.

Require storage card encryption

If you set this policy, the Galaxy Nexus and Nexus S phones, which don't have a separate SD card, will require the user to encrypt the device. Motorola Xoom does not support this policy.

Remote wipe

If you establish a mailbox policy on your Exchange server, you can perform a remote wipe of any pure Google device that has added an account from your server. A remote wipe performs the same action as a factory data reset (**Settings > Backup & reset > Factory data reset**): it erases all of the user's personal data from internal storage, including information about the user's Exchange accounts, Google Accounts, and any other accounts. It also erases all app settings and any downloaded applications. A remote wipe does not erase any system software updates the user has downloaded or any files on the device's shared storage, such as music or photos.

Require manual sync while roaming

If you set this ActiveSync mailbox policy, users must manually synchronize their devices while roaming in order to avoid unexpected data costs.

Allow/Bock/Quarantine(ABQ) list

This policy lets you control device access to mailboxes based on device model or type.

Conflicting security policies

Pure Google devices 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, device model, and manufacturer.