



Over-the-Air Sync Control

With the convenience of wireless, remote access to a Microsoft® Exchange Server to synchronize personal business data (email, calendar, contacts, tasks) lies a hidden danger — there is no way to enforce the protection (encryption) of corporate data on these devices. The loss or theft of an unprotected device could result in loss of customer data and a subsequent (and very expensive and embarrassing) public breach notification. CREDANT Mobile Guardian's Over-the-Air (OTA) Sync Control provides a simple means for enterprises to detect handhelds and smart phones attempting to wirelessly connect to the Exchange Server, and to enforce the protection of those handhelds in order to prevent a possible data breach.

There are two main methods of synchronizing Exchange data between handhelds and the Exchange Server: Local ActiveSync (via a cradle connected to a host PC) and Exchange ActiveSync (via an internet connection direct to the Exchange server). In both cases, live data — emails, contacts, customer information, etc. — is copied to the handheld, presenting a potential security risk if the handheld is unprotected and subsequently lost or stolen. It is therefore critically important that a mobile data security solution be able to detect unprotected devices and to enforce protection of any sensitive company data stored on those devices.

While CREDANT Mobile Guardian already manages the detection and security of cradle synchronization, OTA Sync Control provides the means to control wireless, OTA handheld synchronization for Exchange ActiveSync®.

OVERVIEW

When a company's mobile workforce synchronizes its mobile devices through Microsoft® Exchange ActiveSync, the company has no way to control or protect the device and their data. However, CREDANT Mobile Guardian Over-the-Air (OTA) Sync Control allows enterprises to control such rogue mobile devices. It allows an enterprise to block any device not protected by a CREDANT Shield from accessing Exchange, even if an end user has permissions to use Exchange ActiveSync. This closes out a major vulnerability with respect to mobile wireless devices, as shown in Figure 1.

The OTA Sync Control is an ISAPI plug-in for the Microsoft Front End Exchange Server. It monitors incoming Exchange ActiveSync requests from handhelds and, if no CREDANT Shield is present, returns an error message to the handheld, preventing any further synchronization and optionally directing the user to a web link where they can immediately install the CREDANT Shield. It will prevent any mobile device that is using Exchange ActiveSync (Windows Mobile, Palm, or Symbian®) from synchronizing with the user's Exchange email, calendar, contacts, and tasks until the CREDANT Shield is installed.

MICROSOFT EXCHANGE SERVER ACTIVESYNC®

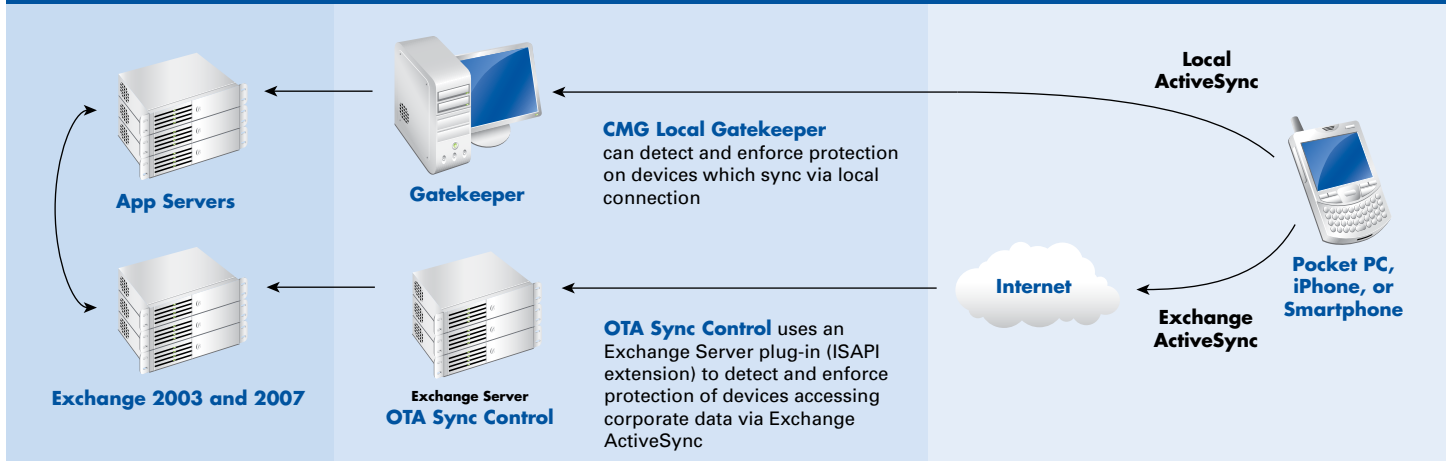
Introduced with Microsoft Exchange Server 2003, Exchange ActiveSync allows a wireless handheld running ActiveSync 4.x and above to sync corporate information — Email, Calendar, Tasks, and Contacts — directly with the Exchange Server, without having to go through an intermediate Laptop/PC. Wireless connections such WLAN, WWAN, and Bluetooth modem are fully supported. In addition, handheld users can configure the device to use an optional feature called Always Up To Date (AUTD), which can provide asynchronous email notification. Configuration of the handheld for Exchange Server ActiveSync is very simple, requiring only Username, Password, and the Exchange Server name.

