IceWarp Unified Communications

ActiveSync Guide

Version 11.4

Published on 2/9/2016

Contents

ActiveSync Guide

Registered Trademarks

iPhone, iPad, Mac, OS X are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft, Windows, Outlook and Windows Phone are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Android is a trademark of Google Inc. IceWarp is a registered trademark in the USA and other countries.

About

Microsoft 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.

Microsoft 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

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

- Windows CE, PocketPC
- Windows Smartphone
- Windows Mobile 5.x, 6.x
- Apple iOS
- Symbian S60, S90 powered Nokia phones (latest firmware)
- Palm OS 4
- Google Android
- BlackBerry 10
- Windows Phone 7.x, 8.x
- Windows 8.x, desktop
- MS Outlook 2013

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
- Notes
- 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
  - add/delete/rename/move operations on folder tree
  - mail folders management is available on all devices
  - native groupware management is available only on Apple devices
  - virtual groupware folders management is available on all devices
- Complete email handling (send, reply, forward, mark read/unread etc.)
- Flags synchronization (flagged, replied, forwarded)
- 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
  - Remote Wipe 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
- User access to devices lists, some policies and Remote Wipe from WebClient
- 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
- Security policies
  - to enforce device password, its strength, maximum allowed unlock attempts, local wipe to delete all data in case of abuse
  - all security policies are implemented on IceWarp Server side – real functionality depends now on a device side
  - list of supported policies

Current Limitations

- TNEF formatted meeting invitations (sent from Outlook) are not supported (can not be responded to by the means of EAS or IceWarp WebClient)

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)
- Tasks as Events/Notes
- Notes as Events

ActiveSync Compatibility Matrix

	Windows Phone 7.x, 8.x **Windows 8 RT/desktop** **Outlook 2013**	**Apple iOS** **(iPhone, iPad)**	**Nokia N Series** **Nokia E Series**
Plugin required	No	No	No Mail for Exchange (free)
Email	•	•	•
Calendar	•	•	•
Contacts	•	•	•
Tasks	•	•	•
Notes	***	•	***
SMS			
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 4.x	**BlackBerry** **NotifySync|** **Astrasync**	**BlackBerry 10**
Plugin required	No	Yes NotifySync| AstraSync	No
Email	•	•|•	•
Calendar	•	•|•	•
Contacts	•	•|•	•
Tasks	•	•|***	•
Notes	***	***	•
SMS			
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.

*** IceWarp Server enables clients to synchronize Tasks and Notes via Tasks as Events and Notes as Events modes

On-server Setup

Setting up ActiveSync service 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 **System – Services**, start **GroupWare Notification** service. In the Properties dialog (of this service), make sure 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. The service collects all changes on all accounts from IMAP/GroupWare in a UDP stream and is used by ActiveSync, SyncML and Outlook Sync to trigger synchronization in real time (as items arrive). Do not enable the service logging unless for a short time if required for troubleshooting, as the amount of data can be overwhelming. In this case, synchronization will not work for any device with 'as items arrive' synchronization schedule.

   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.

   If you have a load-balanced / high availability architecture, you need to disable the **GroupWare Notification** service (and ActiveSync service) on the secondary machine, so that all requests are routed only to the primary server. This server will take care of IMAP/GW notifications for all users and its **Control** service will manage any client ping requests. In other words, Push will not work load-balanced. ActiveSync service can be enabled on the secondary machine only if you do not intend to use Push at all.

3. In **System – Services**, verify that **Control** module 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** module running on port 80.

4. For **GAL** lookup, a user has to be able to read at least one GAL type folder. Search within GAL is performed by EAS itself on the server. To have GAL synchronized into a device, the *Public folders* check box (**ActiveSync Devices** dialog – **Manage Device** – **Device Settings** dialog – **Folders** tab) has to be ticked. See the **GAL Public Folder** section for details.

5. Enable **SSL** on the default port – HTTP (443) in **System – Services**. SSL ensures that mail and other data are securely encrypted during wireless transmission.

   BE AWARE: If SSL is not used, all data (even passwords etc.) are sent in plain text!

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 ***(fastcgi);php\php.exe***. For details and/or Linux version, see the **Troubleshooting** section.

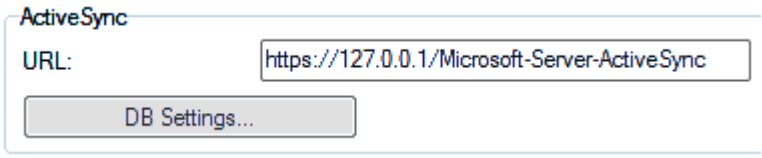
7. In the **ActiveSync** node, do not modify the port and URL end part. Change only the hostname if required by a special setup.

8. On the **<domain>** and **<user> – Policies** tabs, verify whether ActiveSync is enabled. This can be also used to limit access to ActiveSync service to selected users.

9. For **MobileSync (ActiveSync)**, check that in **System – Services – SmartDiscover** the same URL appears as in the **ActiveSync** node ***URL*** field. See the **SmartDiscover** section for details.

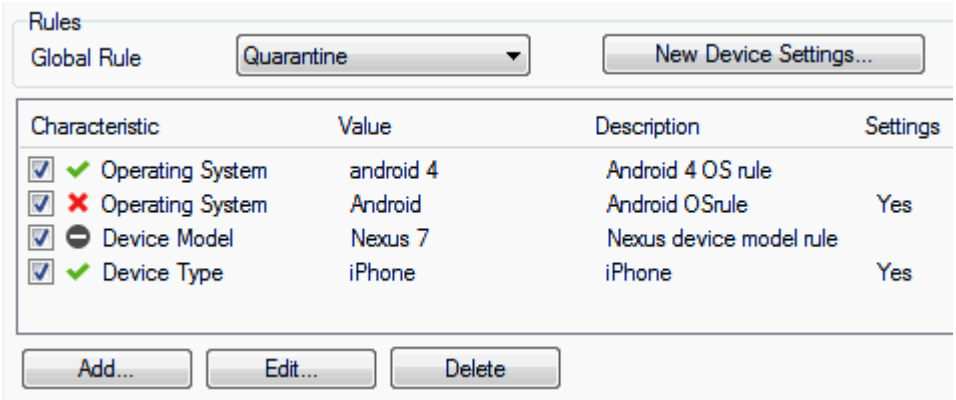
   In **System – Services – General – Web – Properties**, verify that SSL port is set to use port 443. **AutoDiscover** will not work without this setting.

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
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: 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: 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!*
DB Settings	Click the button to reveal the **Database** dialog. Here you can define ActiveSync database properties.

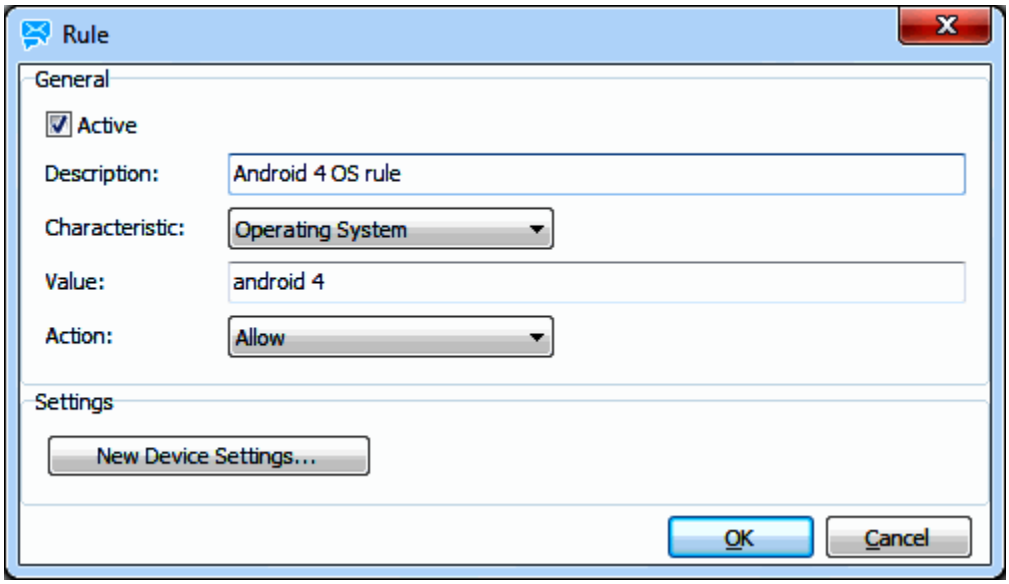
BE AWARE: Access mode to the service can be set on both domain and user levels. See the appropriate places (**<domain> – Policies**, **<user> – Policies**).



