IceWarp Unified Communications

Exchange ActiveSync Guide

Version 10.3

Printed on 30 March, 2011

Contents

CHAPTER 1

Exchange ActiveSync Guide

About

Exchange ActiveSync (EAS) is a proprietary data synchronization protocol created by Microsoft for wireless synchronization of mobile devices with Exchange Server. IceWarp has licensed this protocol to support native over-the-air synchronization of iPhone and Windows Mobile powered devices without the need to install any synchronization plug-in, thus reducing deployment time and enabling new features not available with the open SyncML protocol.

Exchange ActiveSync is optimized to work together with high-latency and low-bandwidth networks typical to mobile devices environments. The protocol, based on HTTP and XML, lets smartphones gain centralized access via IceWarp Server to an organization's most important information. IceWarp with ActiveSync enables mobile device users to access their e-mail, calendar, contacts, and tasks and to have access to this information also while they are working off-line.

To avoid any doubt, the desktop ActiveSync application (Communication Center in Windows Vista) is using a different XML-based communication protocol to synchronize locally connected devices (tethered via Bluetooth, serial or USB). Similarly, iSync in Mac OS X is using a proprietary SyncML-based protocol for synchronization of devices connected locally to the user's computer. Neither of these protocols is supported by IceWarp Server.

Trademarks and Support Disclaimer

Windows, Vista, Exchange, SQL Server, ActiveSync, AutoDiscover, DirectPush, RemoteWipe are registered trademarks of Microsoft Corporation. Blackberry, BIS (Blackberry Internet Service), BES (Blackberry Enterprise Server) are registered trademarks of Research In Motion Inc. iPhone, iSync, Mac, OS X are registered trademarks of Apple Inc. Symbian is a registered trademark of Symbian Software Ltd. Palm, Palm OS, WebOS are registered trademarks of Palm Inc. Android is a registered trademark of Google Inc. Nokia for Exchange is a registered trademark of Nokia Corporation. NotifySync is a registered trademark of Notify Corp. AstraSync is a registered trademarks of MailSite Software Inc. Moxier is a registered trademark of Emtrace Technologies, Inc. MySQL is a registered trademark of MySQL AB.

For support of the aforementioned products, or to inquire about legal and privacy issues arising from their use, please contact the respective vendors or visit their websites for more information.

Compatibility

Exchange ActiveSync supports many mobile operating systems out of the box:

- Windows CE, PocketPC
- Windows Smartphone
- Windows Mobile 5,6
- iPhone OS X
- Symbian S60, S90 powered Nokia phones (latest firmware)
- Palm OS 4
- Palm WebOS
- Google Android (selected models)

If native ActiveSync support is not available, optional 3rd party application needs to be installed on the device to allow synchronization using ActiveSync:

- Older versions of Nokia N Series, E Series, S60 v3: ***Mail for Exchange*** (free download from Nokia)
- Symbian S60/S80/S90/UIQ: ***DataViz RoadSync***
- BlackBerry: ***Notify Corp NotifySync*** (OS 4.0 and higher), ***MailSite Software AstraSync*** (OS 4.2 and higher – 8xxx, 9xxx series)
- Android OS: ***Exchange*** by ***Touchdown*** or ***Moxier Mail*** by ***Emtrace Technologies***.
- Motorola with Java MIDP 2.0: ***DataViz RoadSync***

Features

ActiveSync allows synchronization of the following items (not all items need to be supported by the client device):

- Emails
- Contacts
- Calendars
- Tasks
- DirectPush always-on capability for Email, Contacts, Calendars, Tasks

Advanced and device management features:

- Synchronization of the complete folder structure
  - including shared and public folders
  - displaying non-email folders in IMAP folder structure
  - multiple folder synchronization (if supported by device)
  - selecting folders to synchronize with built-in applications
- Folder management (available only on Windows Mobile 6.0 and higher)
  - add/delete/rename/move operations on folder tree
- Complete email handling (send, reply, forward, mark read/unread etc.)
- Attachment handling (including Windows Mobile platform)
- Using filters (user defined synchronization)
  - Email look-back range – sync emails not older than specified number of days
  - Email filters – sync messages of given size, or not including an attachment
  - Event look-back range – sync events within number of days in the past
  - Tasks – sync tasks that are not marked as completed
- Device Management and Provisioning
  - Listing all connected devices by domain/user including exact model name
  - RemoteWipe to wirelessly delete all data from a stolen/lost handheld
- Remote look-up in company-wide Global Address Lists (GAL)
  - email address auto-complete
  - email contact list look-up

- AutoDiscover
  - simplifies the device setup to entering just username and password
- SmartSync
  - smartly recovers from situations when network error occurs during server response to client requests
- Meeting invitation retrieval and accept/decline actions
  - only if created in WebClient or IceWarp Desktop Client
- Security policies
  - to enforce device password, its strength, maximum allowed unlock attempts, local wipe to delete all data in case of abuse

Current Limitations

- EAS 2.5 full support only, 12.1 devices will gracefully fallback to 2.5 Safe Mode
- EAS 12.0 AutoDiscover and attachments only supported
- EAS 12.1 only envelope (basic sync capabilities) supported
- TNEF formatted meeting invitations (sent from Outlook) are not supported (can not be responded to by the means of EAS or IceWarp WebClient)
- EAS 12.1 specific features (Exchange 2007: S/MIME resolve recipients and decryption, selective download of multiple attachments, extended security provisions, password recovery, search Boolean) are not supported
- No Out of office settings support
- HTML email is translated into plain text for Windows Mobile

Over-the-air Synchronization Advantages

- No middleware servers
- No desktop sync software or cables
- No service or subscription fees

Advantages over SyncML

- Broad device support for out-of-the-box functionality
- Device management features
- Push over TCP/IP
- Access to shared folders
- Multiple folder synchronization on some devices

DirectPush Advantages

- Immediate notification of new emails
- Suitable for slow connections (GSM, WAP, EDGE)
- Messages are downloaded in the background as they arrive
- No fees for SMS alerts

SmartSync Advantages

- Completes the sync gracefully where normal server would initiate a full synchronization
- Saves data transfers, time and battery life
- Ensures data consistency by resolving any possible conflicts
- Prevents infinite loops on synchronization errors
- Suited to networks/areas with low quality of data connection

GroupWare Mailbox Access

- Access to Files, Notes, Tasks within the built-in e-mail application
- One-way synchronization from server to handheld
- Independent on the file size limit of email
- No applications required, works out-of-the-box
- Simple configuration
- SSL-secured access (HTTPS)

ActiveSync Compatibility Matrix

	Windows Mobile **Windows PocketPC** **Windows SmartPhone**	**iPhone** **iPhone 3G**	**Nokia N Series** **Nokia E Series**	**Palm OS 4, 5**	**Palm WebOS**
Plugin required	No	No	No Mail for Exchange (free)	No	No
Email	•	•	•	•	•
Calendar	•	•	•	•	•
Contacts	•	•	•	•	•
Tasks	•	-	•	•	•
DirectPush	• **	•	•	•	•
Push Schedule (Peak/Off-peak)	-	-	•	-	-
GAL Lookup	•	•	•	•	•
Subfolders	•	• ***	-	-	•
Folder Management	6.x	-	-	-	-
Filters email/ calendars/ tasks	•/•/•	•/•/-	•/•/•	•/•/-	•/•/•
AutoDiscover	• **	•	-	-	-
RemoteWipe	•	•	•	-	-
Security Provisioning	•	•	•	-	-
iMIP (meeting response)	•	•	•	•	-

	Android **TouchDown**	**Android** **Moxier**	**BlackBerry** **NotifySync**	**BlackBerry** **Astrasync**	**Symbian** **S60, S80, S90, UIQ** **RoadSync**
Plugin required	Yes NitroDesk TouchDown	Yes Moxier Mail	Yes NotifySync	Yes AstraSync	Yes DataViz** RoadSync
Email	•	•	•	•	•
Calendar	•	•	•	•	•
Contacts	•	•	•	•	•
Tasks	•	•	•	-	-
DirectPush	•	•	•	•	
Push Schedule (Peak/Off-peak)	•	•	•	•	•
GAL Lookup	•	•	•	•	•
Sub-folders	•	•	•	•	-
Folder Management	-	-	-	-	-
Filters email/calendars/ tasks	•/•/•	•/•/•	•/•/-	•/•/-	•/•/-
AutoDiscover	-	•	-	3.x	-
RemoteWipe	•	-	•	3.x	•
Security Provisioning	•	-	•	3.x	•
iMIP (meeting response)	•	-	•	3.x	•

• available

- not available

* DirectPush support is only available on PDAs and smartphones that are running Windows Mobile 5.0 with the Messaging and Security Feature Pack (MSFP/AKU2) and higher (Windows Mobile 6.x). Additionally, SSL with a trusted certificate must be enabled on Windows Mobile devices for DirectPush and AutoDiscover to work properly. See the **SSL and Windows Mobile Devices** chapter.

** RoadSync comes preloaded on select LG, Nokia, Samsung and Sony Ericsson handsets or can be installed as new on most Symbian powered devices. Roadsync Beta is also available for Android. RoadSync (email only) is also available for Java MIDP 2.0 Motorola phones (RAZR, KRZR…) and Palm OS devices.

*** iPhone supports multiple folders (groups) in Mail, Contacts, Calendar, but does not support folder modification.

In This Chapter

On-server Setup

Setting up ActiveSync in IceWarp Server is easy since it does not have almost any administration controls.

1. In **Help – Licenses**, verify that you have at least one valid client license for **ActiveSync**. If expiration shows negative days, the license (full or trial) already expired and you need to obtain an updated license.
2. In **GroupWare - General - Push Server**, verify that the **Push** service is ***Active*** and its default port is not blocked by another local service. You may want to change the port number. You do not need to open any ports on the firewall as this service only runs locally.

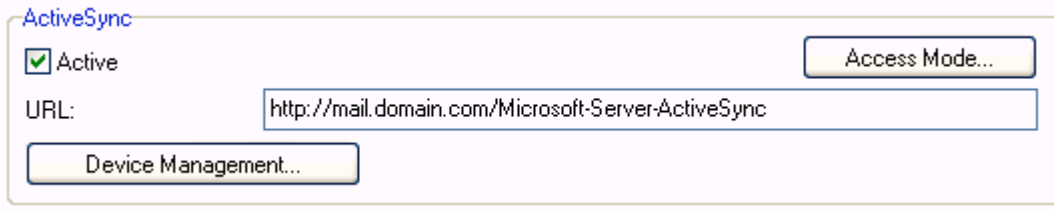
   If you do not intend to use **DirectPush** on any devices which keep the device always up-to-date, but also consume considerable battery power, you may want to leave this service inactive.
3. In **System – Services**, verify that **Control** service is running.

   Open the service properties. Verify the port is set to standard HTTP port 80. If not, set it to use port 80. If the service does not start, it means it is being blocked by another service (such as Microsoft IIS) and you need to either stop the other service or change its port. ActiveSync will not work unless you have the **Control** service running on port 80.
4. For **GAL** lookup, you either need to have one public folder tagged as GAL, or the GAL will be populated with all server users. See the **GAL Public Folder** section for details.
5. Enable **SSL** on default ports for IMAP (993) and HTTP (443) in **System – Services**. SSL ensures that mail and other data are securely encrypted during wireless transmission. Your IMAP service may however run on any ports desired.

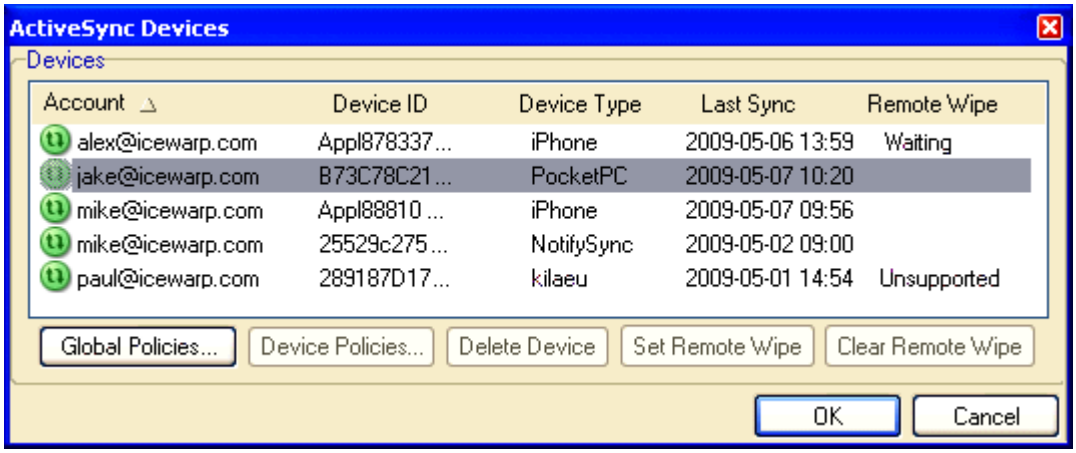
   ActiveSync is an encapsulated protocol, the ports to have open on your firewall are only tcp/80 (HTTP) & tcp/443 (HTTPS). Communication between GroupWare, IMAP services and ActiveSync will be internal on the server.
6. In the **Web Service** node, under the ***Default*** host or another host you have configured, verify that in **Scripting** tab it shows the ***[activesync]*** and ***[autodiscover]*** extensions associated with ***php\php.dll***. For details, see the **Troubleshooting** (on page 33) section.
7. In the **ActiveSync** node, check ***Active*** to enable **ActiveSync** on the server. Do not modify the port and URL end part. Change only the hostname if required by a special setup.