Both Exchange ActiveSync and AUTD require the appropriate permissions to be set by the Exchange administrator. This is done per user, not per device, and there is no way that the Exchange server can check which device the user is using, or whether the device is protected. For some Windows Mobile devices, Exchange can enforce password protection and some minimal security, but this functionality is not available for all Pocket PC and Smartphone devices.



Over-the-Air Sync Control

Figure 1. CREDANT Mobile Guardian's Over-the-Air Sync Control



USER SCENARIO: HOW IT WORKS

- User 'Bob' receives appropriate permissions on the Exchange 2003 or 2007 Server, i.e., Exchange ActiveSync is enabled for Bob.
- Bob buys a wireless handheld device and configures it to use Exchange ActiveSync (adds username, password, server name, and email account details). No CREDANT Shield is present.
- Bob initiates an Exchange ActiveSync session by selecting the 'Sync Now' button, at which time the:
 - Device sends an HTTP request to the Front End Exchange Server that is intercepted by the CREDANT ISAPI extension.
 - CREDANT ISAPI extension retrieves necessary information about the device and user from the HTTP request, and calls the CREDANT Policy Proxy to determine if the device has a CREDANT Shield.
 - CREDANT Policy Proxy verifies whether a CREDANT Shield on this device has communicated with the Policy Proxy within a determined timeframe set by the administrator, for example 8 hours. If a CREDANT Shield is not detected for this device, the CREDANT Policy Proxy returns a "no CREDANT Shield present" message to the ISAPI extension.
 - CREDANT ISAPI extension sends a customizable HTML reply to the device, notifying the user that sync cannot occur until the CREDANT Shield is installed. This message can include a link that allows the user to download and install the CREDANT Shield for immediate remediation. NOTE: OTA Sync Control can be configured to block or allow iPhone access to Exchange ActiveSync, but a Shield for iPhone is not available at this time.
- Bob now loads the CREDANT Shield on to his device, initiates a sync, and this time the CREDANT Policy Proxy confirms the presence of a CREDANT Shield to the ISAPI extension and allows the Exchange ActiveSync session to continue.