Field	Description
Global Rule	Select the default rule for devices that will not match any of ABQ rules set lower. The Quarantine item seems to be the most meaningful.
New Devices Settings	Click the button to open the **Device Settings** dialog. (For detailed description of this dialog, refer to the **ActiveSync Guide – Device Management** chapter.) These settings apply for devices that either do not match any rule or match a rule that has not set *New Device Settings*.
icons in the list	✔ – allowed device ✖ – blocked device ⛔ – quarantined device
Add	Click the button to add a new ABQ rule. The **Rule** dialog opens. See further. *For more information on **ABQ Management** follow the link.*
Edit	Select an existing rule and click the button to edit this rule. The **Rule** dialog opens. See further.

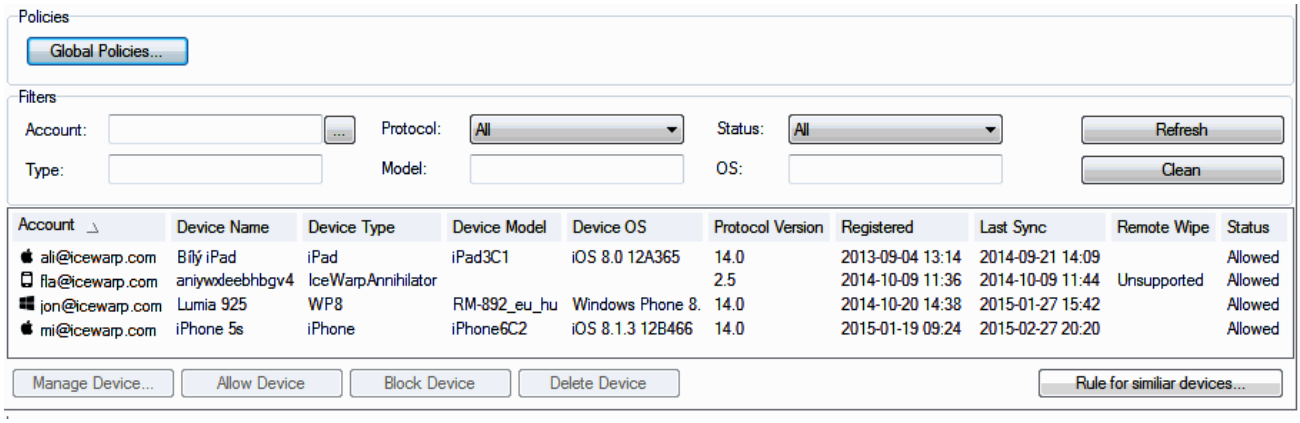
Delete	Select a rule and click the button to remove this rule. *NOTE: You may want to disable a rule but not to delete it. In this case, un-tick the box next to the appropriate rule.*

Rule Dialog



Field	Description
Active	Tick the box to have this rule active.
Description	Enter a short descriptive text.
Characteristic	Select a rule "criteria". Rules are listed according to the following criteria priority: *Operating System, Device Model, Device Type*.
Value	Enter the appropriate value. *For more information on **ABQ Management** follow the link to this chapter.*
Action	Select the appropriate action that is to be done when the rule value is matching. *For more information on **ABQ Management** follow the link to this chapter.*
New Device Settings	Click the button to open the **Device Settings** dialog. (For detailed description of this dialog, refer to the **ActiveSync Guide – Device Management** chapter.) These settings apply for devices that match just this rule.

Device Tab



Field	Description
Global Policies	Click the button to open the **Policies** dialog. Policies set here will be applied for all devices, unless changed within the **Device Settings** dialog (double-click the device – *Device Policies* button) for an individual device. For details about the **Policies** dialog, refer to the **ActiveSync Guide – Security Policies – Default Policies** chapter.
Filters	Use self-explanatory filters to ease your work with extensive device lists. Set a filter and click the *Refresh* button. Click the *Clean* button to show all list items.
Manage Device	Select a device and click this button to manage the device settings. For detailed description of this dialog, refer to the **ActiveSync Guide – Device Management** chapter.
Allow Device	Select a device and click this button to enable synchronization for this device.
Block Device	Select a device and click this button to block synchronization for this device.
Delete Device	Select a device and click this button to remove this device from the list. *NOTE: This action does not prevent the device from synchronization when it contact the server next time. Use the Block Device button to set it.*
Rule for similar devices	Select a device and click this button to create a similar rule. See the **ABQ Management** chapter.

DNS SRV Records Configuration

For information about this topic, refer to the **DNS Records Configuration** chapter (**manual.chm – Shared Topics**).

ABQ Management

Basic Terminology

- Basic means of ABQ management:
  - Device access rules (**ABQ Rules**)
  - Device information (**Characteristics**) sent by a client via the *Provision* or *Settings* commands
- **Standard ABQ Rule** is a triplet that consists of characteristic, its value and ABQ access state.
- Characteristic is one of the following: *Device Type*, *Device Model*, *Operating System*.
- **Value** is a case insensitive string.
- **ABQ access state** is one of the following: *Allow, Block, Quarantine*.
- Standard ABQ rule can have a description, rules can be disabled.

Types of ABQ Rules

- One mandatory simple ABQ rule without characteristic and its value (**Global ABQ Rule**)
- Optional standard ABQ rules will be supported on server level only (**Server ABQ Rules**)
- One optional simple (without characteristic and its value) ABQ rule for all domains and all users (**Domain ABQ Rules** and **User ABQ Rules**)

Determining Access State of NEW Devices

- Requirements:
  - Current device is authenticated
  - ActiveSync is enabled for the current user
  - Policy enforcement criteria are met by the current mobile device
- Is there an explicit rule to allow, block or quarantine the device on the user level (**User ABQ Rule**)? If so, grant full access or block access or quarantine the device. Else, go to the next step.
- Is there an explicit rule to allow, block or quarantine the device on the domain level (**Domain ABQ Rule**)? If so, grant full access or block access or quarantine the device. Else, go to the next step.
- Is this mobile device allowed, blocked or quarantined on the server level (**Server ABQ Rule**) by an *Operating System* characteristic rule? If so, grant full access or block access or quarantine the device. Else, go to the next step.
- Is this mobile device allowed, blocked or quarantined on the server level (**Server ABQ Rule**) by a *Device Model* characteristic rule? If so, grant full access or block access or quarantine the device. Else, go to the next step.
- Is this mobile device allowed, blocked or quarantined on the server level (**Server ABQ Rule**) by a *Device Type* characteristic rule? If so, grant full access or block access or quarantine the device. Else, go to the next step.
- Is this mobile device allowed, blocked or quarantined on the server level by a global rule (**Global ABQ Rule**)? If so, grant full access or block access or quarantine the device.
- How to match characteristic sent by a device with a **Server Rule** query value:
  - Comparison is case insensitive
  - If a query value is e.g. 'Android', then the characteristic sent by a device is compared step-by-step with the following: 'android', 'androi', 'andro', 'andr', 'and', 'an' and 'a'.

ABQ Access States

- Allow:
  - All EAS features are enabled
  - Allowed devices can be blocked by administrator
- Block:
  - Returns an "access forbidden" error to the device
  - Blocked devices are not displayed in WebClient
  - Blocked devices can be allowed by administrator
  - Do not confuse with the *Blocked* status when either *Hard Wipe* (*Soft Wipe* respectively) is set.
- Quarantine:
  - Only default folders are synchronized
  - Only one-way sync (client to server) is enabled
  - User gets information mail about this state
  - Quarantined devices are not displayed in WebClient
  - Quarantined devices can be allowed or blocked by administrator

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 is 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.

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 passcode, 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 screenshot below show the security settings on Apple iPhone that can be user-defined. As soon as the server security policy is enforced, the user cannot modify the enforced options.

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. Microsoft 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 way wipe is done depends on its implementation, some devices overwrite memory with a fixed bit pattern (e.g. iPhone), some do not do it. If security is a critical subject, devices that will be allowed to synchronize with a server should be chosen carefully.

NOTE: Time to complete device wipe on Apple iPhone can take up to an hour. The same applies to any other device that overwrites its memory with a fixed bit pattern (true delete).

