

GO!NotifySync

Administrative Guide

For GO!NotifySync Version 4.11.x Software



Table of Contents

Welcome to GO!NotifySync	3
Requirements	4
Mail Server Specific Functionality	5
Licensing	7
Managing Users	8
Security	10
Data Encryption.....	10
Remote Device Wipe	11
Supported ActiveSync Protocol Security Policies	12
Device Password Requirement.....	12
Minimum Password Length.....	13
Alphanumeric Password Requirement	13
Inactivity Timeout	15
Maximum Failed Unlock Attempts	15
Device Encryption Requirement	16
Simple Password Permission	16
Password Expiration	16
Password History	17
Maximum Calendar Age Filter	17
Maximum Email Age Filter.....	17
HTML Email Permission	18
Enable Password Recovery.....	18
Autodiscover Service Configuration	19
The Autodiscover Process	19
Autodiscover Location Discovery.....	20
Connecting to the Autodiscover Service	20
Microsoft Exchange Autodiscover Configuration	24

Welcome to GO!NotifySync

About GO!NotifySync™ and this Guide

GO!NotifySync™ is a device client application for BlackBerry devices running operating system versions 4.5 – 7.1 that can synchronize email and PIM with mail servers that support the ActiveSync Exchange (EAS) protocol versions 2.5, 12.0, and 12.1.

This document provides administrators with an overview of GO!NotifySync, its requirements, and links to resources that may be helpful in supporting users of the product.

Requirements

Supported ActiveSync Servers

The *GO!NotifySync* device client synchronizes Email and PIM items with groupware servers supporting the Exchange ActiveSync® protocol.

Click here for a list of [supported groupware servers](#).

Note: If you are synchronizing with a Microsoft Exchange 2007 server that has been upgraded to Service Pack 1, please read the following [Knowledge Base article](#).

Device Software Requirements

BlackBerry operating system versions 4.5 – 7.1 are supported.

Port Requirements

GO!NotifySync uses the ActiveSync protocol for synchronization. If you already have users using ActiveSync with your mail server, such as those with Windows Mobile phones, no additional configuration should be necessary for *GO!NotifySync* to work.

For *GO!NotifySync*, ports 80 (HTTP) or 443 (HTTPS)* need to be open.

***SSL (HTTPS) Configuration**

An SSL certificate must be installed on the groupware server. Users may then select the **Use HTTPS** option when they register their device or enable it from the *GO!NotifySync Preferences* menu (Account Settings).

Mail Server Specific Functionality

Please reference the [GO!NotifySync release notes](#) for information on behavior specific to the host mail server. See the sections entitled:

- Using Microsoft Exchange 2013
- Using Microsoft Exchange 2010
- Using Microsoft Exchange 2007
- Using Microsoft Exchange 2003
- Using GroupWise 8.0.2 HP2 or HP3 with Novell Data Synchronizer
- Using Kerio Mail Server
- Using Zimbra
- Using CommuniGate Pro

Mail Server Resources

The following resources may be helpful with configuring the *ActiveSync* protocol:

AXIGEN:

http://www.axigen.com/knowledgebase/How-to-enable-ActiveSync-in-Axigen_277.html

CommuniGate Pro:

<http://www.communiGate.com/CommuniGatePro/AirSync.html>

EX 2013:

<http://technet.microsoft.com/en-us/library/aa998636.aspx>

EX 2010:

<http://technet.microsoft.com/en-us/library/bb124265.aspx>

EX 2007:

[http://technet.microsoft.com/en-us/library/aa998357\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998357(EXCHG.80).aspx)

EX 2003:

[http://technet.microsoft.com/en-us/library/bb123755\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/bb123755(EXCHG.65).aspx)

GroupWise with Novell Data Synchronizer

http://www.novell.com/documentation/datasynchronizer1/datasync1_install_dsgw/?page=/documentation/datasynchronizer1/datasync1_install_dsgw/data/ab32nt1.html

Kerio:

<http://www.kerio.com/manual/kms/en/chap-activesync.html>

Reference [Kerio MailServer Knowledgebase article #500](#) for instructions on how to configure the server to allow synchronization of “unsupported” devices on Kerio MailServer v6.6.0.

Zimbra:

http://wiki.zimbra.com/index.php?title=Moble_Device_Setup

Licensing

The GO!NotifySync Registration Server

The *GO!NotifySync* registration server maintains the total number of seats, the number of active seats and the number of available seats associated with the license issued to a company or service provider.