   Check that WebDAV access is enabled on the **Options** tab for the host under **Web Service**.
8. In **Access Mode**, select an option such as ***All accounts*** or ***Accounts from list***. If you decide for the latter, make sure that in user's properties in **Management – <user@domain> – Options**, the ***ActiveSync*** checkbox is ticked for that users.
9. For **AutoDiscover**, check that in **System - Services – SmartDiscover** the same URL appears as in the **ActiveSync** node ***URL*** field. See the **SmartDiscover** section for details.

   In **System - Services - Control - Properties**, verify that SSL port is set to use port 443. **AutoDiscover** will not work without this setting.
10. For additional security protection and best AutoDiscover/DirectPush performance, install a digital certificate on the server from a trusted certificate authority such as **Verisign**.



Field	Description
Active	Check this option to enable the **ActiveSync** functionality.
URL	URL consists of: ▪ The server address or alias: <***mail.domain.com***> This hostname (alias) has to be set in a client exactly otherwise synchronization will not work. NOTE that default ports (80 for HTTP, 443 for HTTPS) are not specified. The use of other ports for control service is NOT recommended – the service could fail. ▪ The path specified by Microsoft – ***Microsoft-Server-ActiveSync*** NOTE that this part of URL cannot be changed. This part is only made visible for troubleshooting, so that you can identify the session in web server logs. This URL tells you where each ActiveSync capable device connects by default. You should not use this URL part in server name when setting up the device!
Access Mode	Push the button to define the **ActiveSync** access mode.
Device Management	Click this button to reveal the **ActiveSync Devices** dialog. This dialog lists all devices that use ActiveSync. See lower.



Button	Description
Global Policies / Domain Policies / User Policies	Click the button to set security policies on server/domain/user level for all devices. For more details, refer to the **Security Policies** (on page 11) section.
Device Policies	Click the button to set individual security policies for the selected device. For more details, refer to the **Security Policies** (on page 11) section.
Delete Device	Click the button to delete the selected device. This action will remove the device from the ActiveSync database and will cause it to full synchronize on the next scheduled or manual sync. This option can be safely used to resolve some synchronization errors without affecting other devices.

Set Remote Wipe	Click the button to initiate ***Remote Wipe*** for the selected device. You will be asked to confirm that you wish to wipe the device. Once ***Remote Wipe*** is initiated, you can observe its status in the Remote Wipe column. The dialog will automatically refresh as the ***Remote Wipe*** command is in progress. **Unsupported** means that the device does not support ***Remote Wipe*** (or other security provisions as well). **Waiting** means that the command will be sent upon the next synchronization, if the device is not set for Push or out of coverage, the server needs to wait before it reconnects. After ***Remote Wipe*** is successfully performed on a device, the **device is deleted from the list** and the system sends an acknowledgment message to the account owner (and system administrator in Cc) as soon as the device receives the wipe command, alerting the account owner that the wipe occurred (and has been completed successfully). The **device will appear in the list** again after the first successful synchronization once the ActiveSync account has been reconfigured. NOTE that ***Remote Wipe*** is specific to a device, user can synchronize his/her account with a secondary device even if Remote Wipe has been initiated (in Waiting state) for the primary device.
Clear Remote Wipe	Click the button to cancel set ***Remote Wipe***. You will be asked to confirm it. You can cancel ***Remote Wipe*** only when it is in the ***Waiting*** state before another synchronization. Normally you will have little chance to cancel ***Remote Wipe*** if the device is enabled for Push.

Security Policies

Security Policies can be applied to mobile devices synchronizing data with IceWarp Server over ActiveSync protocol, to impose a greater level of security on sensitive user data, including e-mail, contacts, address book entries and any other data or documents stored on the mobile device. Security Policies are enforced by the server before the transmission of any user data occurs, and the device is provisioned upon the next synchronization over-the-air even if the policy did not apply to it before.

It's recommended to use them corporate-wide, exempt as little users as possible, replace any non-compatible devices with fully compatible models or upgrade the firmware or operating system of partially capable devices with a fully compatible version (e.g. Microsoft Feature Pack for Windows Mobile 5.0).

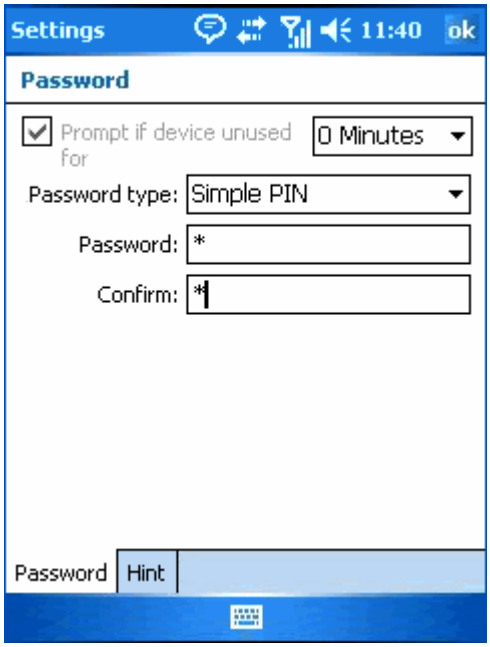
When coupled with the remote device wipe mechanism (Remote Wipe), these Security Policies help to provide an effective means of preventing an attacker from recovering data from a device. At the same time they allow engaging the built-in device passlock, with the (strongly recommended) option to perform off-line device wipe (Local Wipe) in case the unlock attempts are expended. This leaves little room for a potential attacker to guess the password, and deletes all user data after preset number of failed attempts even when the device is unable to access network, and thus unable to receive the Remote Wipe command.

In addition, these Security Policies do not have the performance or battery life overhead of solutions that encrypt all data on the device as it is created or moved, and consume very little data traffic even when re-enforced on a regular basis.

The screenshots below show the security settings on Windows Mobile and Apple iPhone that can be user-defined. As soon as the server security policy is enforced, the user can not modify the enforced options.

Windows Mobile

Settings – Personal – Lock



Apple iPhone

Settings – General – Passcode Lock

Local and Remote Device Wipe

When a mobile device is lost or stolen, the potential security risk can be significant. Mobile devices often contain sensitive business data, including personally identifiable information of employees and customers, sensitive e-mail messages, and other items. Exchange ActiveSync helps minimize this risk by providing two levels of device wipe capability.

Wiping the device locally or remotely has the effect of performing a factory or hard reset; all programs, data, and user-specific settings are removed from the device. The device wipe implementation wipes all data, settings, and private key material on the device by overwriting the device memory with a fixed bit pattern, greatly increasing the difficulty of recovering data from a wiped device.

NOTE:

Device wipe in Windows Mobile 6 includes wiping the removable storage card. Time to complete device wipe on Apple iPhone can take up to an hour.

Local Device Wipe

Local device wipes are triggered on a device with device lock enforced if a user incorrectly enters the password more than a specified number of times (the policy default is 8 times, but the administrator can adjust this value). After a few missed attempts, the device displays a confirmation prompt that requires the user to type a confirmation string (usually "a1b2c3") to continue. This prevents the device from being wiped by accidental key presses. Once the password retry limit is reached, the device immediately wipes itself, erasing all local data.

Remote Device Wipe

Remote wipes occur when the administrator issues an explicit wipe command through the Exchange ActiveSync Device Management dialog. Remote wipe operations are separate from local wipes, and a device can be wiped remotely even if Exchange ActiveSync security policies are not in force. The wipe command is pushed as an out-of-band command, so that the device receives it on its next synchronization. The device user cannot opt out of the remote wipe.

E-mail Confirmation

The system sends an acknowledgment message as soon as the device receives the wipe command, alerting the account owner (and the system administrator in Cc) that the wipe occurred (and has been completed successfully).

Devices that do not support security policies do not support Remote Wipe and the ***Remote Wipe*** status in the **ActiveSync Devices** dialog will show ***Unsupported***. The administrator will need to exempt such devices from security policies (on his own decision), and instruct the device user to engage the on-device security features to passcode protect the device and perform Local Wipe after 10 unsuccessful passcode entry attempts.

Defining the Policies

System administrator can define mobile security policies on global, domain, user and device levels and they will be applied to individual users automatically, unless the policy is specifically disabled (or modified) for a particular domain, user or device. No policies are enforced by default.

NOTE that the window title of the ActiveSync Devices dialog tells you for which account or domain the policies apply.

Global Level Policies

GroupWare – ActiveSync – Device Management… – Global Policies…

The global level policies are applied to all domains, users and devices accessing the server, unless configured otherwise on lower level.

Default Policies

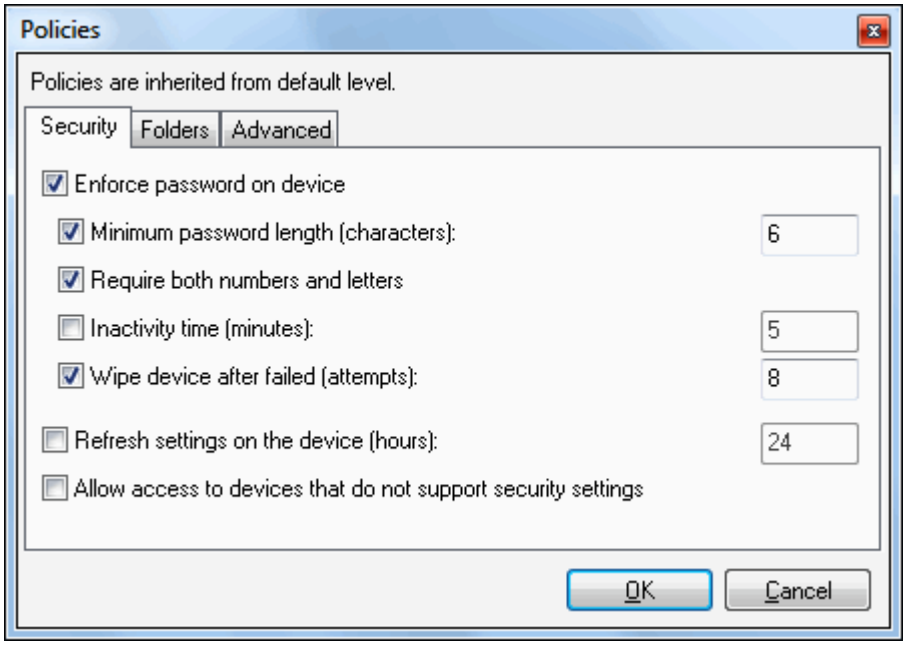
By default, global level policies are not enforced and configured to use so called "neutral provision" – this is a policy which cancels any previously defined policies and reverts the on-device security settings to factory defaults, where they can be freely configured by the user, or turned off completely.

On the picture below, you can see the neutral provision (the default policy) which will be set if you click Inherit on the global level:

- turns off the password requirement*
- sets password length to any length
- allows the user to select alphanumeric or plain numeric password
- allows the user to change the default 5 minute inactivity time
- allows the user to disable Local Wipe and redefine the number of default failed unlock attempts
- this policy will no longer be re-introduced to the device

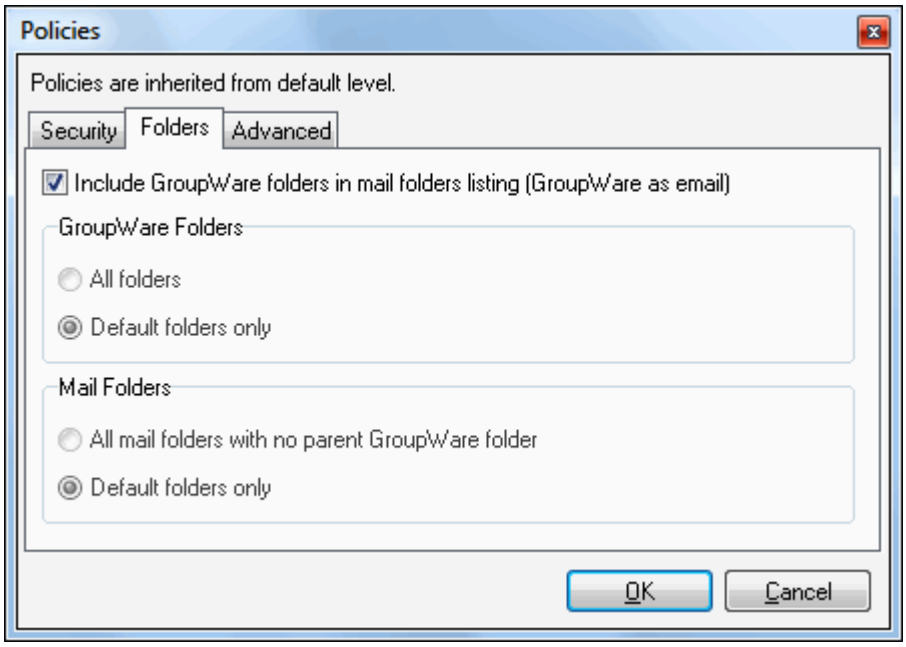
- all devices which support the security policies fully, partially or not at all will be able to synchronize with the server, useful for building device lists and deciding on disallowing the unsupported devices later