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 Microsoft Exchange ActiveSync Device Management dialog. Remote wipe operations are separate from local wipes, and a device can be wiped remotely even if Microsoft 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 should not be able to opt out remote wipe. However, this again relies solely on device implementation . There are devices that allow a user to cancel remote wipe, which completely wastes its security purpose.

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

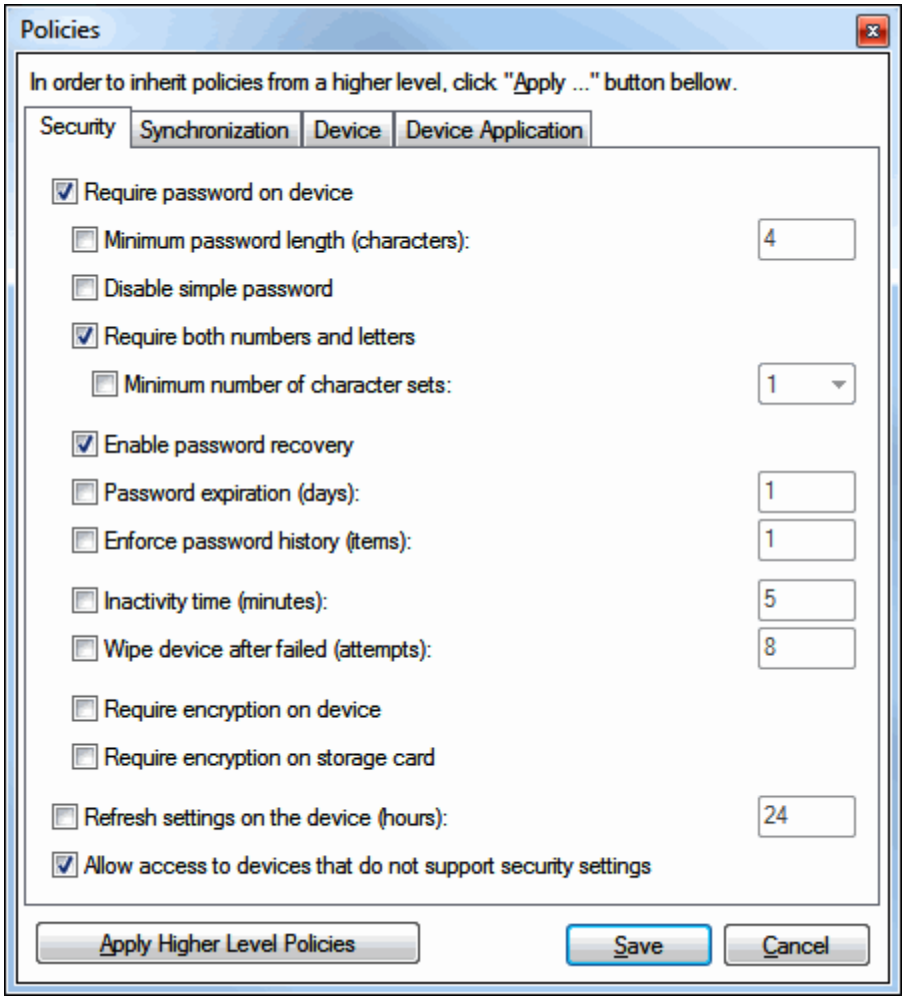
Global Level Policies

GroupWare – ActiveSync – Device tab – Global Policies button

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

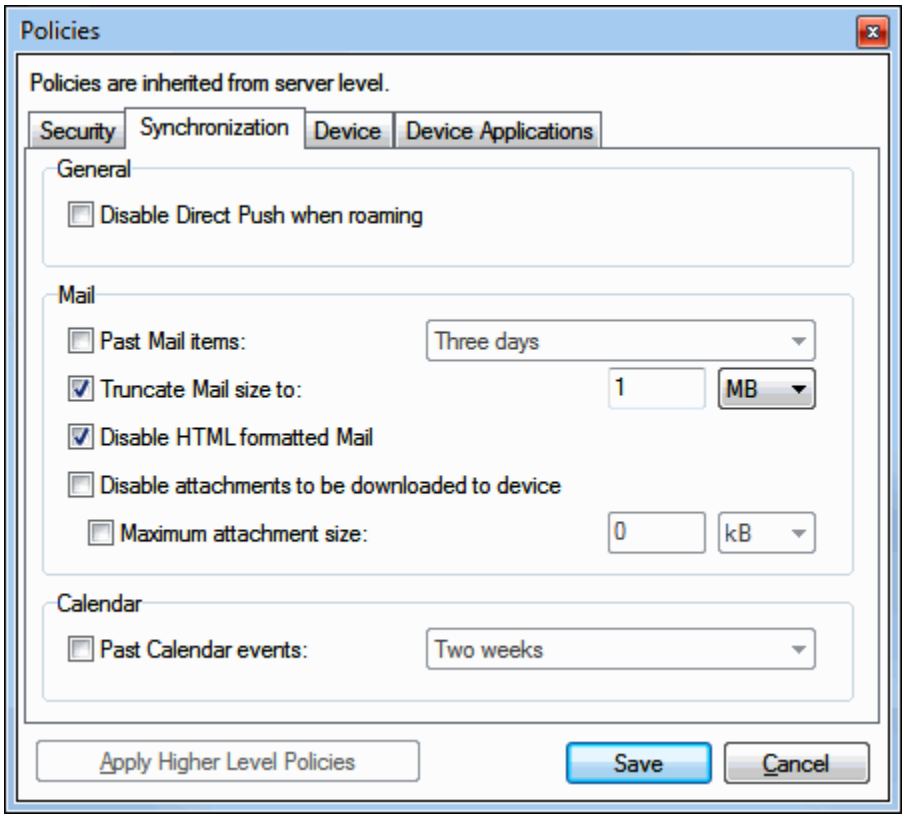
Default Policies

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.

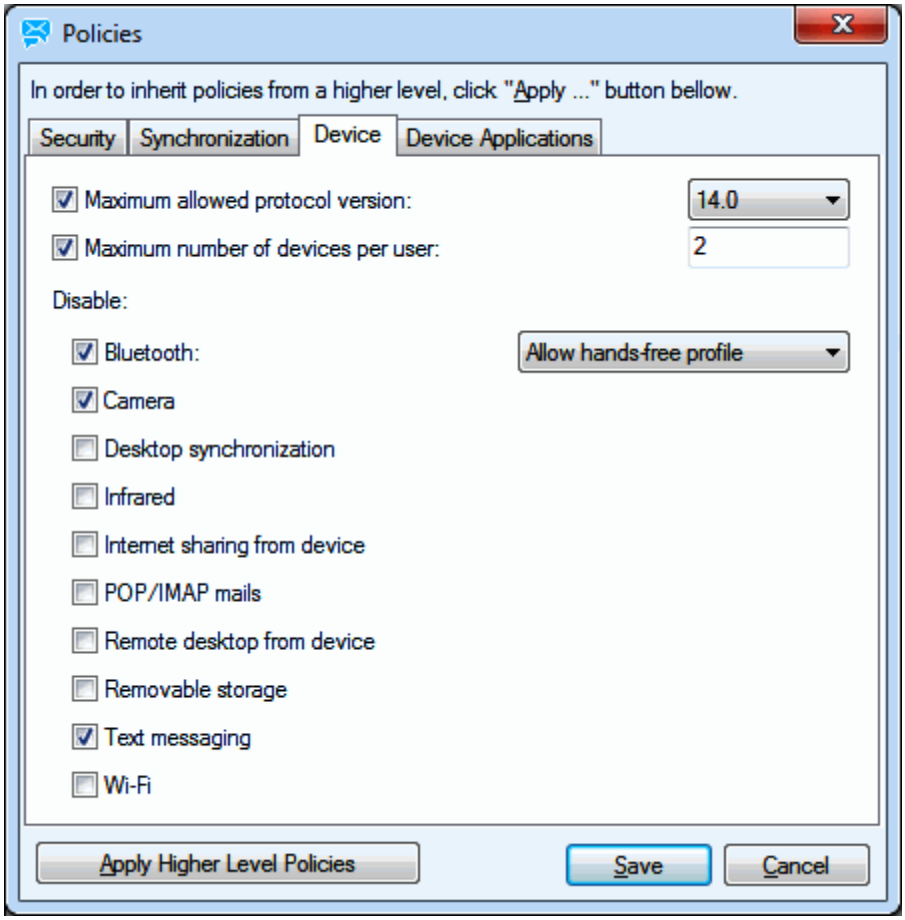


Field	Description
Require password on device	Check this box if you want to have possibility to enforce password properties to devices. *NOTE: If this box is not ticked, the related options are disabled.* *NOTE: Password parameters set here override device settings.* *NOTE: If this box is ticked, but none 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.
Disable simple password	Tick the box if you want to restrict users from using simple passwords – e.g. *1234* or *abcd*.