IMPLEMENTATION ARCHITECTURE

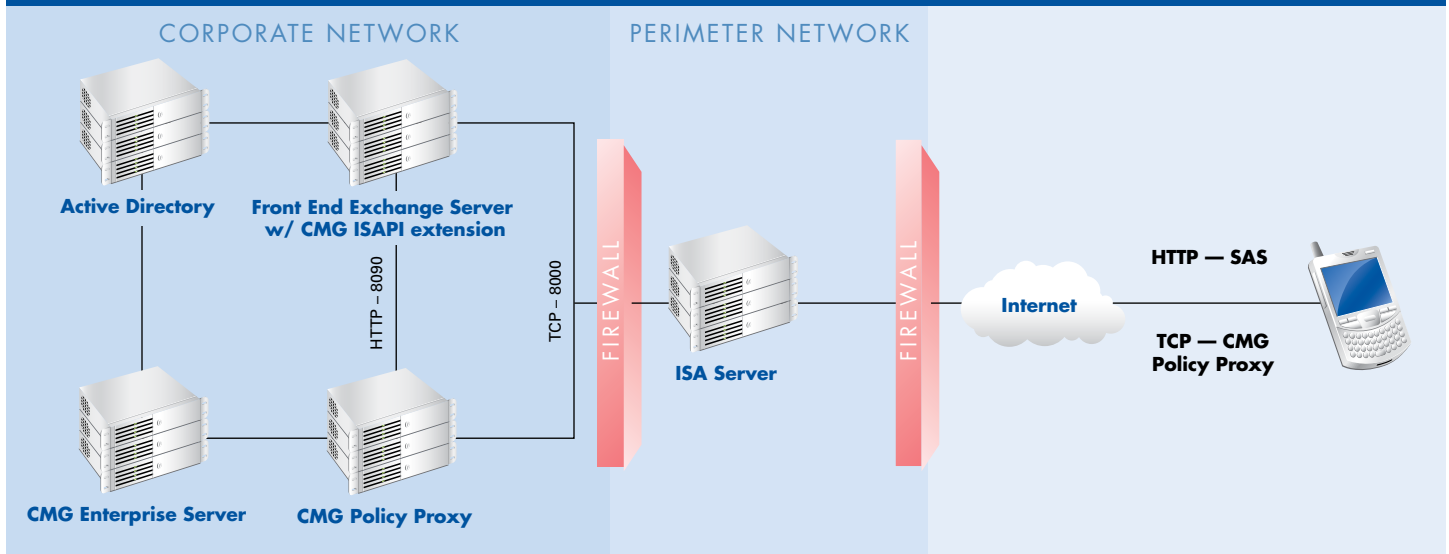
Figure 2 (on the following page) represents the architecture of a typical Exchange implementation.

The OTA Sync Control component is an ISAPI extension that resides on the Front End Exchange Server. For CREDANT Enterprise Edition customers, this extension is the only additional



Over-the-Air Sync Control

Figure 2. Typical Exchange Implementation Architecture



software that has to be installed. Port 8090 must be opened on the Front End Exchange Server to allow communication between the CREDANT Policy Proxy and the OTA Sync Control plug-in.

The available settings to configure OTA Sync Control are:

ENABLE OTA SYNC CONTROL

This CREDANT Server policy turns OTA Sync Control on or off for a user, a group of users, or everyone

EXCHANGE ACTIVESYNC BLACKLIST

blocks individual users or devices from synchronizing even if the CREDANT Shield is installed — based on username or device unique ID.

EXCHANGE ACTIVESYNC WHITELIST

allows Exchange ActiveSync access for individual users or devices even if their device does not have CREDANT Shield installed — based on username or device unique ID.

FAILURE MESSAGE

the message presented to the user upon failure to sync because no CREDANT Shield is present on that user's device.

MINIMUM OTA SYNC POLLING THRESHOLD

this CREDANT Server policy defines how often to verify that a device is still Shielded.

SUMMARY

CREDANT Mobile Guardian OTA Sync Control solves the problem of authorized users using unauthorized (un-protected) handheld devices to access their Exchange data. OTA Sync Control monitors all Exchange ActiveSync traffic and enforces protection by refusing access to devices not protected by a CREDANT Shield. In doing so, it ensures that any corporate data within Exchange (Inbox data including attachments, Calendar, Contacts, Tasks) is encrypted in the event that a device is lost or stolen. CREDANT's OTA Sync Control enables customers to be compliant with State and Federal legislation that is increasingly surrounding data security.