Device Registration

During registration end users must enter their email address. The email domain is used to obtain the *GO!NotifySync* product license key and the mail server address. Both the license key and the server address are used to validate the registration. The device sends the BlackBerry device PIN to the registration server where it is stored and used once a day to check that the device requesting a connection is associated with an authorized user.

Users may be required to enter a license key during registration if:

- multiple licenses with the same domain exist for the organization
- multiple users in the same organization are purchasing the application individually
- users are a part of an Internet mail domain such as gmail or yahoo

Users may be required to select a server during registration if there are multiple server configurations associated with the license.

Each user that registers a device activates a seat in the license. When a user is deactivated, a seat becomes available again.

See also [Managing Users: User Changes](#)

Managing Users

Adding Users

Users can download and install the *GO!NotifySync* software over-the-air. As long as seats associated with the license are available, a user may register a device with the license key and their mail server credentials.

Refer users to the [GO!NotifySync for BlackBerry](#) user guide for installation and registration instructions.

User Changes

If a user obtains a new device or is no longer using *GO!NotifySync*, his/her *GO!NotifySync* account must be deactivated so that the seat is made available for re-registration on another device or for redistribution to another user. Users can be deactivated from the following web site or by your sales representative.

To deactivate a user

1. Access the web page at www.notifysync.com/deactivate
2. Enter the **license key** (found in *Account Settings*) and the **device PIN** (found in *Device Info*) or the **username/domain** (found in *Account Settings*).
3. Click **Submit**.

Existing users who have obtained a new device

- *Deactivate the user's account as outlined above.* This frees up the license seat.
- Download and install *GO!NotifySync* on the new device and register it. The *GO!NotifySync* registration server will obtain the new device PIN.
- Uninstall *GO!NotifySync* from the first device. This removes the *GO!NotifySync* application and all the application data files.

Provision a device previously used for another *GO!NotifySync* account

- On the device, select the *GO!NotifySync* icon, then select *Preferences > Account Settings*.
- From the *Account Settings* menu, select *Delete Account*. This will delete the user account and remove any Email associated with it from the device.
- Reregister the device with the new user's information. During the registration process enable synchronization for Calendar, Contacts, Email, and Tasks. Enabling Calendar, Contacts, and Tasks will remove all old PIM data from the device and allow the new user's PIM data to load and synchronize.

User Preferences/Policies

Users may set options for customizing the functionality of *GO!NotifySync* through the *GO!NotifySync Preferences* menu on the device. Users should be instructed to set preferences so that they are in line with the policies outlined by their organization. Refer users to the [GO!NotifySync for BlackBerry](#) user guide for instructions on setting user preferences.

Policies set for devices using *ActiveSync* may not affect *GO!NotifySync* users. See [Supported ActiveSync Protocol Security Policies](#) for more information.

Users Can Backup the Preferences/Policies. If a user is changing devices, the preferences can be saved to a storage card and restored on a different device during its registration.

1. On the old device, open *GO!NotifySync* and press the menu button.
2. Select **Preferences > Account Settings**.
3. Press the menu button and select **Backup Configuration**.
4. Remove the storage card and insert it in the new device before you register the *GO!NotifySync* app on it.
5. At the first registration screen (on the new device), press the menu button and select **Restore Configuration**.

Security

Data Encryption

Encryption for Data-in-Motion

Data transferred between the server and devices can be encrypted using SSL (HTTPS).

1. Install an SSL certificate on the groupware server. The secure certificates listed below have been tested and confirmed to work with all supported *GO!NotifySync* devices.
 - [VeriSign/RSA Secure Server CA](#) “Secure Site” or “Secure Site Pro”
 - [Thawte Server CA](#) “SSL Web Server Certificate”

NOTE: You are required to have a domain name when purchasing an SSL certificate for your website. The domain name listed on the SSL certificate must match the domain name of the website you are using or the SSL handshake will fail. GPRS and CDMA BlackBerry devices are using a WAP gateway – the gateway determines which CA’s are trusted.

2. Have users enable SSL on their devices by checking the **Use HTTPS** box when they are registering or through the *Account Settings* on the *GO!NotifySync Preferences* menu.

Encryption for Data-at-Rest

Users can enable data-at-rest encryption for the email database on the device storage disk. This database contains all *GO!NotifySync* email data.

