

Exchange 2003 Mobile Messaging Part 3 – Installing, Administering, and Using the Microsoft Exchange

Contributed by David Noel-Davies

In the last article in this series we covered how you, with the help of properly configured device security settings, could have a device erased (similar to a local wipe) after a user entered x number of incorrect PINs or passwords. But there may be situations where you want to have a lost or stolen device wiped immediately. This is where the Exchange Server ActiveSync Web Administration tool comes into the picture. The tool is designed for administrators who want to manage the process of remotely erasing lost, stolen, or otherwise compromised mobile devices. With the Exchange Server ActiveSync Web Administration Web tool, administrators can perform the following actions:

- View a list of all devices that are being used by any enterprise user
- Select/De-select devices to be remotely erased
- View the status of pending remote erase requests for each device
- View a transaction log that indicates which administrators have issued remote erase commands, in addition to the devices those commands pertained to

The Microsoft Exchange Server ActiveSync Web Administration Tool is designed specifically for Exchange Server 2003 with SP2 applied and Windows mobile 5.0 devices, but the tool is also supported on SBS 2003. Bear in mind though that there are a few issues to be aware of when installing the tool on SBS 2003. I won't go into detail on those issues here, but instead refer you to the Troubleshooting section in the Deploying Windows Mobile 5.0 with Windows SBS whitepaper. Installing Exchange Server ActiveSync Web Administration tool There's no hocus pocus in installing the Microsoft Exchange Server ActiveSync Web Administration Tool, when you have downloaded a copy here you simply extract the MobileAdmin.exe file, then run the MobileAdmin.msi package on your Exchange 2003 SP2 front-end server (or back-end server if you only have one Exchange Server in your organization).

When the installation wizard appears click Next (see Figure 1 below).

Figure 1: Microsoft Exchange Server ActiveSync Web Administration Tool Installation Wizard Accept the EULA then click Next once again. Let the installation complete, then click Finish to exit the installation wizard. Using Exchange Server ActiveSync Web Administration tool When the Exchange Server ActiveSync Web Administration tool has been installed, you can access the mobile admin tool from any remote computer by typing <https://server/mobileadmin> in your browser. You will then be asked to authenticate, and in order to access the tool you need to do so using an account which is a member of either Exchange administrators or local administrators on the server (or another group or account that has been given permissions to the MobileAdmin virtual directory, see instructions on how to do so later in this article).

When you have authenticated with an account with appropriate permissions, you get the Mobile Admin Web Form shown in Figure 2.

Figure 2: Mobile Admin Web Form From here you can select between the two administrative options Remote Wipe and Transaction Log. Let's start by selecting the Remote Wipe option. From here you can manage the user's devices, or more specifically initiate remote wipes for specific devices and/or cleanup device partnerships (Figure 3).

Figure 3: Remote Device Wipe In order to see which devices are associated with a particular mailbox, you need to either enter the mailbox name or SMTP address of the user. When you have done so you'll get a list similar to the one in Figure 3, which has 5 columns, all listed below:

- Device Id
- Type (whether it's a SmartPhone or PocketPC)
- Last Sync (time and data when last sync was performed)
- Status (Status of the device can be either OK, Wipe initiated, Sent to device, Device acknowledged and Wipe operation completed successfully)

- Action (where you can select to either Wipe a device or delete a partnership) As you can see in Figure 3 one of the partnerships listed hasn't been synchronized since November 2005, it should therefore be safe to delete it. So let's hit Delete and see what happens. First we're asked whether we really want to delete this partnership (Figure 4).

Figure 4: Partnership deletion confirmation box When clicking OK the partnership is deleted and a few seconds later it will no longer appear on the list of associated partnerships. When a partnership is deleted it's logged in the Transaction log as can be seen in Figure 5. Deleting a partnership will clean out all state information associated with the particular mobile device on the server, and is primarily useful for housekeeping purposes. If a device which had its partnership deleted is connected again, it will be forced to re-establish the deleted partnership with the server through a recovery process. But don't worry, this process is completely transparent to both you as the Exchange administrator as well as the end user.

Figure 5: Partnership deletion log entry in Transaction log When you initiate a remote wipe action, it will remain active until you cancel it via the Cancel Wipe option shown in Figure 6, this means that the server will continue to send a remote wipe to a device (even though the device has been remotely wiped already), so remember to cancel the remote wipe action after a lost or stolen device has been recovered.

Figure 6: Remote Wipe initiated As can be seen in Figure 7 below a remote wipe of a device will be logged in the Transaction log.

Figure 7: Remote Wipe entry in the Transaction log Controlling Access Permissions As mentioned earlier in this article

only Exchange Administrators and local administrators on the Exchange server are allowed to use the Microsoft Exchange Server ActiveSync Web Administration tool, but chances are you want to allow helpdesk personnel or other individuals in your IT department access to the tool as well. In order to do so without adding them to the respective groups, you can allow them access by modifying the permissions on the Microsoft Exchange ActiveSync Administration installation folder, which after a default installation can be found under C:\Program Files as shown in Figure 8 below. Figure 8: Microsoft Exchange ActiveSync Administration installation folder Here you simply right-click the installation folder then select Properties. On the property page click the Security tab then add the group(s) or user(s) who need access to the tool (Figure 9).

Figure 9: Giving additional groups or users access to the tool
Known Issues If you receive an HTTP 401 error message when either trying to delete a partnership or initiating a remote wipe, it's most likely because Integrated Windows authentication isn't enabled on the Exadmin virtual directory and/or because the MobileAdmin virtual directory doesn't run under the ExchangeApplicationPool application pool. If this is the case please see MS KB article 916960. As mentioned in the beginning of this article you may also run into problems when running the tool on an SBS 2003. To resolve these problems see the Troubleshooting section in the Deploying Windows Mobile 5.0 with Windows SBS whitepaper. Conclusion In this article which is part 3 in a 5 part article series on Exchange Mobile Messaging, we covered how to install, configure and most importantly use the Exchange Server ActiveSync Web Administration Web tool, which offers you, as an Exchange administrator, features that will help manage and protect the mobile devices in your organization even better than was previously possible. In Part 4 I'll uncover the new GAL lookup feature, which surprisingly enough, also is a feature included in Exchange 2003 SP2 and the Messaging and Security Feature Pack (MSFP).