**** User is still required to enter the previous passcode until parameters can be changed on the device, including completely disabling the passlock.***

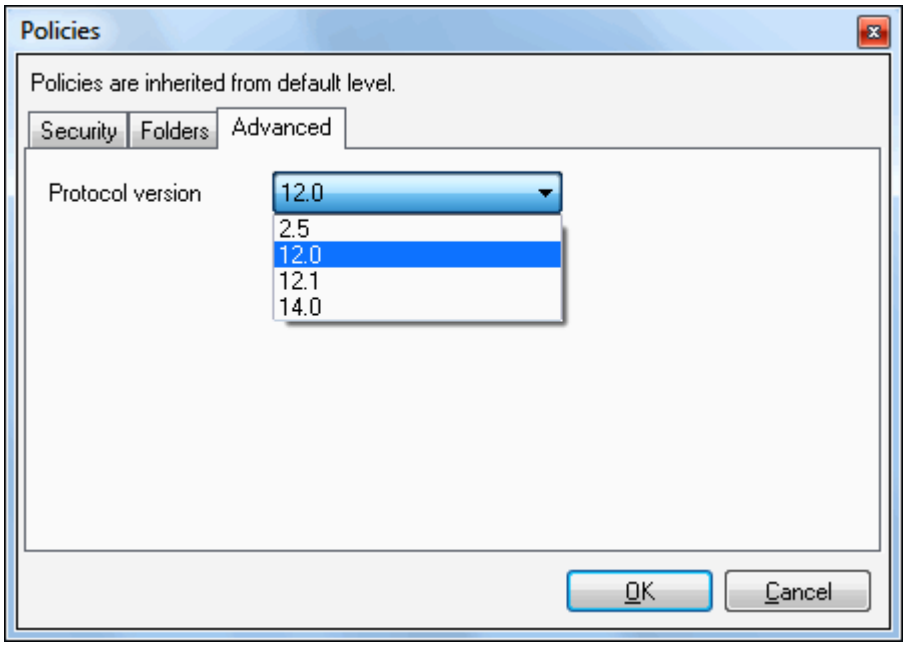


Field	Description
Enforce password on device	Check this box if you want to have possibility to enforce password properties to devices. NOTE: If this box is not ticked, the intended options are disabled. NOTE: Password parameters set here override device settings. NOTE: If this box is ticked, but non of intended options is ticked and defined, password use is enforced, device password parameters are used.
Minimum password length (characters)	Tick this box to enforce password length defined here.
Require both numbers and letters	Tick this box to enforce use of stronger passwords. If the box is not ticked, only numbers are used.
Inactivity time (minutes)	Tick the box if you want to define the time after that an inactive device will lock.
Wipe device after failed attempts	Tick the box if you want to enforce defined number of failed PIN entry attempts before the device wipes itself. If set to zero (0), this feature is disabled.
Refresh settings on the device (hours)	Tick this box if you want to enforce settings refresh interval. This feature is a powerful tool for device security enhancement.

Allow access to devices that do not support security settings	Tick this box if you want to allow devices that do not support provisioning to communicate (and work) with the IceWarp Server EAS module.



Field	Description
Include GW folders in mail folders listing	Not all EAS clients support folder management, groupware folder hierarchy, creation of mail type folders within gw ones and synchronization of some folder types (e. g. notes, files, tasks). Tick this box to have these functions available. NOTE that if this box is ticked, all other features on this tab are disabled.
All folders	Select this option if you want to have these functions available for all GW folders.
Default folders only	Select this option if you want to have these functions available for default GW folders.
All mail folders with no parent GW folder	Select this option if you want to have these functions available for all mail folders except for those that are created (submerged) within GW folders.
Default folders only	Select this option if you want to have these functions available for default mail folders only.



Field	Description
Protocol version	Select the highest supported protocol version. All lower versions are supported too. By default, version 12.0 is set (and recommended). Versions 12.1 and 14.0 are supported too, but not tested for all devices in full scale.

Domain Level Policies

Domains & Accounts – Management – <domain> – Services – ActiveSync Devices… – Domain Policies…

The dialog allows you to configure domain-specific security policies, or exempt some domains from the security provisioning by unchecking the ***Enforce password on device*** option. If you select a particular device from the **Devices** list and click the ***Device Policies*** button instead (or double-click an item), you are opening the security policies configuration dialog on the device level.

User Level Policies

Domains & Accounts – Management – <domain> – <user> – Services – ActiveSync Devices… – User Policies…

The dialog allows you to configure account-specific security policies, or exempt some users from the security provisioning by unchecking the ***Enforce password on device*** option. If you select a particular device from the **Devices** list and click the ***Device Policies*** button instead (or double-click an item), you are opening the security policies configuration dialog on the device level.

Device Level Policies

Device-specific security policies are special, since they can be created only for a device which has already connected to the server before (meaning its ***DeviceID*** is known to differentiate it from other similar devices of the same user).

GroupWare – ActiveSync – Device Management… – <user | device type> – Device Policies…

or

Domains & Accounts – Management – <domain> – Services – ActiveSync Devices… <user | device type> – Device Policies…

or

Domains & Accounts – Management – <domain> – <user> – Services – ActiveSync Devices… <user | device type> – Device Policies…

or

double click an item in the device list on any level.

The dialog allows you to configure device-specific security policies, cancel or exempt some device from policies inherited from an upper level, from the security provisioning by unchecking the ***Enforce password on device*** option. This is particularly useful in case the account is synchronized with several devices, and you wish to relieve just a specific device from the previously applied policies, while any other devices the user is using or will use as a replacement in the future should have the security policies applied.

Policies Inheritance

Lower level provision are meant for fine tuning or customization of higher-level provisions. Policies configured on an upper level are automatically propagated to all lower levels. If they were previously customized, they can be overwritten using the ***Inherit*** button.

When you open a policy configuration dialog for a domain, the options configured on the global level will be already enabled, and similarly for domain-user and user-device levels.

NOTE – the label at the top of the ActiveSync Devices dialog – it reads whether the policies were inherited from default/server/domain/user level, or if they were customized, tells you that you can inherit them from upper level.

You can tell that a policy was inherited from an upper level by opening the policies configuration dialog and observing the ***Inherit*** button – if it is greyed out, it means the policy was not set on this level but inherited from higher or default level. If it's enabled, it means the policy was customized on this level (domain, user or device), and gives you the option to cancel the customization and revert to the policy configured on higher level (global, domain, or user).

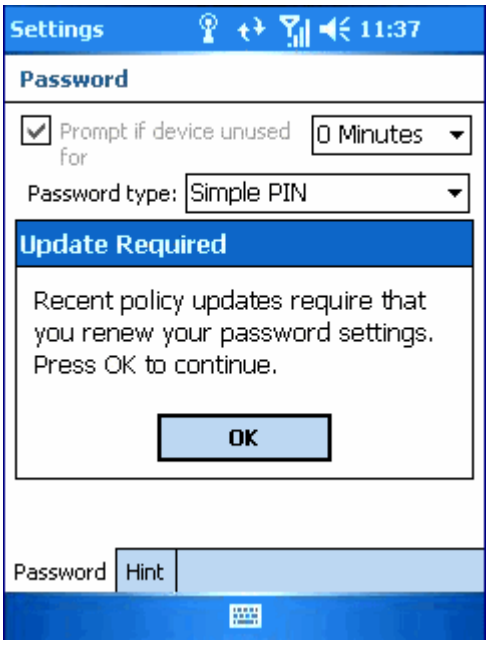
Accepting the Policies

Once the device security policy is defined on the server, it is sent over-the-air to each device upon the next synchronization, including the first synchronization after configuring ActiveSync on the device. On the initial receipt of the policies, the user is asked to accept or decline the policy. If the policy is not accepted, the user will be unable to synchronize with the system and no data will be sent to the device from the server. Once the policies are accepted, the only way to disable them is to do a hard reset on the device, which will also delete any user data including the previously configured ActiveSync account.

Similar dialog is shown when the policies have been changed, requiring the user to change password according to the new policy requirements.

E-mail Confirmation

If the policy is not accepted by the user, or if the security policies are not supported by the device (see the **ActiveSync Devices** dialog, the ***Remote Wipe*** column would read ***Unsupported***) and administrator does not allow non-conforming devices, the user (and server administrator in Cc) will receive an e-mail informing that the device could not connect to the server.



Exempting Non-Provisionable Devices

Another feature allows the administrator to specify that users with older devices without security policy capacity may still connect to the system. This enables administrators to allow connections from older devices (Windows Mobile 5.0 without Feature Pack, Palm devices) until those devices can be replaced, while still providing policy controls for devices that fully implement Exchange ActiveSync, and automatically enforce them as soon as the older devices are replaced with fully compatible models.

To exempt a device, open the **Device Policies** dialog (or double-click the device in the device list) and tick the ***Allow access to devices that do not fully support password settings*** check box. *

Exempting Trusted Users

Administrator can also exempt individual domains or users from policies defined on global or domain level, respectively, by creating an individual policy configuration on the corresponding level. For example you can specifically disable the security policies for individual users who you want to exempt from the settings you have configured on a global/domain level. These exceptions are useful if you have specific, trusted users who do not require device security settings. However, when using this feature bear in mind that executives or other key employees who might request exemptions most likely have highly valuable data on their devices and should not necessarily be exempted from security policies.

To exempt a user, open the **ActiveSync Devices** dialog in that user's **Service** tab, click ***User Policies*** and tick the ***Allow access to devices that do not fully support password settings*** check box. *

***** It may be useful to leave the ***Refresh settings on device*** option enabled, so that the provisioning is regularly retried: in case the device firmware or ActiveSync client version was upgraded with the support for security policies, the password policy would be automatically applied. In other cases it may be turned off.

Cancelling the Security Policy

To cancel the security policy on a particular device, navigate to the device level security configuration dialog, uncheck the ***Enforce device password*** option, click ***OK*** and click ***Apply***. The 'neutralization provision', as described in the **Defining the Policies** section, will be sent to the device, cancelling the previously configured policies. The existing security policy will be overwritten with the default factory settings as soon as the next synchronization occurs (immediately if Push is turned on).

NOTE that this does not automatically cancel the passcode lock. User first needs to enter the existing password before he/she is able to modify the security settings or disable the passcode requirement.

NOTE that when you uncheck the ***Enforce device password*** option, the neutralization provision is sent to the device in order to cancel any existing security policies, but the previous configuration will be preserved in the security configuration dialog (in the form of greyed-out options) for this device until the device is removed using the ***Delete Device*** option. This behavior allows administrators to review their decisions and quickly re-enforce exactly the same security policy in case they cancel it by mistake.

Reference

The system or domain administrator can use security provisioning in Exchange ActiveSync version 2.5 to engage a passlock on the device, to set password length and strength, and to control the inactivity period and number of failed password attempts before a device is wiped.

NOTE that in this chapter, the term password refers to the passcode or PIN a user enters to unlock his or her mobile device (sometimes called passlock). It is not the same as a user account password or a SIM PIN.

Field	Description
Policies are inherited from default/server/domain/user level	This label informs that policies were not customized on this level and tells from which level they were inherited: ▪ default ▪ server ▪ domain ▪ user If policies were customized on this level and not inherited automatically, the label reads: ***In order to inherit policies from a higher level, click "Inherit" button bellow***. NOTE that inheritance concept is as follows: Once inheritance is set for the appropriate level (e.g. for a user), policies from the immediately higher level (the domain one here) are used.