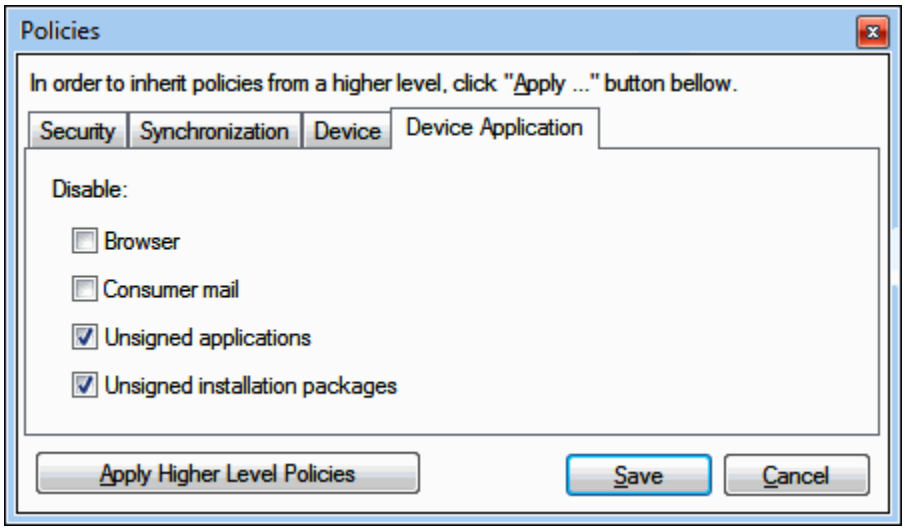
Require both numbers and letters	Tick this box to enforce use of stronger passwords.
Minimum number of character sets	Specifies the required level of complexity of the client password. Valid values are 1 to 4. The value specifies the number of character groups that are required to be present in the password. The character groups are defined as: *lower case alphabetical characters*, *upper case alphabetical characters*, *numbers* and *non-alphanumeric characters*. For example, if the value is 2, a password with both upper case and lower case alphabetical characters would be sufficient, as would a password with lower case alphabetical characters and numbers.
Enable password recovery	A recovery password is a password that is created by the device that gives the administrator or user ability to log on to the device once, using the recovery password. Next time, this user is forced to create a new password. The device then creates a new recovery password. If checked, the device can send a password, but the server does not enforce the policy. If not checked, the device should not send a recovery password, because the server will refuse to store the password.
Password expiration (days)	The password expiration is policy that specifies the maximum number of days until a password expires. ***0*** = passwords do not expire.
Enforce password history (days)	This is the policy that specifies the minimum number of previously used passwords stored to prevent their reuse by the client. ***0*** = storage of previously used passwords is not required. Value > 0 = minimum number of previously used passwords to be stored.
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.
Require encryption on device	Tick the box if you want the device to use encryption.
Require encryption on storage card	Tick the box if you want the device to encrypt also content that is stored on the storage card.
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
Disable Direct Push when roaming	If ticked, the device requires manual synchronization when roaming.
Past Mail items	Specifies the email age limit for synchronization. Messages that are older than the specified age are not synchronized. Tick the box and select from the list.
Truncate Mail size to	Specifies the truncation size for plain text or HTML formatted email messages: -1 = no truncation 0 = truncate only the header value > 0 = maximum size, in bytes (emails are truncated to this size) Tick the box, enter the size and select units.
Disable HTML-formatted Mail	If ticked, the device uses plain text formatted email.
Disable attachments to be downloaded to device	If ticked, email attachments download is disabled.
Maximum attachment size	You may want to limit the attachment size. If ticked, the specified attachment size is used as download limit. Bigger attachments are not downloaded.
Past Calendar events	You may want to specify the maximum number of calendar days that may be synchronized. Tick the box and select from the list.



Field	Description
Maximum allowed protocol version	Tick the box and select the maximum allowed protocol version. After device firmware upgrade, some synchronization issues can occur. In this case, lowering the protocol version can help.
Maximum number devices per user	Tick the box and enter the maximum number of devices.
Disable	Tick the items (device features) you want to disable. For Bluetooth select level.



Field	Description
Disable	Tick the items (applications) you want to disable.

NOTE: Usually, devices do not have implemented all the features present on the last two tabs. In such a case these settings are ignored.

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).

iOS devices do not identify themselves at the beginning of synchronization, which means some options depending on the *DeviceID* will be greyed out on this level, such as *Maximum Allowed Protocol Version* option. Server will accept the highest version offered by iPhone – 14.1. To force a lower one, the policy needs to be applied on user level.

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

or

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

or

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

or

double click an item in the device list on any level and select Device Policies.

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 provisions 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 (hardcoded, server, 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 capability 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 Microsoft 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).

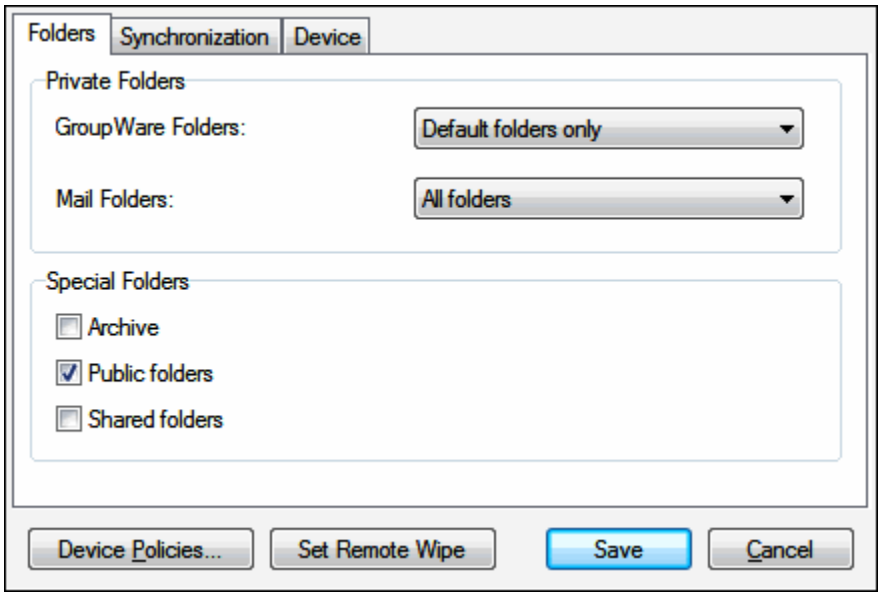
NOTE: This does not automatically cancel the passcode lock. User first needs to enter the existing password before he/she is able to modify the security settings or disable the passcode requirement.