	If inheritance is set also for this level (domain, that inherits from the server level), the first level (user here) also inherits from this (server) level. This applies for all levels except for the default one. Inheritance is removed in the moment of setting of different policies for the appropriate level.
Enforce password on device	By default, mobile devices do not require users to use password to unlock them when turned on. By checking ***Enforce password on device***, the password will be required after the device is powered on, or after certain inactivity period. At the same time, the rest of the options become available, that you can use to specify the type of password that must be used on the mobile device and other related settings. By unchecking ***Enforce password on device***, the security policy will be cancelled and any devices, to which this policy level applies, will allow to use user-defined security options (including disabling the password requirement altogether).
Minimum password length (characters)	If checked, specifies that the length of the password will be controlled by server settings and allows to specify the required length for the user's device password. The default is 4 characters. Acceptable range is 2 to 18 characters. If the number you enter is out of the range, it will be automatically updated to 2 or 18 as soon as you click elsewhere, press the ***Tab*** key or leave the dialog by clicking ***OK***. If unchecked, specifies that the length of the password will be user-defined.
Require both numbers and letters	If checked, specifies that the password complexity level will be controlled by server settings, and requires that password must contain both numbers and letters (strong alphanumeric password). For example, checking ***Require both numbers and letters*** and setting ***Minimum password length*** to 8 will require a Windows Mobile user to create a password made of 5 or more letters and at least 3 punctuation, upper case or numbers. It will not allow to change the ***Password Type*** to PIN, the only option available will be ***Strong password***. An iPhone user will be asked to create a password with 8 or more letters combined with some numbers and one of special characters: &#@. If unchecked, specifies that the user can select the password complexity by deciding to use alphanumeric or numeric passwords, with the exception of simple patterns (1234, 1111) which are always blocked by the device itself. If the Minimum password length option is also checked, the user can use numeric or alphanumeric password, with respect to the minimum allowed length.
Inactivity time (minutes)	If checked, specifies that the inactivity settings will be applied and controlled by server settings, and specifies how many minutes of inactivity are allowed before the device locks, requiring the user to log on again using the device password. If selected, you can specify the amount of time without user input after which the user must reenter their password. Enter the time of inactivity (including stand-by) before the password must be re-entered. This setting is independent on power-saver settings, i.e. if the device goes to standby after 2 minutes, and the inactivity time is set to 5, activating the device within 3 minutes after it goes to standby will not require the user to re-enter the password. Acceptable range allowed by server is 0-9999 minutes. If you enter a greater number it will be saved as 9999. Default is 5 minutes. 0 means to require password immediately when activated from stand-by. If no power-saver is activated and the device never goes to standby, 0 means that password is required only when powering on the device. If unchecked, specifies that the inactivity time will be user-defined.

Wipe device after failed (attempts)	If checked, specifies that the local wipe settings will be applied and controlled by server settings, and specifies after how many successive failed logon attempts the device memory will be wiped. NOTE that after a half of the available attempts are about to be missed, the device prompts user for a confirmation string (usually ***a1b2c3*** string instead of the password) to continue. This prevents unintentionally wiping the device memory by accidentally pressing some buttons on the device when asked for the password (when a keyboard lock is inactive). Enter the number of permitted failed logon attempts. Acceptable range allowed by the server is 0-99. If you enter a greater number, it will be saved as 99. Default is 8 attempts. 0 means that local wipe is disabled on the device and user is not allowed to enable it. If unchecked, local wipe settings are user-defined. On some devices, the user can set the number of failed logon attempts, others do not have any such user setting and use a default of 8 to 10.
Refresh settings on the device (hours)	Specifies the time interval for the security policies to be pushed to the device. This is useful in case of advanced users who can work around the device operating system and disable some or all of the server provisioned security policies. If they succeed, the policy will be refreshed after the time interval specified by this setting, overwriting any previous modifications. If checked, the security policies will be refreshed on given schedule. Specify how many hours can pass before a device will be resent the Security Policies. Acceptable range allowed by server is 1-9999. If you enter an out-of-range number, it will be saved as 1 or 9999. Default is every 24 hours. If unchecked, the security policies will be only applied once; to the first synchronization (after the ActiveSync account is configured on the device) or to the next synchronization (if the device has already synchronized with the server before).
Allow access to devices that do not support security settings	Allows devices that do not fully support the Security Policies (non-MSFP devices, sometimes referred to as legacy hardware) to synchronize with IceWarp Server. If checked, it specifies that any devices will be allowed to synchronize with IceWarp Server. This is the default setting. If unchecked, the incapable devices will receive the ***449 Needs provisioning*** error message when they attempt to synchronize with the server, thus will be unable to receive any data from the server. The user (and server administrator in Cc) will receive an e-mail informing that the device could not connect to the server if not conforming with the policies (either by not supporting them, or by the user not having agreed when prompted).
Inherit	Click the button if you want to inherit security policies from a higher level. For details, see the ***Policies are inherited ...*** field description in this table.
OK	After you click ***OK***, the configuration will be saved but the Security Policy not applied until the ***Apply*** button is pressed. If the Security Policies are the same as before, the ***Apply*** button will not be available. Also in other cases when the ***Apply*** button was available, the mechanism is smart enough to recognize that a device would be provisioned with the same security policies as previously enforced, and no provisions are sent until the time specified for refreshing the Security Policies on schedule.

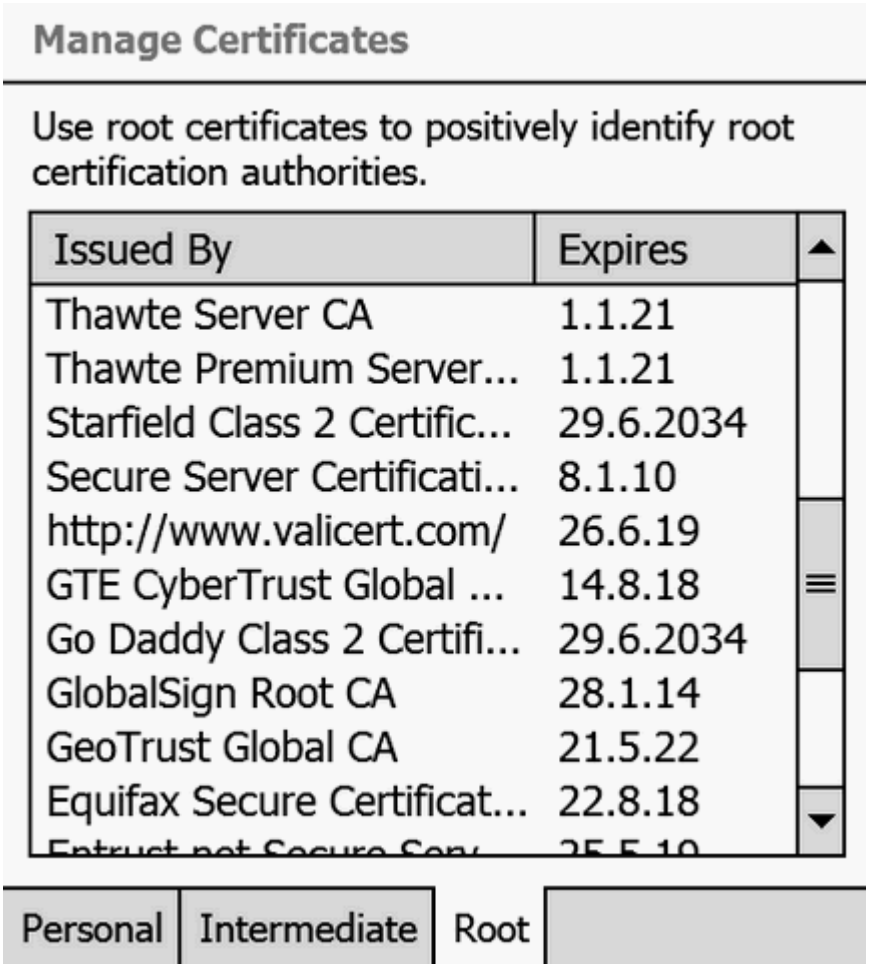
Cancel	Click ***Cancel*** to leave the dialog without saving any changes.

SSL and Windows Mobile Devices

SSL Requirements

DirectPush and AutoDiscover features on Windows Mobile devices work properly only if SSL is enabled when configuring the ActiveSync account. Additionally, the SSL certificate provided by the server needs to be already trusted by the device – user will not be asked to trust the certificate, it will be rejected and the SSL connection won't be established. An SSL connection can be achieved by any of these options:

1. ***(Recommended.)*** Obtain a **trusted certificate** (issued by a third party Certification Authority) which is already trusted by your mobile devices (see Windows Mobile Trusted Certificates below or check ***Settings – System – Certificates – Root*** on the device). Install this certificate onto your server. For details, see the **Getting a Digital Certificate** chapter in System Node Reference, or refer to the **System - Certificates** section in Administration GUI and press F1 for help.



2. ***(Not recommended.)*** Obtain a third party certificate for your server which is already trusted by your mobile devices which is signed by an intermediate store, which means you will have to still install the **intermediary certificate** on mobile devices.
3. ***(Special/testing purposes only.)*** Use your own **self-signed certificate**, but import the root certificate into the root certificate store on all your mobile devices.

Windows Mobile 5.0 and Windows Mobile 6.x

If you choose option 1, you don't have to do anything on the device. If you choose option 2 or 3 from the previous list and want to install an intermediary-signed or self-signed certificate to the device, follow these steps.

1. Export the root certificate using SSL utilities into DER encoded binary X.509 format with a **.cer** file name extension.
2. Copy the exported root/intermediary certificate file to either the **\Storage** directory on the device or on the root folder of a storage card using a cable connection via desktop ActiveSync application (**Tools – Explore**).
3. Or email the certificate file to yourself through an IMAP/POP account that you setup prior to an ActiveSync account configuration, then download it from Mailbox.
4. Finally locate the file on the device using File Explorer, double-click the file and confirm that you wish to import this certificate into the device.
5. To verify that the certificate was installed correctly, press ***Start***, select ***Settings***, and then select the **System** tab – ***Certificates***; the certificate should appear on either the Intermediary tab or the **Root** tab.

NOTE that whether a root certificate can be installed on the device depends on how the device was configured by the original equipment manufacturer (OEM) or by the mobile operator.

PocketPC/Smartphone 2002 and 2003

There is no support for DirectPush or AutoDiscover on this platform, but you will want to use SSL connections anyway. PocketPC 2002, PocketPC 2003 powered devices connect over Secure Sockets Layer (SSL) only. Windows Mobile 2003 powered devices do not require SSL. However, it is strongly recommended that you use SSL to protect your data and credentials, which are otherwise transmitted in plain text as the only other possibility allowed by the EAS protocol architecture.

This platform is using Microsoft Crypto API (CAPI) certificate store to securely store root certificates and may require a special utility from Microsoft to import the certificate.

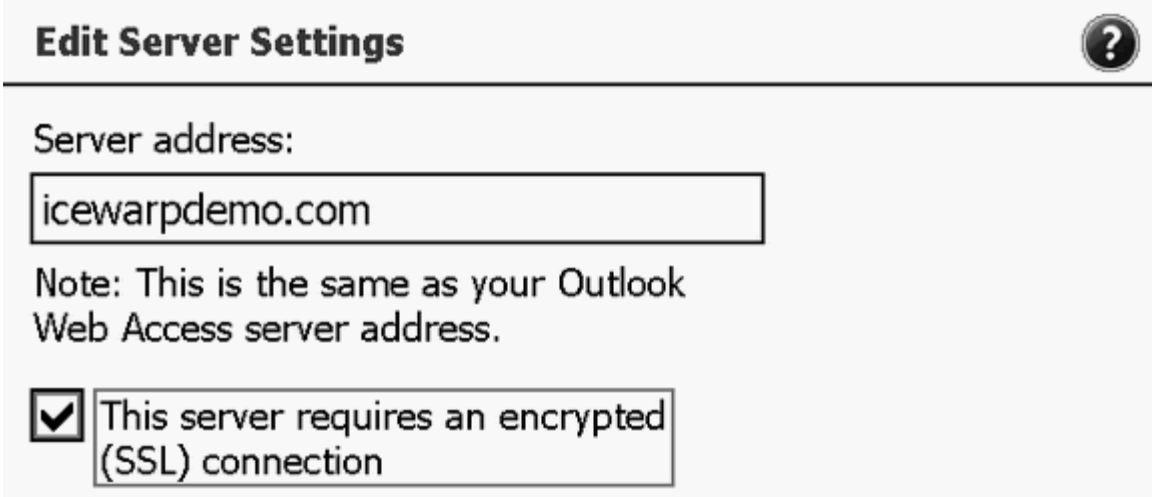
More details and the utility download link can be found in this Microsoft article:

http://support.microsoft.com/?id=841060

NOTE that the mobile carrier who has supplied the device might have restricted the device not to accept certificates into the root store. Also the device must use the Unrestricted Application Security Policy for the unsigned utility to run.

Enabling SSL for ActiveSync

To enable SSL authentication on Windows Mobile 2003/5.0/6.0/6.1 powered devices (and therefore enable DirectPush and AutoDiscover), in the ActiveSync Server Synchronization settings, select the ***This server requires an encrypted (SSL) connection*** option.



Windows Mobile Trusted Certificates

To simplify deployment and enable trusted and secure access to all other IceWarp Server's services, we strongly recommend to install a certificate on your server that is issued by an authority that the devices already trust. Alternatively, you can install a certificate that is issued by a company that is chained to an authority that the device trusts. Known third-party Secure Sockets Layer (SSL) certificates are issued by trusted root certification authorities that have a root store presence in Windows Mobile-based devices.

If you are deploying a mixture of devices, select the certification authority that is present in the oldest Windows Mobile operating system version you have.