*NOTE: 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.*

Device Management

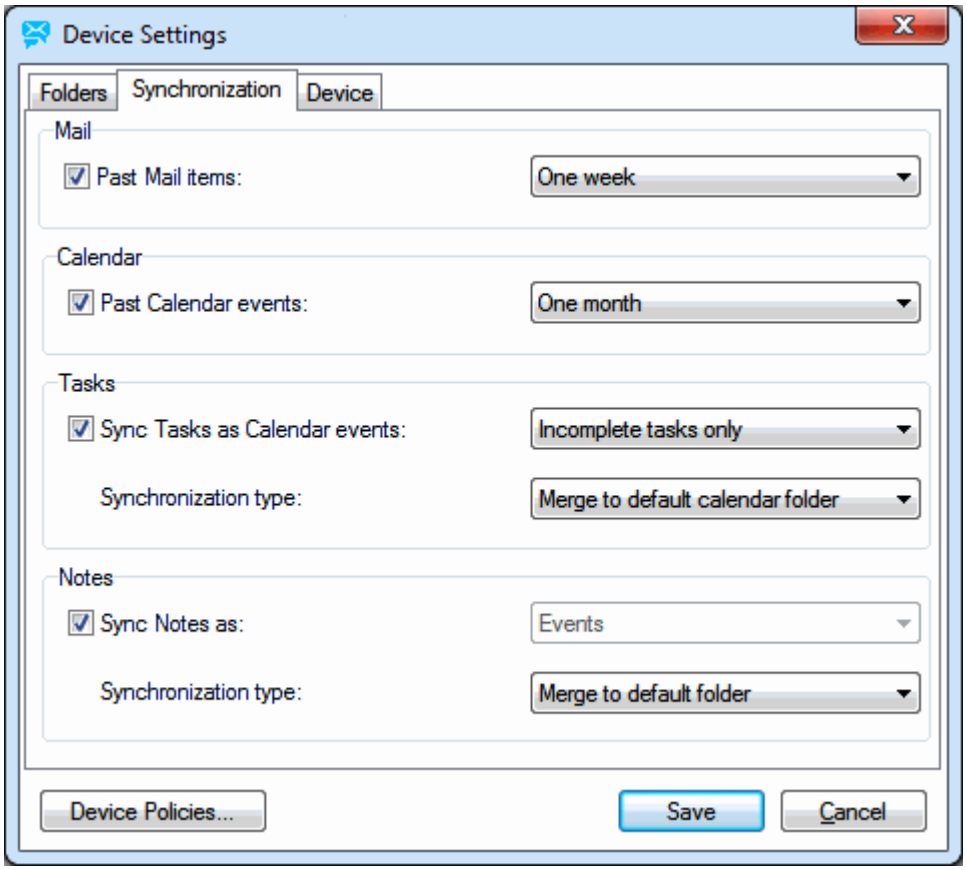
The **Device Settings** dialog allows you to manage other device features – Folders, Synchronization, etc.

Folders Tab



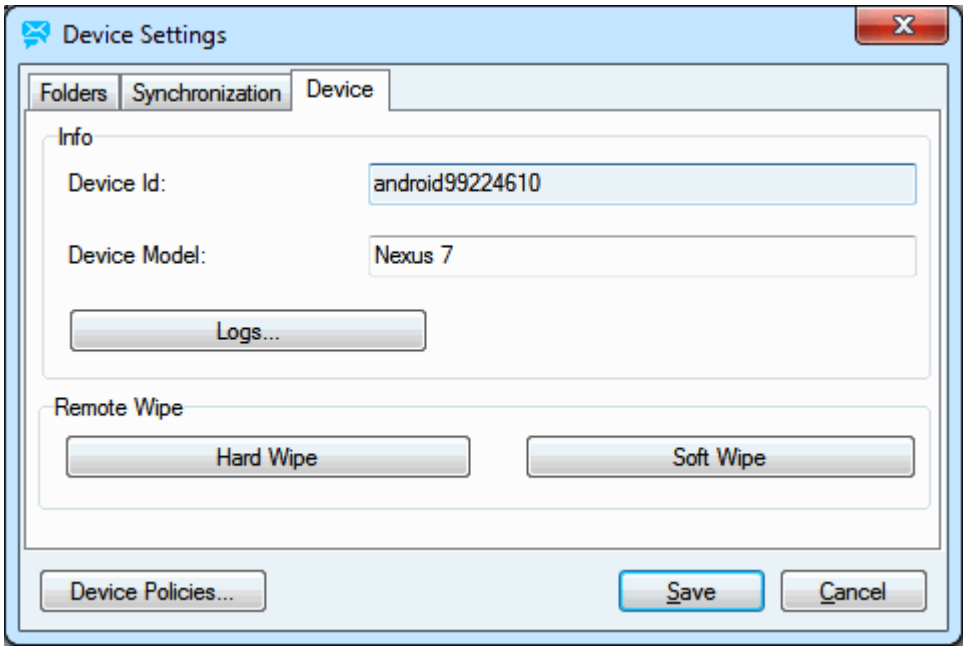
Field	Description
GroupWare Folders	Select whether you want to have ***Default folders only***, ***All folders*** or ***All with GroupWare as email*** (folders) synchronized to the device. ***All with GroupWare as email*** – select when a user has complicated folder structure, where groupware folders are embedded within mail folders and vice versa.
Mail Folders	Select whether you want to have ***Default folders only*** or ***All folders*** synchronized to the device.
Special Folders	Tick the box if you want to have respective folders synchronized to devices. • Archive • Public folders • Shared folders
Device Policies	Click the button to open the **Policies** dialog. For more details, refer to the **Defining Policies** chapter.

Synchronization Tab



Field	Description
Past Mail items	Tick the box if you want to limit age of mail items synchronized into the device on the server side. The device can be only more restrictive. Select how old items are to be synchronized. *NOTE: Older protocol versions do not support this feature. However, the server will respect the policy on its side.*
Past Calendar events	Tick the box if you want to limit age of calendar events synchronized into the device on the server side. The device can be only more restrictive. Select how old items are to be synchronized. *NOTE: Older protocol versions do not support this feature. However, the server will respect the policy on its side.*
Sync Tasks as Calendar events	In the case the device does not support tasks synchronization, tasks can be synchronized as events. Tick the box and select whether you want to have synchronized ***All tasks*** or ***Incomplete tasks only***.
Synchronization type	Those tasks can be synchronized either to a ***New calendar folder*** or ***Merge***d ***to default calendar folder***. In the case of a ***New calendar folder*** option, a new calendar type folder with an original task folder name is automatically created.
Sync Notes as	In the case the device does not support notes synchronization, notes can be synchronized as other item types. Select whether you want to have notes synchronized as ***Events***, ***Tasks*** or ***Tasks & Notes (Android app)***.
Synchronization type	Those notes can be synchronized either to ***New folders*** or ***Merge***d ***to default folder***. In the case of ***New folders*** option, a new folder (of the respective type) with an original notes folder name is automatically created.

Device Tab



Field	Description
Device ID	This field shows the device ID which cannot be edited.
Device Model	This field shows the device model.
Logs	Clicking this button opens the **Status – Logs** tab.
Hard Wipe	Click the button to set this kind of wipe. When the device contacts the server next time, all is deleted – the device is reset into the factory default state.
Soft Wipe	Click the button to set this kind of wipe. When the device contacts the server next time, all data related to the appropriate account are deleted.

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 ones 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.

   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** support (or setups for which AutoDiscover cannot work – especially accounts with an email domain different from IceWarp Server's FQDN), 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, Tasks, Notes or even SMS synchronization.

5. Advanced settings may include option to enable Push or a scheduled synchronization (should it 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; authentication is performed on http level.

We strongly recommend turning 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 Microsoft 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 or newer server?

   The settings backup is not backward compatible and your configuration file – ***webservice.dat*** – will be incompatible because of its obsolete content. 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.

   At least 40 upgrade scripts are executed through the upgrade to another major version (the bigger version gap, the more scripts), most prominently GroupWare database transformation takes place, thus skipping this part of installation is strongly discouraged and advanced services including Microsoft Exchange ActiveSync are poised to fail. Please follow the correct upgrade procedure first – for more information, refer to the **IceWarp Server Quick Start Guide** document – **Existing Installation Upgrade** section. .

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***. This indicates a 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 at least GPRS 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.

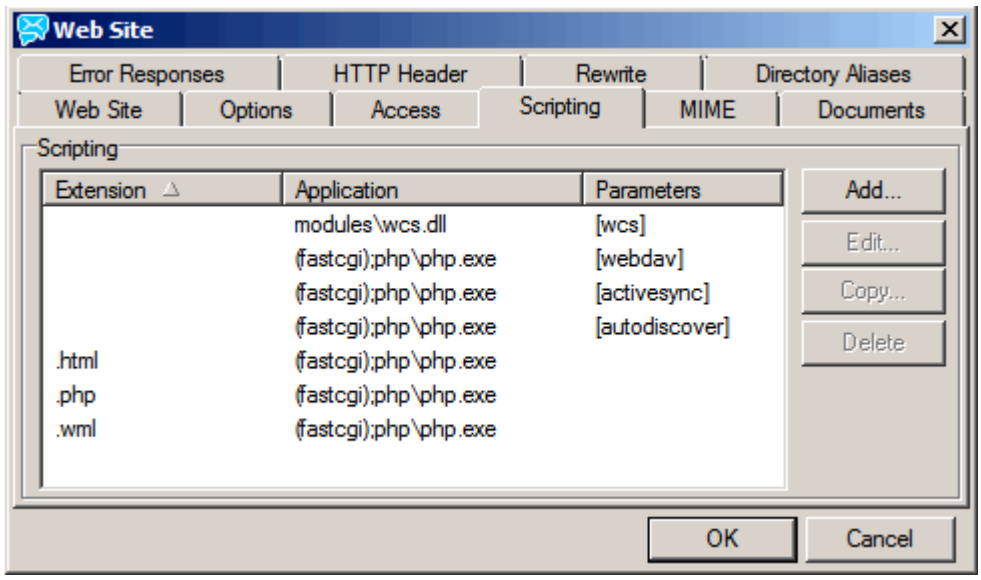
   To check whether the connection to IceWarp web service is working, point your browser on a computer (or a phone) located within the same LAN as the device to:

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

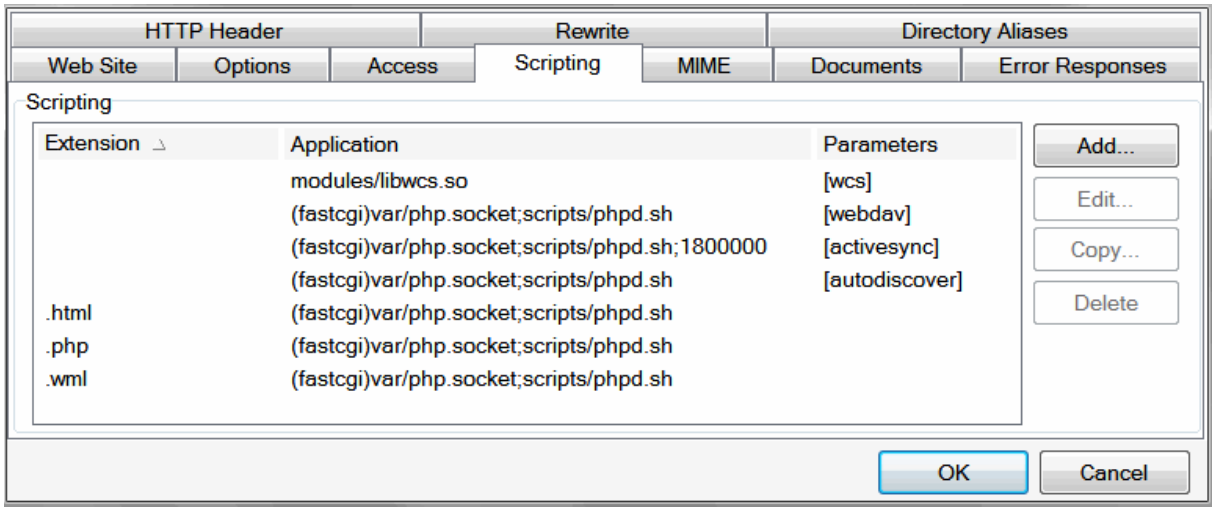
   A dialog window should come up asking for username and password. If it does not, the web service is misconfigured, the Scripting settings for ActiveSync are missing for the (***Default***) web service host, a firewall is blocking the connection or there is some other network error (i.e. wrong DNS resolution). 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**.

For Windows:



For Linux:



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

Example for Windows:

```
<EXTENSIONS>
   <ITEM>
     <TITLE>[activesync]</TITLE>
     <EXT/>
     <MODULE>(fastcgi);php\php.exe</MODULE>
   </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 Microsoft 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 misconfigured 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 EAS 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 Heartbeat interval, or set it to a lower value (maximum supported by the server is 30 minutes, see the **Changing the Server Heartbeat Interval** chapter). 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 misconfigured 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 mobile data network (i.e. 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. It can take the full heartbeat interval for the device to reconnect after it is 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**. All Windows Mobile devices and some Nokia handsets require SSL to be enabled for push to work. See the **SSL and Windows Mobile Devices** 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). 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 – Notification** group box – **Enabled** is active. Enable the logging in **System – Services – General – GroupWare Notification Logging** dropdown. 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: 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: The device can change the heartbeat interval according to synchronization frequency and the battery life.

Resetting the ActiveSync Database

WARNING: This will make all devices to perform full synchronization and will lead to a loss of your ABQ rules configuration.

Full synchronization means that all data which were up to now synchronized to the device will be deleted and synchronized again. This will cause undesired data transfers, tax the battery battery and could cause a device to hang while processing data. Full synchronization can be triggered due to a bug or protocol implementation as well. Even if all is fine, consider that a mobile device was not designed to work with thousands of items.. Therefore it is always recommended to use a limited look-back range for email synchronization.

ActiveSync server is using a database storage for synchonization metadata that needs to be preserved when the service is restarted. No maintenance is required from the server administrator, the database entries that are manageable in the Administration Console or even in WebClient. Both ways allow an administrator or user to list active devices, disable the account, remove a dead device, perform RemoteWipe and set Security Policies. Ofcourse, a user can control only his/her own devices while admin can manage settings on server-wide, domain-wide, user-wide and device-wide scopes.

IceWarp Server comes with a preconfigured SQLite database to provide out-of-the-box functionality, however we recommend switching to the proper database engine. In this case, MySQL is the only choice supported. Adminstrators are encouraged to use MySQL, especially when ABQ and/or EAS protocol of version 14.0 or newer is used by clients. Switch can be easily achieved with integrated database migration tool (**System – Tools – Database Migration**).

NOTE: When converting to MySQL from the default EAS SQLite database:

- *Open **/php/php.ini** in IceWarp installation folder, uncomment the line of **extension=php_mysql.dll**and copy it, create the **php.user.ini** file, insert the line into this file and save it into the same folder, so that it is not overwritten during upgrades.*
- *Copy **mysql/bin/libmysql.dll** to **/windows/system32** folder (x86 systems), or to **/windows/syswow64** folder (x64 systems); when using 64bit database version, obtain the 32bit version of the **libmysql.dll** driver from **dev.mysql.com***

*For more details, refer to the **Installation Guide – Database Selection** chapter.*

To resolve synchronization problems with an individual account, administrator can try to delete device from a server (**GroupWare – ActiveSync – Devices** tab – *Delete Device* button).The appropriate user should delete the account on the device as well. Once both device and server are clear of the account, the user should add its account to the device again. This will cause the device to do a full synchronization which can fix a synchronization issue. Note that many items can be synchronized for a long time, thousands of them may take hours – during this period of time, the device may seem not syncing at all. Check logs to learn what is really happening.

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 (examples for Windows, Linux versions use **tool.sh**):

tool display system C_PushServer_Heartbeat

To set the heartbeat to specified value in milliseconds:

tool set system C_PushServer_Heartbeat 1800000

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>

Email Message: ActiveSync Folder Push Request Status

Users can experience the situation when they obtain the following message:

For technical maintenance reasons, the server requests your mobile device (iPhone: appl866254sede) to perform a synchronization of your folders. In the case, the synchronization is not performed by the device automatically, remove and add your ActiveSync account. If problems persist, contact your technical helpdesk.

Explanation

This email is sent to the user when the device is requesting changes for an invalid folder ID (such as when the folder was deleted) and does not react to folder synchronization request sent by the server. The server attempts 3 times to send folder synchronization command to the device, when the device does not react, server stops responding to ping commands regarding that folder.

Solution

Just do what it says, delete and recreate the EAS account on the device.

Or, if everything continues to work normally, you can ignore it.

Ms Outlook 2013 Synchronization

Known Issues

In version 11.2.0, you can experience the following issues:

IceWarp Server Issues

The *Done* flag set in a client will become red flag on a server. This is because the *Done* flag is not supported by the IMAP server.

Exception from a recurrent event (single occurrence from a series) is updated wrongly. This is because of incomplete implementation of support for this functionality which in most cases results in saving of the updated properties in the occurrence (other properties that should be read from the master object are lost). This problem will be fixed in future releases.

Outlook Issues

Outlook does not use the *SmartReply* nor *SmartForward* command violating EAS v14 specs. As IceWarp Active Sync server expect these commands used when communicating via v14 protocol, reply and forward flags are not set on the server side. Outlook does that only locally (you will have them in Outlook only, nowhere else).

Quick step actions do not work as expected, you may find some combination that actually works, but in general consider this feature faulty.

Impossible to synchronize, add, update or remove notes as Outlook does not support notes synchronization in the native mode. No request is sent to an EAS server. You can overcome this with an IceWarp feature, see the **Best Practices** chapter.

Contacts folder synchronization is limited to the default folder only as no other folder of this type is supported by Outlook. There is nothing you can do about it.

Outlook does not reflect send out failures. Even thou the status of 110 is returned from the server, a client keeps on sending the message. User is not informed and the message persist in outbox. IceWarp ActiveSync server behavior was altered to overcome this behavior since version 11.2.0.

Outlook adds folders before it deletes them. This can lead to unnecessary *[1]* suffix in folder names – this may occur when *tasks as events* or *notes as events or tasks* enabled. It seems that this behavior is mainly related to groupware folders. Since version 11.2.0, IceWarp Server replies to a client in a way that might mitigate this issue.

Reply and/or forwarded flags are sent in the server reply, however Outlook does not display them. You will have those flags e. g. in WebClient, but will not be present in Outlook.

When deletion or move fails on the server side, the client ignores the response and performs deletion on its side only. The item does not reappear after synchronization (which it should, as this delete action failed on the server). IceWarp ActiveSync server altered its behavior to work around this issue since version 11.2.0.

First (seed) synchronization of already existing account is terribly slow, lasting hours or even days. This particularly applies to accounts with thousands of items. Note that the way Outlook makes its request is not efficient at all and once data is acquired from server it takes some time to render it. It even happened that synchronization never finished due to problems described in SmartSync chapter (motivation to implement it). SmartSync was improved in version 11.2 to overcome problems that would trouble/prevent synchronization.

Best Practices

Outlook

Outlook was invented as a thick email client. As such, it is not suitable for a use with ActiveSync. EAS plugin implementation for Outlook does not resolve this fact and treats the protocol for mobile communication as a hard disk. That is why we recommend to restrict synchronization as much as possible:

- Use time filters for emails and events – one month limit seems to be reasonable.
- Synchronize only default folders, or as few as possible.

Following this recommendation should have positive impact on performance.

Communication with IceWarp Server via EAS (instead of standard protocols) brings to a user only restricted groupware data access in Outlook. This communication is really very restricted because of implementation in Outlook and we do not recommend it. For those who do not like to use Outlook like a "mobile device" i. e. for those who want a client with a full functionality, we have IceWarp Outlook Sync (equivalent of the Outlook with Exchange synchronization).

Outlook does not support notes synchronization, but one of IceWarp Server features allows to deal with this insufficiency. This functionality can be found in device settings (IceWarp Server administration console – **GroupWare – ActiveSync – Devices** – double-click ***Outlook*** – **Device Setting**s dialog – **Synchronization** tab – ***Notes*** section). To enable it, do the following:

- Tick the *Sync Notes as:* check box.
- Select either *Events* or *Tasks* from the drop down.
- If applicable, select *Synchronization Type*. This is possible only when more than default folders are synchronized. By default, you will find notes in a task or event folder depending on your choice.

In general, you can get more functionality with Outlook when the *GroupWare As Email* feature (explained in separate chapter) is turned on, but be aware that doing so will come at a price of performance – the more you synchronize the longer it takes. Also, in versions prior 11.2.0 synchronization could get broken by some problematic item, so the more is synchronized the higher the chance to encounter a problem.

GroupWare Mailbox Access (GroupWare as Email)

GroupWare Mailbox Access extends the capability of ActiveSync enabled devices and applications to work with resources which are not natively supported by Microsoft Exchange ActiveSync protocol itself or their support was not implemented – 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 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 standardized groupware format) is always attached, and can be easily forwarded to another user in need of the data, who can read it or save it directly into their groupware.

Briefly, if a device is capable to synchronize mail folders (must be able to synchronize more than default ones) and calendar only, GroupWare Mailbox Access is a good choice to get more data into the device.

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 or clients
- **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 item (notes, tasks and files) synchronization from server to client only