The root certificates that are included with the **PocketPC 2002**-based devices represent the following certificate authorities:

- VeriSign
- Cybertrust
- Thawte
- Entrust

The root certificates that are included with the **PocketPC 2003**-based devices represent the following certificate authorities:

- VeriSign
- Cybertrust
- Thawte
- Entrust
- GlobalSign

- Equifax

The root certificates that are included with the **Windows Mobile 5.0**-based devices represent the following certificate authorities:

- Class 2 Public Primary Certification Authority (VeriSign, Inc.)
- Class 3 Public Primary Certification Authority (VeriSign, Inc.)
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- Equifax Secure Certification Authority
- GlobalSign Root CA
- GTE CyberTrust Global Root
- GTE CyberTrust Root
- Secure Server Certification Authority (RSA)
- Thawte Premium Server CA
- Thawte Server CA

Windows Mobile 5.0 with AKU2(MSFP) has the following additional root certificate installed:

- Godaddy http://www.valicert.com/

The root certificates that are included with the **Windows Mobile 6.X**-based devices represent the following certificate authorities:

- Comodo AAA Certificate Services
- Comodo AddTrust External CA Root
- Cybertrust Baltimore CyberTrust Root
- Cybertrust GlobalSign Root CA
- Cybertrust GTE CyberTrust Global Root
- Verisign Class 2 Public Primary Certification Authority
- Verisign Thawte Premium Server CA
- Verisign Thawte Server CA
- Verisign Secure Server Certification Authority
- Verisign Class 3 Public Primary Certification Authority
- Entrust Entrust.net Certification Authority (2048)
- Entrust Entrust.net Secure Server Certification Authority
- Geotrust Equifax Secure Certificate Authority
- Geotrust GeoTrust Global CA
- Godaddy Go Daddy Class 2 Certification Authority
- Godaddy http://www.valicert.com/
- Godaddy Starfield Class 2 Certification Authority

Technical Details

Please refer to this Microsoft Technet article for more details on Windows Mobile certificates:

http://technet.microsoft.com/en-us/library/cc182301.aspx

Device Configuration

WARNING – the first synchronization will delete all current contacts and calendar data from your device and replace them with the data in your server account. This is the intended behaviour when a new device is assigned to an employee and avoids item duplication.

Backup Existing Data

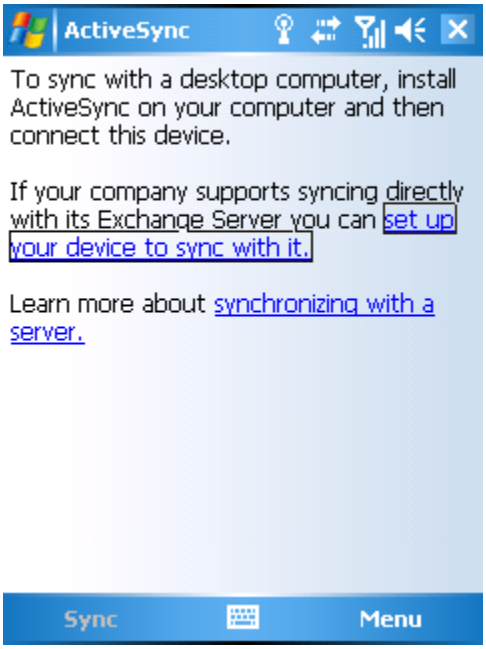
However in real world, valuable data often exist on the device before wireless synchronization is enabled. Some devices have the option to merge existing data with server account (***two-way sync***) while other do not; you need to use another synchronization method to keep any existing data.

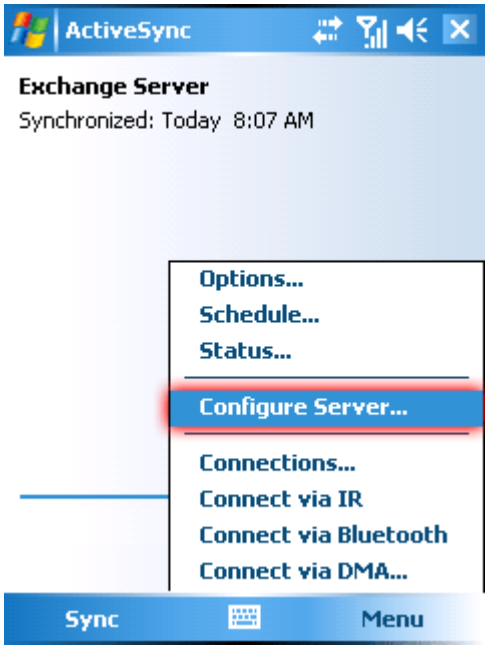
- For testing, create a backup of your device data using desktop tethering and application supplied with your mobile device (ActiveSync, iSync, Nokia PC Suite…). You can then restore the data on the device and synchronize them back to your account.
- For production, you can either move your contacts to a SIM card first, and after ActiveSync setup, copy them back to your address book, or use a SyncML client prior to ActiveSync setup to synchronize all contacts and calendar data to your server (***two-way sync*** or ***one-way sync*** to a server) first. The same data will then be available after the first synchronization on the device and within your server account.

Configuration

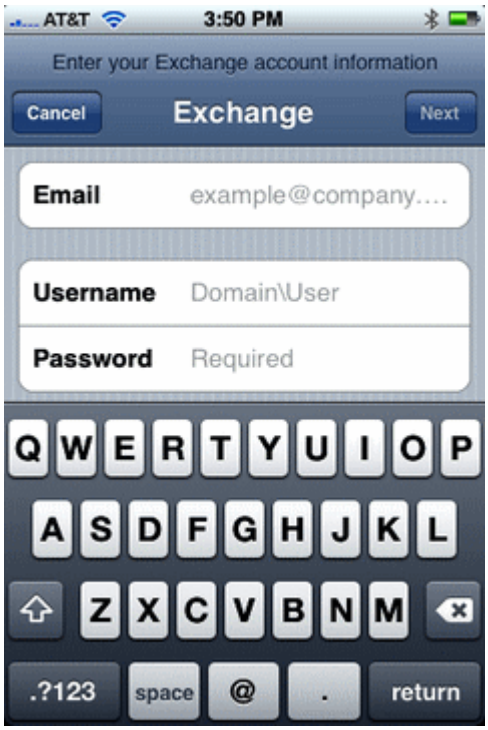
1. Locate ActiveSync settings on the device. Usually when you create a new account, a wizard will walk you through the setup process. If there are any existing ActiveSync accounts, you need to remove them first.

   • **Windows Mobile** – Start – Programs – ActiveSync – Menu – Add Server Source



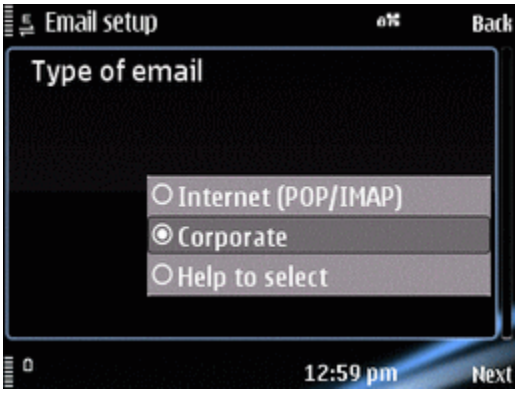


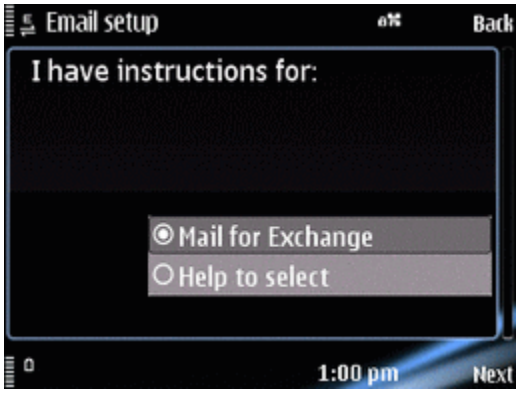
• **iPhone** – Settings – Mail, Contacts, Calendars – New Account – Exchange



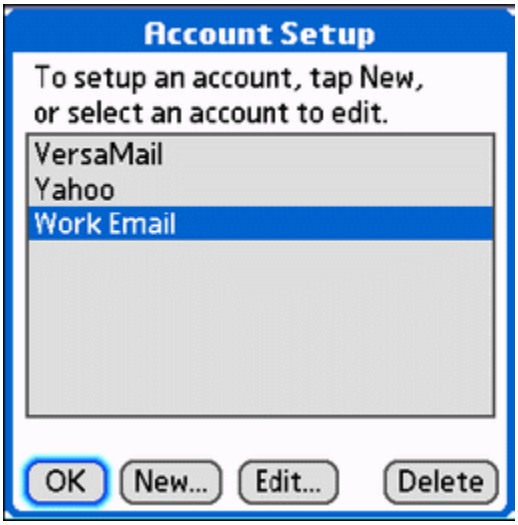
• **Nokia (Symbian S 60)** – Menu – Messaging – Options – Settings – Email – Options – New Mailbox (select Mail for Exch. in account wizard)

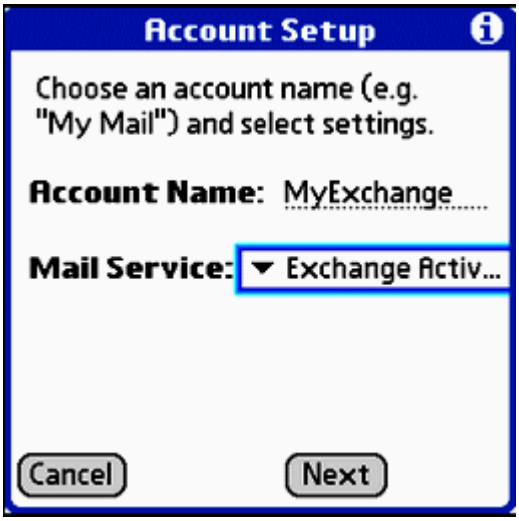
You can run the Email setup wizard directly from the home screen by selecting ***Set up e-mail*** in active menu.



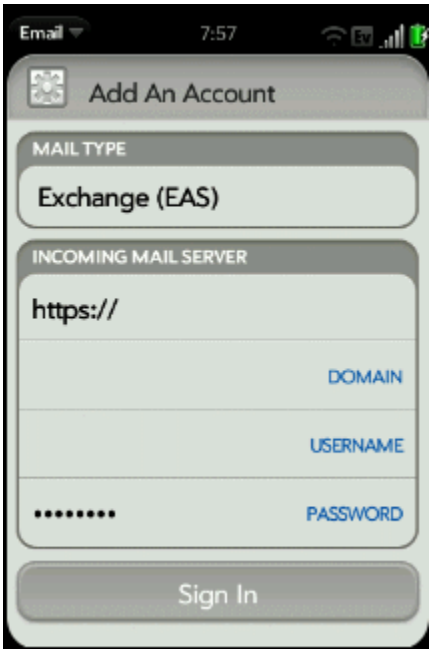


• **Palm OS** – Menu – Email – Accounts – Account Setup… – New – Mail Type: Outlook (EAS)



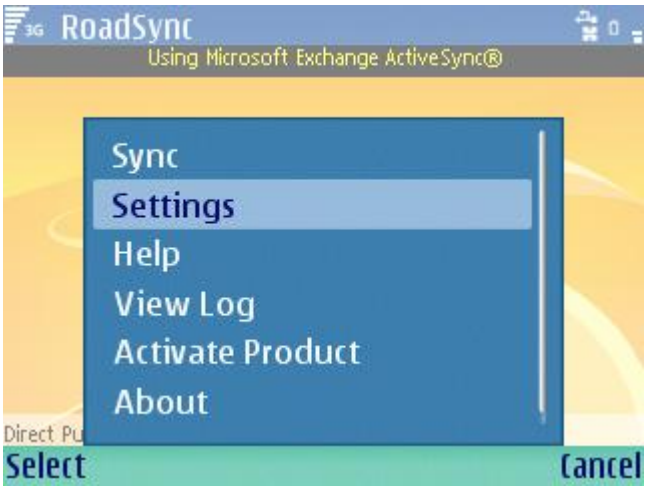


• **Palm Pre** - Quick Launch dock - Email - (Preferences & Accounts - Add an account if adding another email account) - enter email address and password - change Mail Type option to Exchange (EAS).



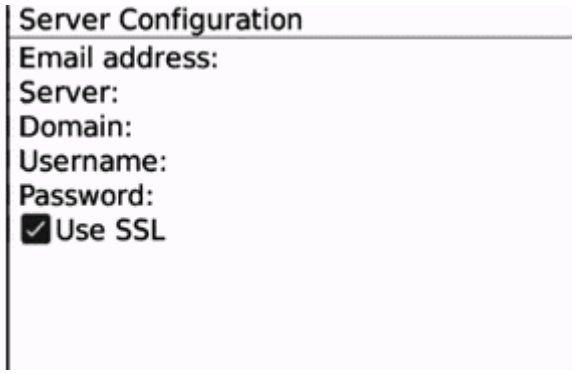
• **Symbian UIQ** – Menu – Applications – RoadSync – Options – Settings

When you install the client application on the device, a wizard will walk you through the setup process. For details see the accompanying literature to these products.



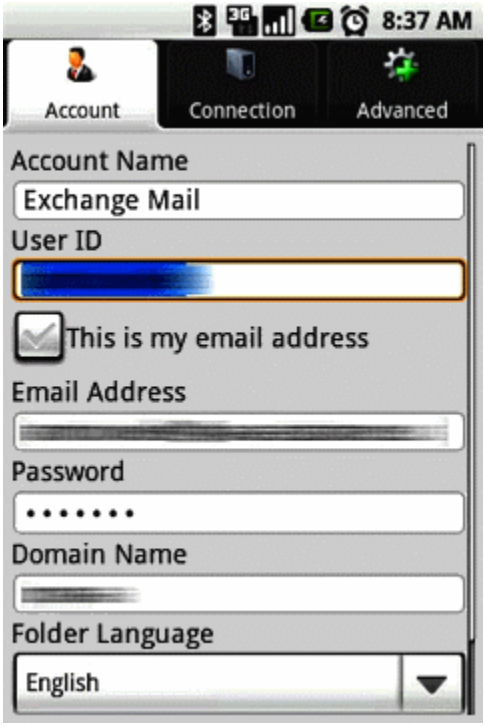
• **Blackberry** – Applications – Astrasync/NotifySync – Options

When you install the client application on the device, a wizard will walk you through the setup process. For details see the accompanying literature to these products.



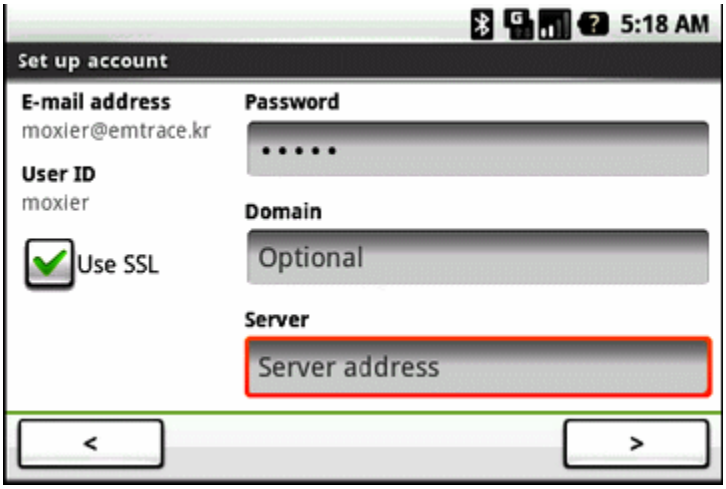
• **Android (TouchDown)** – Menu – Applications – Touchdown – Settings – Account

When you install the client application on the device, a wizard will walk you through the setup process. For details see the accompanying literature to these products.



• **Android (Moxier Mail)** - Menu - Applications - Moxier Sync - Account

When you install the client application on the device, a wizard will walk you through the setup process. For details see the accompanying literature to these products.



2. For devices with **AutoDiscover,** you will need to enter only username (this is your email address) and password, the server name and domain name will be located according to the email address domain part if it matches a part of the server hostname, or using an ***MX DNS lookup*** if it does not.

   Description/Account ID: <description>

   Any descriptive account name.

   Username: <user@usersdomain>

   Full email address of the user.

   Password: <Password>

   User's password.

   You may be asked to accept an untrusted SSL certificate if it's not already installed on the device, or if your server is using a self-issued rather than CA Certificate for HTTPS.

3. For devices without AutoDiscover support, you will need to provide additional information:

   Server name: <hostname> e.g.: ***mx99.icewarpdemo.com***

   Domain: <usersdomain> e.g.: ***icewarpdemo.com***

   NOTE – Do **NOT** use ***http://*** or ***https://*** protocol prefix with the hostname. Do not enter anything else after the hostname, not even a forward slash.

   You can safely leave the domain blank, this field is ignored. Users are identified solely by their full e-mail address.

4. Finally, there should be options to enable Email, Contacts, Events and Tasks synchronization.

5. Advanced settings may include option to enable Push or if a synchronization should occur on a defined schedule, set date range of items to synchronize, select folders to synchronize with built-in applications, set custom notifications and other settings mostly specific to a device platform or application version.

6. Passwords are transmitted in plain text as a limitation of the EAS protocol.

   We strongly recommend to turn on the SSL option to encrypt all communication.

NOTE – as a best practice, email look-back range should be set to a limited number of days. This means considerable savings in data transfers and power consumption should an error occur and the device would have to synchronize all data from scratch (***full synchronization*** or ***initial synchronization*** when account is deleted and added back).

Troubleshooting

To resolve possible problems with Exchange ActiveSync, go through the following steps:

1. Have you upgraded from version 9 or older by other means than by in-place upgrade? Have you restored settings of version 9 or older on your version 10 server?

   The settings backup is not backward compatible and your ***webservice.dat*** settings will be corrupted. Read on for the correct configuration, but you may not be able to make it work and other services are likely to fail as well.

   As many as 40 upgrade scripts are executed through the upgrade to version 10, most prominently GroupWare database transformation takes place, thus skipping this part of installation is strongly discouraged and advanced services including Exchange ActiveSync are poised to fail. Please follow the correct upgrade procedure first.

2. Make sure the steps in the **On-server Setup** section have been followed.
3. Make sure the **Device Configuration** steps have been properly followed.
4. Note any error message displayed by the wireless device when synchronization is attempted.

   * ***Authentication failed***. Double-check the user credentials configured on the device. ***The username is always a full email address***.

   * ***Connection to the server failed***. Network error. Check your wireless connection. Some devices come pre-configured to use a WAP access point to connect to Internet. This will not work for ActiveSync over HTTP protocol – you need to subscribe to a data plan and configure GPRS/3G access point such as internet.t-mobile.com.

   Check the hostname in ActiveSync settings. Check that you can connect to WebClient from within the browser on your device (adding ***/webmail/pda*** to the hostname). Check if you have the web server running on a standard port number (use 80 or 443 for secure connection). Check if you have any ***Rewrite*** rules configured in **Web Service** settings. Check that default document includes **index.php**.

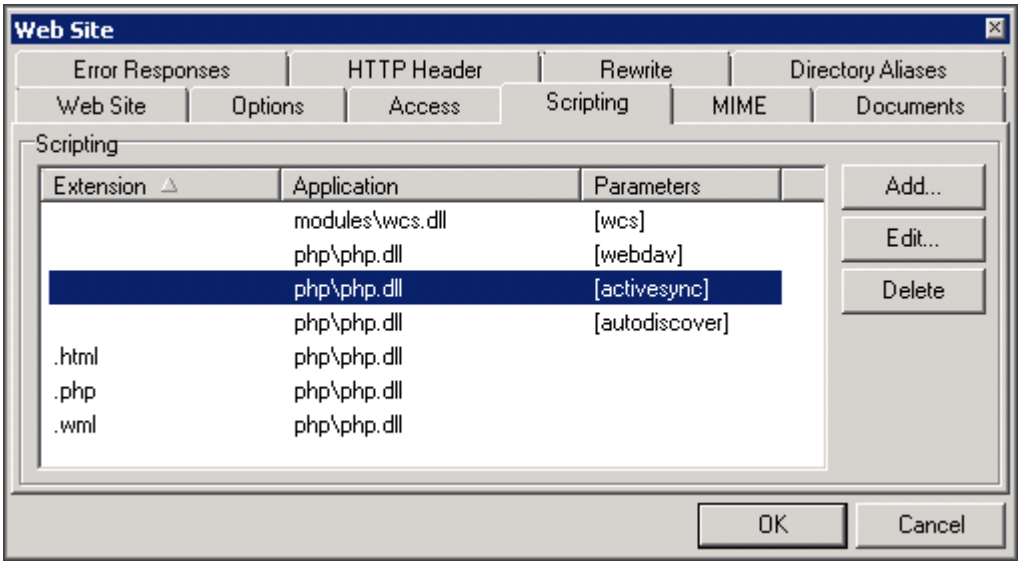
   Normally after providing the authentication details (email address and password), the client configuration should proceed with ***SSL certificate warning*** in case of untrusted (self-signed) certificate, as the device is connecting to AutoDiscover service first. If the service is not found, the same dialog would come up later in the second round after your enter the server hostname. If it does not, most probably the problem is not in ActiveSync, but rather in web server settings of your server, or network configuration.

   To check whether the connection to IceWarp web service is working, point your browser on a computer located within the same LAN as the device to:

   https://hostname/Microsoft-Server-ActiveSync/

   A dialog window should come up asking for username and password. If it does not, the web service is misconfigured, the Scripting settings for ActiveSync are missing for the (***Default***) web service host, a firewall is blocking the connection or there's some other network error.You can confirm this by checking the web server log and PHP error logs for some related entries – in this case, there would be no track of the ActiveSync connection.

   Verify the settings in **Web Service – Default** (or other site you have configured) – **Scripting**. It should look like on the picture below. The corresponding entries can be found in **[Installation root]\config\webserver.dat**.



NOTE that there should be ActiveSync related entries under the <EXTENSIONS> group as well as under the <SPECIAL> group.

```
<EXTENSIONS>
  <ITEM>
    <EXIT/>
    <MODULE>php\php.dll</MODULE>
    <TITLE>[activesync]</TITLE>
  </ITEM>
</EXTENSIONS>
<SPECIAL>
  <ITEM>
    <TITLE>/Microsoft-Server-ActiveSync</TITLE>
    <MODULE>[activesync]</MODULE>
    <SCRIPT>activesync\index.html<SCRIPT>
  </ITEM>
</SPECIAL>
```

* ***Other error message***. See the error detail displayed on screen or in help. Perform a hard-reset of your device. Turn Off and back On the synchronization of the affected item(s). Delete the synchronization profile (the user's **ActiveSync Account** on the device) and configure it from scratch. Use the **ActiveSync – Device Management – Delete Device** option to reset the device and cause it to full synchronize. Upgrade your device to the latest firmware version or obtain the latest version of the synchronization application. Refer to user's manual, support pages or contact the device/application vendor's helpdesk.

For Windows Mobile devices, there is a useful listing of all numeric error codes available on the web. The textual descriptions may be useful for troubleshooting with other devices implementing Exchange ActiveSync. Note that most entries are specific to Microsoft Exchange and some resolutions won't be directly applicable.

http://www.pocketpcfaq.com/faqs/activesync/exchange_errors.php

* ***No errors were produced but no items have been synchronized from the server***. Review all reason listed above. If none applies, it indicates an incorrectly migrated GroupWare database. This may happen after upgrade from an older version of IceWarp Server, causing localized folder names to be incorrectly translated to UTF. To verify this is your case, try the synchronization with a newly created account. If it works, you need to fix records in your GroupWare database. First of all, make a proper backup for roll-back in case of any problem. Then in the **Administration GUI – System – Tools – Database Migration**, select the destination DB and tick the ***Repair UTF-8 character set*** check box. Click ***Start Migration***. When done, go to the **GroupWare - General** tab, and in **Database Settings**, select the database you have just created. Apply the settings and restart GroupWare service. In case the issue persists, contact our support engineers.

5. Enable the ActiveSync logging (**System – Logging – Services**). Then check ActiveSync log for activity related to the affected account.

6. If there are no entries in ActiveSync log, the service has failed to initialize. This can be due to mis-configured PHP processor. See the PHP Error log for unusual entries. Re-install IceWarp Server to recover a corrupt PHP installation. Re-install IceWarp Server to recover a corrupt ActiveSync installation.

7. If there are some errors in ActiveSync log that you are unable to decipher and the problem still persists (having attempted all the resolutions above), copy the relevant part of the log along with some entries before and after the error to a plain text file and email it with a brief issue description and device model to our Product Support Helpdesk.

8. Push works sometimes, gets stuck, stops after period of time, stops randomly. Check if there are no schedule settings causing Push to stop. When using WiFi only, in network connection settings (e.g. ***Connections – WiFi Settings – Power Mode***) make sure there are no settings enabled that would prevent WiFi from working while the screen is off or the device in standby/sleep/locked. On device, disable any 'force'-like settings related to Hearbeat interval, or set it to a lower value (maximum supported by the server is 30 minutes, see chapter Changing the server Heartbeat interval). Heartbeat interval means how much time that the device calculates should pass between pings to the server. See ActiveSync logs after how much time the device disconnects, and if it reconnects afterwards or not. In some cases, a mis-configured WiFi access point may prevent the device from reconnecting – try on a different network, or turn off WiFi to test if this is specific to WiFi connection only or Wifi mixed with 2G/3G.

   Verify power saving settings on the device. Some models (such as new Nokia E-series) turn off data connectivity automatically to conserve the remaining power when on low battery. Blackberry's turn off the radio completely on low battery. It can take the full heartbeat interval for the device to reconnect after its charged, and only the first and the following events after the reconnect will be notified. In such cases the user should be instructed to use ***Synchronize Now*** option to re-establish the connection after the charge.

9. Push does not work. Push capability may not be available (PocketPC, Windows Mobile 5.0). See the **ActiveSync Compatibility Matrix** (see "Exchange ActiveSync Guide" on page 1). All Windows Mobile devices and some Nokia handsets require SSL to be enabled for push to work. See the **SSL and Windows Mobile Devices** (on page 23) chapter. The SSL certificate used by the server may be expired.