- Two-way folder synchronization enhanced with a special feature. When a new folder is created on the client side, its type will be the same as its parent native type (i.e on a client you see a calendar folder as email folder, but if you create a new folder nested in it, the new folder type will be also calendar)

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 do not list any extra folders but the default ones (Inbox, Drafts, Sent, Trash) and therefore the GroupWare Mailbox Access cannot be used.

What can be achieved with this feature?

- Synchronization of files
- Folder management
- Displaying folder hierarchy (under virtual root)
- Displaying a groupware folder which is nested into mail folder and vice versa

Folder Synchronization Explanation

For certain folder synchronization settings (**Device Settings** dialog – **Folders** tab), IceWarp ActiveSync server uses so called virtual root. This folder is nested into the client root and folder hierarchy as it is on the server is synchronized into it. Virtual root can be confusing first as it creates duplicity of some folders – such folders are the same and contain the very same items.

Virtual Root

Why to use it?

- synchronization of mail folders under groupware folders and vice versa
- GW folders tree hierarchy
- possibility to change default folders while the server is running

When synchronization is set on the server so, that VR is not needed, a client will not use it.

How to orientate:

default folders are in the root (client can place here some other folders locally)

whole folder structure is placed under the virtual root – some folders may be duplicate

Folder Occurrence Table

	Folder Synchronization Mode				
Folder Type	Groupware as Email	All Mails All Groupware	All Mails Default Groupware	Default Mails All Groupware No Virtual Root Used	Default Mails Default Groupware No Virtual Root Used
Mail Default	2	2	2	1	1
Mail	1	1	1	0	0
Groupware Default	2	1	1	1	1
Groupware	2	1	0	1	0

where:

- 0 – not present in client i.e. not synchronized
- 1 – present; displayed in the client's native way or under a virtual root; synchronized without duplicity
- 2 – present; displayed in the client's native way and under a virtual root; synchronized, duplicity occurs

Folder Synchronization – Detailed Description

Folder Synchronization (Way from Client)

Create New Folders (FolderCreate):

Outlook limitations:

- Outlook supports creating mail folders only.

Mobile devices limitations:

- Only Apple devices support creating groupware folders.

IceWarp limitations:

- Prohibits creating mail folders when synchronization of only default mail folders is set.
- Prohibits creating groupware folders when synchronization of only default groupware folders is set.

Functionality:

- Create folder on a server side.
- Move the created mail folder to a virtual root folder tree if it has not a virtual root parent on the client side.
- Rename a created groupware folder to its full path on the client side.
- Create a virtual mail folder for the created groupware folder on the client side (optional).
- Force *FolderSync* if required.

Delete Folders (FolderDelete):

Outlook limitations:

- Outlook prohibits deleting default folders.
- Outlook supports deleting mails folders only.

Mobile devices limitations:

- Mobile devices prohibit deleting default folders.

IceWarp limitations:

- Prohibits deleting default folders (directly and also via their virtual mails folders).
- Prohibits deleting special folders (virtual root folder, Archive, Public, etc.)

Functionality:

- Delete a folder on the server side.
- Delete its subfolders on the client side.
- Delete a virtual mail folder on the client side if the deleted folder is its groupware folder (optional).
- Delete a groupware folder on the client side if the deleted folder is its virtual mail folder (optional).
- Force *FolderSync* if required.

Update (Rename and/or Move) Folders (FolderUpdate):

Outlook limitations:

- Outlook prohibits updating default folders.
- Outlook supports updating mail folders only.

Mobile devices limitations:

- Mobile devices prohibit updating default folders.

IceWarp limitations:

- Prohibits updating default folders (directly and also via their virtual mail folders).

- Prohibits updating special folders (virtual root folder, Archive, Public, etc.).
- Prohibits moving folders outside the virtual root folder tree!!!

Functionality:

- Update (rename and/or move) a folder on the server side (use the folder name only – not the whole path if such is displayed as a folder name).
- Force update for an updated folder itself on the client side if the updated folder is a groupware folder.
- Force update for an updated folder's virtual groupware folder on the client side (real GW folder is updated) if the updated folder is a groupware folder (optional).
- Force update for all updated folder groupware subfolders on the client side.
- Force *FolderSync* if required.

Folder Synchronization General (Way from Server)

Mail Folders:

Outlook limitations:

- None, it supports multiple mail folders synchronization without any known limitations and keeps their hierarchical order.

Mobile devices limitations:

- None in general, they support multiple mail folders synchronization without any known limitations and keep their hierarchical order.

IceWarp limitations:

- None.

Functionality:

IceWarp Server synchronizes mail folders under a virtual root folder (owner) and only default folders keep their root positions.

E.g. Following mail folders structure

SERVER side:		CLIENT side:	
|-Inbox		|-Inbox	default folder keeps its root position
| |-A	will be synchronized as	|-Owner	virtual root folder
|-B	---------->	| |-Inbox	general mail folder with the same name and content as the default folder
| |-C		| | |-A	general mail folder
|-Sent		| |-B	general mail folder
		| | |-C	general mail folder
		| |-Sent	general mail folder with the same name and content as the default folder
		|-Sent	default folder keeps its root position

Groupware folders:

Outlook limitations:

- Supports only one contacts folder (default).
- Supports multiple events and tasks folders synchronization (this is not a limitation, but a property to be considered).
- Adds prefix e.g. '*Tasks* - ' to all synchronized tasks folders except the default task folder.
- Does not support notes folders synchronization.

Mobile devices limitations:

- They usually support only one folder (default) per groupware resource type except Apple devices.
- Devices with native support of notes type folders are uncommon.

IceWarp limitations:

- None.

Functionality:

IceWarp Server removes hierarchical order for all groupware folders and uses their paths for their names!!!

IceWarp can synchronize also groupware folders as mails folders

E.g. Following groupware folders structure

SERVER side:		CLIENT side:	
|-Contacts		|-Contacts	
| |-Contacts2		|	only one contact folder (default) is synchronized
|-Events	will be synchronized as	|-Events	
| |-Events2	---------->	|-Events\Events2	groupware folders are in root and their names are their paths
|-Notes		|	
|-Tasks		|-Tasks	
|-Tasks2		|-Tasks - Tasks\Tasks2	Outlook adds 'Tasks - ' prefix

IceWarp Server can optionally synchronize groupware folders as mail folders (*Groupware as email*).

E.g. Following groupware folders structure

SERVER side:		CLIENT side:	
|-Mails1		|-Owner	virtual root folder
| |-Contacts2		|	only one contact folder (default) is synchronized
||-Events1	will be synchronized as	| |-Mails1	mail folder
| -Events2	---------->	| | |-Events1	virtual mail folder for groupware folder
|-Mails2		| |-Events2	virtual mail folder for groupware folder
		| |-Mails2	mail folder
		|-Mails1\Events1	groupware folder
		|-Events2	groupware folder

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 the rest of item types included in 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 data connection using 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 or other device.

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, Comodo, etc.) 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 computer application 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 in combination with ABQ rules 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, Outlook Sync plugin, 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: 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 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)

   To view DNS records of the domain, open the administration console – **Domains and Accounts – Management – <domain> – Information** tab. All relevant DNS records for IceWarp Server are listed in a while. You can click the *Domain Information* button to refresh the data. DNS records for SmartDiscover are located almost on the top of the list.

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 ActiveSync devices that do not allow custom server port setting.

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. IceWarp Server offers similar functionality to Exchange in this manner.

ActiveSync server is searching GAL items despite GAL folder presence in a client. This means that GAL contacts are offered as possible recipients when composing message on the client side.

What is GAL in IceWarp Server?

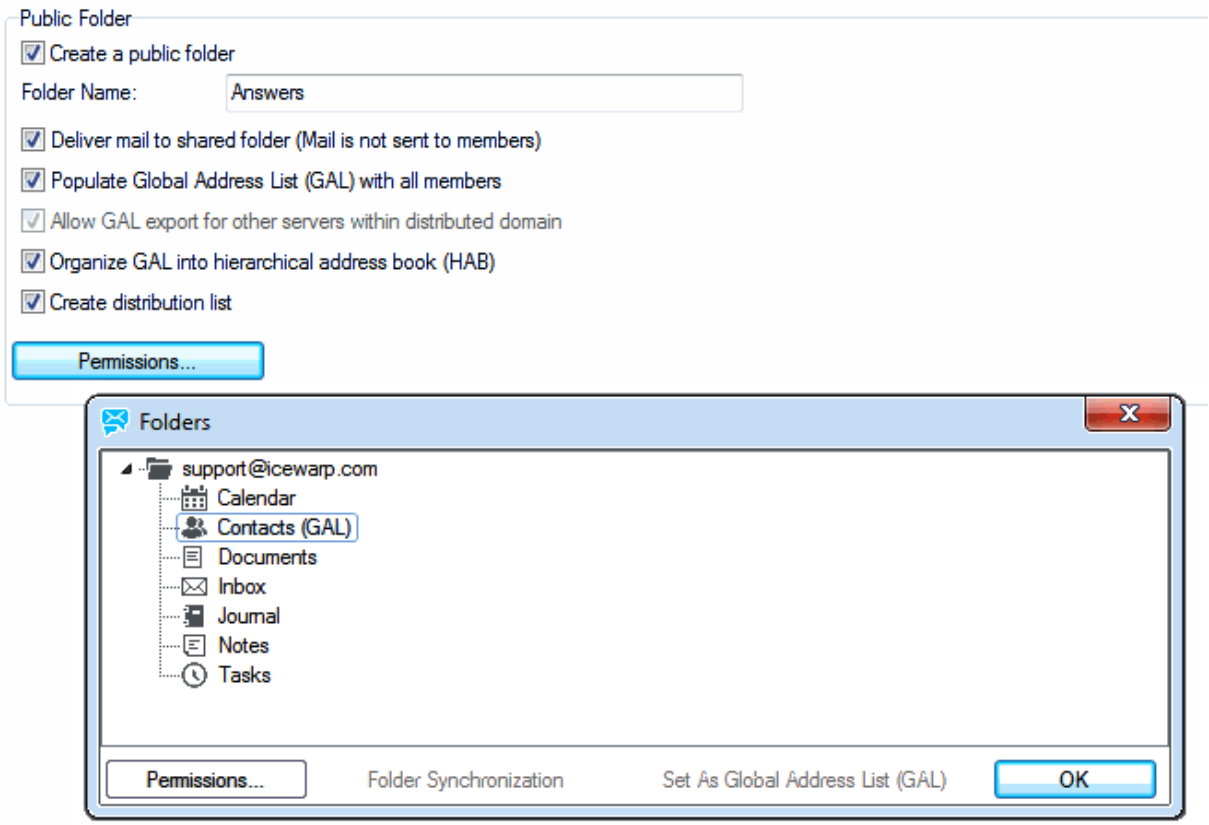
- GAL is any public contacts folder with a GAL flag
- GAL is automatically populated from a group's member list (nested groups are not included automatically)
- there can be multiple GAL folders (one for each public folder) and user can browse through all of them on Windows Mobile, iPhone or Blackberry, 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 in the form of distribution lists.

Creating GAL

Create a new group account (***Ctrl+G***), check the ***Create a public folder*** box and provide a name for this folder, then check the ***Populate GAL with all members*** box too. Switch to the ***Members*** tab, click ***Add...*** and select any account 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 (lr) is enough for GAL. You can also add a whole domain or group as a member. In the case you want to exclude some account from GAL, you can set its API variable – ***u_excludefromgal*** – to *true* (account API console – right click account/API).


Public Folder
Create a public folder
Folder Name:
Answers
Deliver mail to shared folder (Mail is not sent to members)
Populate Global Address List (GAL) with all members
Allow GAL export for other servers within distributed domain
Organize GAL into hierarchical address book (HAB)
Create distribution list
Permissions...
Folders
support@icewarp.com
Calendar
Contacts (GAL)
Documents
Inbox
Journal
Notes
Tasks
Permissions...
Folder Synchronization
Set As Global Address List (GAL)
OK

SmartSync

SmartSync functionality since IceWarp Server version 11.2.0:

If a client performs the request with a *synckey* that does not correspond to the one from the last server answer, we can expect a problematic item in the server answer. This leads to a creation of so called SmartSync set (i.e. a set of items sent in the previous answer) and SmartSync mode activation. In this mode, the server sends one SmartSync set item in each of answers until the whole set is sent. In the case the client request shows a problem with the last sent item, this item is not sent again. The server sends a virtual message (= it is not present in a mail storage) to Inbox. This message informs that the item was omitted from synchronization and server proceeds to processing of the next set item. After the set is emptied, the SmartSync mode is ended and synchronization continues as usually until another problem occurs.

Motivation for implementation improvement:

Outlook is sending Sync request for all folders at once without any filtering. This can halt synchronization completely (for all resources) even if there is only one problematic item (means Outlook is unable to parse it) included in the server response. In real life, it usually means that one invalid RFC822 formatted mail halts all synchronization! We had to find a way around this behavior.