   On device, make sure Push is turned on (for Windows Mobile, go to **ActiveSync - Menu - Schedule - Peak times/Off-peak times** and select ***As Items Arrive***, for iPhone go to **Settings - Mail, Contacts, Calendars - Fetch New Data** and turn ***Push*** on, other devices will have similar options in advanced settings). Windows Mobile devices are not capable of Push if Wi-Fi is the only connection available, in spite you configure them for Push, they will poll the server each 30 minutes for changes until you activate a cellular data connection (GPRS, EDGE or 3G). Note that most devices are set to turn off data connections while abroad (roaming) – make sure it is not the case. Some clients also allow you to set a schedule for Push (e.g. each workday 8AM to 5PM) – make sure you are within the schedule or disable this option. On IceWarp Server, check that **GroupWare – General – Push Server** is active. Enable the logging in **System – Logging – Services – GroupWare Push**. If it is blank for a long time while there is conclusive email and groupware activity on the server, restart the **Control** service. Try changing the UDP port where the **Notification** service is running. You should see events in the log corresponding to account activity. Observe the ActiveSync log to see if the device initiates a sync upon some activity.

   Remember: no ping, no push. The device must first send the ping command in order to receive push responses. Look for the ***<<< Ping*** entries linked with the affected user account/device according to the DeviceID (the first string of the log entry).

A healthy log entries upon receiving an alert from the server about new data to push should look like this:

```
5715efb8b0cd303a3d2c8262625559ef [0000] 14:18:47 <<< Ping
<Ping xmlns="Ping:">
  <Folders>
    <Folder>
      <Id>029dd8578cdd59125628c9c33327a11d</Id>
      <Class>Contacts</Class>
    </Folder>
    <Folder>
      <Id>ffc4c02e222b3350bda0d55b98b038b9</Id>
      <Class>Calendar</Class>
    </Folder>
    <Folder>
      <Id>af1cd994dfcb9286c394d142687ff5a0</Id>
      <Class>Email</Class>
    </Folder>
  </Folders>
</Ping>

5715efb8b0cd303a3d2c8262625559ef [0000] 14:21:23 >>> 200 OK
<Ping xmlns="Ping:">
  <Status>2</Status>
  <Folders>
    <Folder>af1cd994dfcb9286c394d142687ff5a0</Folder>
  </Folders>
</Ping>

5715efb8b0cd303a3d2c8262625559ef [0000] 14:21:28 <<< Sync
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Email</Class>
      <SyncKey>335</SyncKey>
      <CollectionId>af1cd994dfcb9286c394d142687ff5a0</CollectionId>
      <DeletesAsMoves></DeletesAsMoves>
      <GetChanges></GetChanges>
      <WindowSize>50</WindowSize>
      <Options>
        <FilterType>2</FilterType>
        <Truncation>1</Truncation>
        <MIMETruncation>1</MIMETruncation>
        <MIMESupport>0</MIMESupport>
      </Options>
    </Collection>
  </Collections>
</Sync>

5715efb8b0cd303a3d2c8262625559ef [0000] 14:21:28 >>> 200 OK
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Email</Class>
      <SyncKey>336</SyncKey>
      <CollectionId>af1cd994dfcb9286c394d142687ff5a0</CollectionId>
      <Status>1</Status>
      <Commands>
        <Add>
          <ServerId>68503</ServerId>
          <ApplicationData>
            <DateReceived xmlns="Email:">2009-04-20T12:53:40.000Z</DateReceived>
            <DisplayTo xmlns="Email:">"John Doe" <john.doe@icewarp.com></DisplayTo>
            <From xmlns="Email:">"Jon Lord" <jon.lord@icewarp.com></From>
            <Importance xmlns="Email:">3</Importance>
            <MessageClass xmlns="Email:">IPM.Note</MessageClass>
            <Read xmlns="Email:">0</Read>
            <Subject xmlns="Email:">Re[2]: EAS s novym Push pro iP na icewarp.com</Subject>
            <To xmlns="Email:">"John Doe" <john.doe@icewarp.com></To>
            <Body xmlns="Email:">Hello, this is just a test email.</Body>
            <BodySize xmlns="Email:">33</BodySize>
            <BodyTruncated xmlns="Email:">0</BodyTruncated>
          </ApplicationData>
        </Add>
      </Commands>
    </Collection>
  </Collections>
</Sync>

5715efb8b0cd303a3d2c8262625559ef [0000] 14:21:33 <<< Ping
```

NOTE that in some cases, there are tag bodies that would not be valid in XML. E.g. <DisplayTo xmlns="Email:">"John Doe" <john.doe@icewarp.com></DisplayTo>. The < and > signs would have to be replaced with the < and > entities. In this case, the code is WBXML where these signs are allowed and are not in conflict with syntax rules. In the log, these signs are not replaced to allow better readability and to show exact content of the sent data.

NOTE: The ping command from device is sent each X minutes (where X is the heartbeat interval; the range of this interval is preset on server from 1 to 30 minutes – i.e if the device requests e.g. X = 60 minute heartbeat, it is reduced to 30 minutes) to alert the server that it is listening for changes on the originating IP address, and to keep the session alive. The server pings the device within these X minute periods whenever a change in server data occurs, and a synchronization of the corresponding resource (email folder, calendar…) is initiated. Once the synchronization is done, a new ping command is sent immediately regardless the heartbeat interval.

NOTE that the device can change the heartbeat interval according to synchronization frequency and the battery life.

Resetting the ActiveSync Database

WARNING – this will cause some devices to full synchronization and some devices which were enabled for Push may experience up to one-hour break before Push kicks in again.

Full synchronization means that all data which were up to now synchronized to the device will be deleted and synchronized again in one step. This can cause undesired data transfers and tax the battery. Therefore it is recommend to always use a limited look-back range for email synchronization.

ActiveSync is using a database storage for data which are processed on-the-fly but need to be preserved when a service is restarted or server rebooted. No maintenance is required from the server administrator, the database entries are manageable from GUI: in **Management – <user> – Options – ActiveSync** settings you can list active devices, disable the account, remove a dead device, perform RemoteWipe and set Security Policies.

The database comes pre-configured with server installation and is using PDO connection to the server. By default it is using SQLite RDBMS (same as WebClient) which comes default with PHP installation, but for better performance can be switched to MySQL or Microsoft SQL Server through controls in **WebClient – PDO Connection**.

To resolve general errors with ActiveSync, you may want to delete the database (or just rename it to keep a backup for roll-back):

Delete the file ***<IceWarp Installation Root>\calendar\activesync\db\sync.db***.

No data will be lost (these are stored separately in GroupWare database), only the list of devices will be cleared and populated automatically as the devices reconnect.

To resolve synchronization problems with an individual account, administrator should better use the **ActiveSync - Device Management - Delete Device** option to the very same purpose. However, in this case only the specific device will be reset and caused to full synchronization.

Changing the Server Heartbeat Interval

In some rare cases, you may want to experiment with the optimal heartbeat interval. IceWarp Server accepts any heartbeat interval requested by the device which is lower than 30 minutes. Usually the device will configure the optimal setting automatically. On some devices you can set it manually. Setting it higher can improve battery life while on push, but longer than 30 minutes is not recommended as sessions may be interrupted on network level by routers. Setting it lower will guarantee frequent updates of the IP address the device is listening on and could be used in cases where Push is stopping after a regular period of time.

Setting the maximum heartbeat acceptable for the server can be done by setting the internal server variable through a command-line tool:

To display current heartbeat in milliseconds:

tool display system C_PushServer_Heartbeat

To set the heartbeat to specified value in milliseconds:

tool set system C_PushServer_Heartbeat 1800000

If you wish to set the heartbeat higher than the default 30 minutes, you need to modify the web server settings to extend PHP session timeout. In case you are running ISAPI web server mode (this is the default on Windows), this step is not required.

In case you have switched the default ISAPI mode to FCGI (Fast CGI, see **WebClient Administration Guide** for details or search the knowledge base for FCGI), or if you are running Linux where FCGI is default, then you need to modify the web server settings accordingly:

Edit this section in **<Installation root>\config\webserver.dat** and set the same value in milliseconds:

- for Linux

  <ITEM>
  <TITLE>[activesync]</TITLE>
  <MODULE>(fastcgi)var/phpsocket;scripts/phpd.sh;1800000</MODULE>
  </ITEM>

- for Windows

  <ITEM>

  <TITLE>[activesync]</TITLE>

  <MODULE>(fastcgi);php\php.exe;1800000</MODULE>

  </ITEM>

GroupWare Mailbox Access

GroupWare Mailbox Access extends the capability of ActiveSync compatible mobile devices to work with resources which are not natively supported by Exchange ActiveSync, such as Files, Notes, and Tasks. These items are transparently converted to email messages and made available in mobile email client under the corresponding folder name- exactly as seen in WebClient or Outlook, multiple folders or localized folder names are supported too. Where users would normally need to install and multitask with several applications on their devices to enable the synchronization (such as WebDAV client, SyncML task manager), thanks to GroupWare Mailbox Access, the items are securely synchronized to the device as emails (on-demand or using DirectPush where available), including their full detail, categorization, attendees and attachments. The original Versit object (the native GroupWare format) is always attached, and can be easily forwarded to another users in need of the data, who can read it or save it directly into their groupware.

How it works:

- GroupWare folders are mapped to IMAP email folders
- GroupWare items are converted to e-mails
- Accessible in any client which supports email sub-folders (see Compatibility Matrix)
- Fully transparent to any mobile device, immune to problems with incapable devices
- **Notes**: include full detail, sorted by modification time, attachments included
- **Tasks**: completed are not synchronized if email filter is set to less than 7 days
- **Files**: acceptable file size is limited only by the device capability
- Category is recorded as the email sender
- One-way synchronization from server to client

The setup on Windows Mobile-based and most other devices requires the user to check-mark the GroupWare folders for synchronization under the ActiveSync synchronization settings. Mail.app of the Apple iPhone lists all folders including sub-folders by default and they are available out-of-the box, only DirectPush needs to be enabled in Settings if desired. Some devices don't list any extra folders but the default ones (Inbox, Drafts, Sent, Trash) and therefore the GroupWare Mailbox Access cannot be used- in some cases it might be possible to move the GroupWare folders under the Inbox to access them.

Battery Life Considerations

Turn Push off to conserve battery life. On some devices, Push can be turned off just for email and remain on for PIM synchronization – this will provide some advantage in battery life over downloading each new email to the device instantly and still keep the address book and calendar always in synchronization. Push generates only a little data traffic until items get actually synchronized with the server, comparable to IMAP IDLE for example. It is the open network connection which consumes power.

Turn WiFi off if you have a working connection using 2G or 3G mobile network. Turn off scanning for new WiFi networks at the very least.

Set your home mobile network (manual network selection) and turn off scanning for other networks (automatic network selection) unless you are travelling.

Disable Bluetooth unless you frequently use a wireless headset.

Set the heartbeat interval (if such option is available) on the device to a longer period of time, up to 30 minutes. If you experience issues like fewer new email notifications, use the default or automatic heartbeat.

Do not alter the Heartbeat interval set in IceWarp server unless you urgently need to. Setting it lower will cause more frequent updates (pings) from the device to server, which will tax the battery exponentially more.

Security Tips

Establish a strong password policy for server authentication through **Administration GUI – Policies – Password Policy**.

Instruct users to always enable the encrypted SSL connection. At best install a CA-issued certificate (VeriSign, DoCoMo, …) on your server.

Use on-server anti-spam and anti-virus wherever possible to filter out malicious emails (phishing and malware).

Use encryption options (or install software enabling this) for any sensitive user data stored on memory cards.

Never store passwords, PIN numbers and other sensitive information on a mobile device. If you have to, use a password manager application which allows setting a strong keychain password, can wipe data on failed password entry, and synchronizes with a desktop software so that you do not lose data when device is lost, stolen or wiped.

Disable Bluetooth Discoverable mode and enable it only when pairing with a new accessory (e.g. a headset) or another mobile device (e.g. when receiving a business card).

Consider to install Anti-Virus even on mobile devices, especially on Windows Mobile platform.

Use the advanced Security Provisioning features to establish corporate security policies:

- Set a reasonably short Inactivity timeout before the device locks
- Require PIN for unlocking
- Local Wipe on failed unlock attempts
- Minimum PIN length, strength and expiration

Instruct users to engage the built-in security features themselves even if they are not predetermined by Security Provisioning.

SmartDiscover

Overview

Due to many different services and protocols used in communication software these days, end users are often in doubt how to setup their client applications (email client, mobile synchronization, VoIP client and so on). Administrators need to use various mass-configuration tools or create detailed how-tos for end users.

It is also time consuming and prone to error to configure all server's protocols in the client application. A solution to retrieve all the server's capabilities and supported protocols is required.

SmartDiscover is a mechanism which ensures that any client application once supplied email address and password (every user must know their email address and password) and authenticated by the server, will receive a complete list of available protocols, ports, URLs and server addresses. All communication is encrypted by SSL connection between client and server, and SSL certificate is also used to validate the server hostname. User can start working immediately with zero configuration required.

SmartDiscover within ActiveSync is 100% compatible with Microsoft AutoDiscover technology. Microsoft has implemented AutoDiscover in Exchange server for Outlook and Windows Mobile ActiveSync clients only. IceWarp goes further and extends available applications by its own email client, SIP and IM clients, and the notifier utility. Virtually any protocol settings can be configured using SmartDiscover feature, provided that the corresponding client has SmartDiscover support built-in.

MSDN Links:

http://msdn.microsoft.com/en-us/library/cc433481.aspx

http://msdn.microsoft.com/en-us/library/cc463896.aspx

Test:

https://www.testexchangeconnectivity.com/

How it Works

The client application once supplied with the user's email address will try to contact the server through ***HTTP GET requests***, using the domain part of the email as a basis. The communication is secured by SSL for data encryption and validation of the remote host. This assumes an SSL certificate installed on the server that the device can recognize (CA issued). If the URL does not exist or failed with an error, the client retries the other URL using the same mechanism until the server's SmartDiscover service can be contacted.

The preset URLs are following in order to be compatible with ActiveSync enabled devices:

https://autodiscover.domain.com/autodiscover/autodiscover.xml

https://domain.com/autodiscover/autodiscover.xml

The client will then authenticate by HTTP authentication, using the same email address and password combination, and if successful, the server will return the configuration details in the form of an XML formatted plain text file. The client reads the parts corresponding to services it provides, and configures itself without any user's interaction.

Request

1. SmartDiscover domain attempt

   A client having an email address and password of the user will issue a simple HTTP GET request to:

   https://autodiscover.domain.com/autodiscover/autodiscover.xml

   Authentication request should be returned from the server. When authenticated properly via HTTP Authentication an XML response is returned from the server.

2. Original domain attempt

If the URL does not exist or failed with an error the client should retry additional URL using the same mechanism:

https://domain.com/autodiscover/autodiscover.xml

3. MX query host attempt

   If still not successful, a client MAY issue a DNS MX query for the domain to list the records that correspond to the server's hostname. It checks all MX records in the order of preference and attempts to contact the same URL as in step 2):

   https://mxhost1/autodiscover/autodiscover.xml

   https://mxhost2/autodiscover/autodiscover.xml

NOTE – that this step is specific to clients developed by IceWarp and does not follow the original Microsoft specification.

Response

When received a successful HTTP 200 OK response with Content-Type: text/xml the following structure is returned:

...

<Autodiscover>

<Response>

<Culture>en:en</Culture>

...

<User>

<DisplayName>John Doe</DisplayName>

<EMailAddress>john@doe.com</EMailAddress>

</User>

...

<Account>

...

<Protocol>

<Type>MobileSync</Type>

<Server>http://localhost/Microsoft-Server-ActiveSync</Server>

<Name>http://localhost/Microsoft-Server-ActiveSync</Name>

<LoginName>john@doe.com</LoginName>

</Protocol>

...

<Protocol>

<Type>XMPP</Type>

<Server>localhost</Server>

<Port>5222</Port>

<LoginName>john@doe.com</LoginName>

</Protocol>

...

</Account>

...

</Response>

</Autodiscover>

...

Each server type consists of these attributes. Some of them are optional, some of them apply only to certain types.

<Type> - ID of the protocol

<Server> - Server address or URL

<Port> - Port for for hostname based services

<LoginName> - Username used for authentication

Configuration

1. The administrator needs to ensure that either of these DNS records exist:

   • DNS A record: ***autodiscover.icewarpdemo.com*** (normally it does not exist)

   • DNS A record: ***icewarpdemo.com*** (where the domain is the exact hostname of the server where all services are running; normally it does not exist for a plain mail server, but can be already established for web, XMPP or SIP services)

   Use the supplied DNS Query utility found in <Installation root>\dnsquery.exe to check your A records (Host address) if the SmartDiscover fails for ActiveSync clients.

   NOTE – that for Notifier and other IceWarp native clients, the records do not have to be established in DNS – these clients will also check the hostname using the MX records, i.e. if the email is working, Notifier will configure itself without additional DNS changes. However for ActiveSync, one of the A records above must exist.

2. A non-expired, CA-issued SSL certificate needs to be installed on the server for SmartDiscover to work with iPhone. Windows Mobile requires a non-expired, either self-signed or CA-issued SSL certificate public key to be installed on the device, corresponding to the certificate installed on the server. Otherwise the SmartDiscover will fail due to untrusted connection with the server (and therefore untrusted authentication).
3. In **System – Services – Control – Properties**, set SSL port number to 443. SmartDiscover will not work without this setting on most ActiveSync devices.

Global Address List

The Global Address List (GAL) also known as Global Address Book is a directory service within the Microsoft Exchange email system. The GAL contains information about all email users, distribution groups, and other Exchange resources.

What is GAL in IceWarp Server?

- GAL is any public contacts folder with a GAL flag
- an IMAP user account which contains a public Contacts folder set as GAL
- a Public Folder which contains a public Contacts folder set as GAL
- GAL can be automatically populated from a group's member list
- there can be multiple GAL folders (one for each public folder) and user can browse through all of them on Windows Mobile, iPhone or Blackberry, taking advantage of a transparent multi-folder access
- having multiple GAL is also a great feature if the user is a member of more groups
- GAL can contain photos, certificates and other resources associated with a contact

Groups in GAL

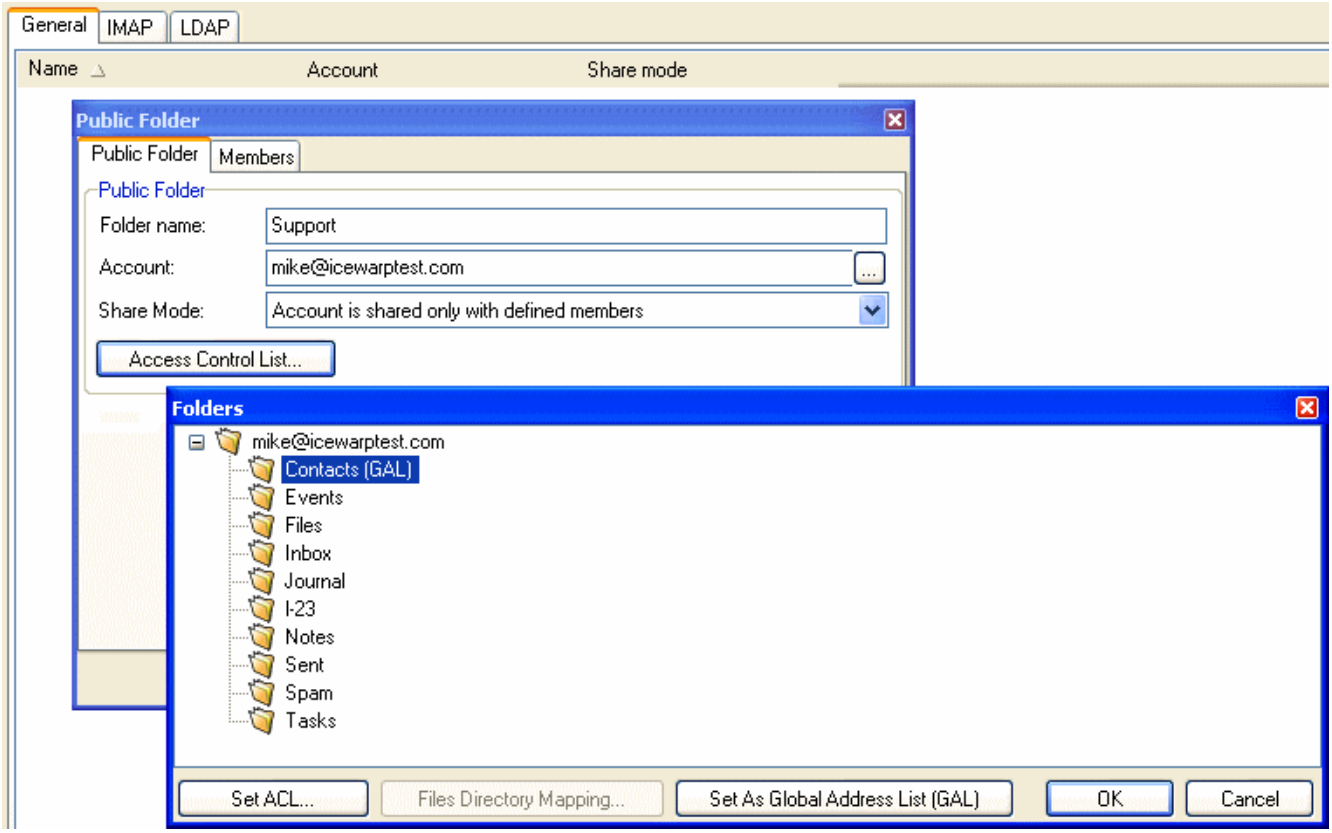
GAL supports listing of group accounts. Groups are represented by

Creating GAL

1. Automatically:

   Create a new group account (***Ctrl+G***), check the ***Create a public shared folder*** option, name the folder (e.g. Contacts) and check the ***Populate GAL with group members*** option. Switch to the ***Members*** tab, click ***Add...*** and select any accounts on the server, then confirm the selection by clicking the ***Select Account*** button. You can repeat this step until the GAL is populated with all members. READ access is enough for GAL.
2. Manually:

Assume you have a user account, a group account or a Public Folder which contains a public **Contacts** folder that you want to publish as GAL. Go to **GroupWare – Public Folders**, select the account, select the **Contacts** folder (if there are multiple Contacts resources, you can select which of them will be your GAL) in the **Folders** dialog, click ***Set as Global Address List (GAL)***. The ***(GAL)*** tag will appear next to the selected folder.



SmartSync

SmartSync is a unique extension to EAS protocol, fully transparent for any client. Similar to suspend and resume sync in SyncML, it is able to recover from situations when network error occurs in the moment when server responds to client requests. The client can't tell if there was a network error unless the connection drops altogether on TCP/IP level, such as when the network session times out, PHP instance is terminated or times out.

SmartSync is initiated whenever client sends another request with SyncKey equal to the preceding request received. This indicates that server response (status and on-server changes) didn't arrive to client, so it didn't increment the SyncKey. Exchange Server would initiate a full synchronization at this point, to prevent data loss or corruption- items could have changed on client or server side in the meantime.

When in SmartSync mode, IceWarp ActiveSync server sends status response to all preceding incomplete requests and then repeats all preceding requests to add/change/delete items as they were, or changed if they have changed in the meantime on the server, with conflicts resolved according to user-defined settings or the default 'server wins' policy. If there were client changes in the meantime, server only confirms the status to proceed with synchronization and any client changes are reflected later after the resume.

The synchronization then continues normally. SmartSync can be activated as many times as needed, and is able to recover the sync even if up to every other sync request is not completed as it should.

The commented log snippet illustrates an interrupted synchronization with subsequent change of the item on the server (client device is an iPhone).

```
a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:35:01 <<< Sync

<Sync xmlns="AirSync:">

  <Collections>

    <Collection>

      <Class>Contacts</Class>

      <SyncKey>31</SyncKey>

      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>

      <DeletesAsMoves/>

      <GetChanges/>

      <WindowSize>50</WindowSize>

      <Commands>

        <Add>

          <ClientId>26477</ClientId>

          <ApplicationData>

            <FileAs xmlns="Contacts:">Alex</FileAs>

            <LastName xmlns="Contacts:">Alex</LastName>

            <Picture xmlns="Contacts:"/>

          </ApplicationData>

        </Add>

      </Commands>

    </Collection>

  </Collections>

</Sync>


<!-- Client added an item successfully, but server response is missing here due to an
error -->


a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:35:43 <<< Sync

<Sync xmlns="AirSync:">
```

```
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>31</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <DeletesAsMoves/>
      <GetChanges/>
      <WindowSize>50</WindowSize>
    </Collection>
  </Collections>
</Sync>


<!-- Client proceeds but SyncKey is the same, SmartSync is initiated, there was a
change on server -->


a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:35:43 >>> 200 OK
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>32</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <Status>1</Status>
      <Responses>
        <Add>
          <ClientId>26477</ClientId>
          <ServerId>3b137c61c028</ServerId>
          <Status>1</Status>
        </Add>
```

```
      </Responses>
    </Collection>
  </Collections>
</Sync>


<!-- Server sent OK status to resume the synchronization of the preceding item but
with a new SyncKey -->


a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:36:12 <<< Sync
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
      <SyncKey>32</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <DeletesAsMoves/>
      <GetChanges/>
      <WindowSize>50</WindowSize>
    </Collection>
  </Collections>
</Sync>


<!-- Client requested standard incremental sync -->


a4a5231d6acc77f60e477a8e23c12c2c [alex@icewarpdemo.com] [0000] 15:36:34 >>> 200 OK
<Sync xmlns="AirSync:">
  <Collections>
    <Collection>
      <Class>Contacts</Class>
```

```
      <SyncKey>33</SyncKey>
      <CollectionId>2d97d4e09a89f127e37a69c79b45c159</CollectionId>
      <Status>1</Status>
      <Commands>
        <Change>
          <ServerId>3b137c61c028</ServerId>
          <ApplicationData>
            <LastName xmlns="Contacts:">Alex E</LastName>
            <FileAs xmlns="Contacts:">Alex</FileAs>
          </ApplicationData>
        </Change>
      </Commands>
    </Collection>
  </Collections>
</Sync>

<!-- Server sent the changed item to the client -->
```