Through the *General Security* settings on the *GO!NotifySync Preferences* menu, users may set one of the following encryption levels:

- Secure (128-bit)
- More Secure (192-bit)
- Most Secure (256-bit)

NOTE: Higher levels of encryption are more processor intensive and some users may experience a slight delay (several seconds or less) while opening and closing email when using them.

Remote Device Wipe

Description

Remote device wipe is a feature that enables the administrator to issue a command, from the ActiveSync server to the GO!NotifySync user's device, to delete data the next time the device connects to the server. The feature is intended for use when a device is lost, stolen or otherwise compromised, or when a device must be reassigned to another user.

Function

When GO!NotifySync receives the remote wipe command through the ActiveSync protocol, from a Microsoft Exchange server, remote wipe removes the GO!NotifySync user account, all *GO!NotifySync* mail data, and all PIM data (calendar, contacts, tasks) from the device. It also wipes all data from the SD card.

Exceptions

Remote wipe commands sent from mail server systems that adhere to the supported ActiveSync protocol versions may function similarly. There are known exceptions, however, where remote wipe may not function to the extent described above. Other systems may not support the remote wipe feature at all. Consult the mail server documentation for further information.

- On **Kerio MailServers**, remote wipe does not function to the full extent as described above. Issuing a *Remote Wipe* from the Kerio mail server will wipe only email and PIM data from the device.
- **Zimbra Collaboration Suite** does not support the *Remote Wipe* feature.

The following resources may be helpful:

Microsoft Exchange Server 2013 / 2010

<http://technet.microsoft.com/en-us/library/bb124591.aspx>

Microsoft Exchange Server 2007:

<http://technet.microsoft.com/en-us/library/aa998614.aspx><http://technet.microsoft.com/en-us/library/aa998614.aspx>

Microsoft Exchange Server 2003 SP2:

http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfp_8.msp

[http://technet.microsoft.com/en-us/library/aa995996\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/aa995996(EXCHG.65).aspx)

<http://technet.microsoft.com/en-us/magazine/2006.01.staybetterconnected.aspx>

Kerio:

<http://www.kerio.com/manual/kms/en/sect-activewipe.html>

Supported ActiveSync Protocol Security Policies

The Microsoft ActiveSync protocol provides a way in which server-defined security policies may be applied to a device client. This section lists the policy settings that can be applied to *GO!NotifySync* devices via the ActiveSync protocol.

Microsoft Exchange Server 2010/2007

- Device Password Requirement
- Minimum Password Length
- Alphanumeric Password Requirement
- Inactivity Timeout
- Maximum Failed Unlock Attempts
- Device Encryption Requirement
- Simple Password Permission
- Password Expiration
- Password History
- Maximum Calendar Age Filter
- Maximum Email Age Filter
- HTML Email Permission
- Enable Password Recovery

Microsoft Exchange Server 2003

- Device Password Requirement
- Minimum Password Length
- Alphanumeric Password Requirement
- Inactivity Timeout
- Maximum Failed Unlock Attempts

Device Password Requirement

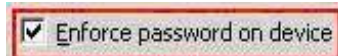
Supported On:

Setting Label

Exchange Server 2010/2007



Exchange Server 2003



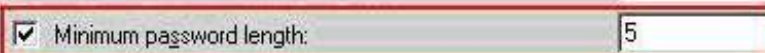
The **Require Password** (2010/2007) and **Enforce password on device** (2003) settings specify whether or not the device is required to enforce a security password. In *GO!NotifySync*, the security password is used for two purposes: To access security option menus, and to dismiss the **Inactivity Timeout** pop-up dialog (see Section 3.2.8). When enabled, the device client is required to use a password which respects the enforced password strength (see Section 3.2.2) and minimum length (see Section 3.2.7) requirements. If such a password has not already been created, a pop-up window will display, prompting the user to create a sufficient password.

When the setting is disabled on the server, *GO!NotifySync* will permit the user to create a password of any length between zero (0) and twenty (20) characters. If the setting is disabled after having previously been enabled, any existing password will not be affected.

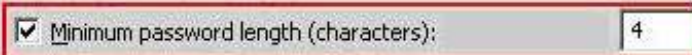
Minimum Password Length

Supported On:	Setting Label
---------------	---------------

Exchange Server 2010/2007



Exchange Server 2003



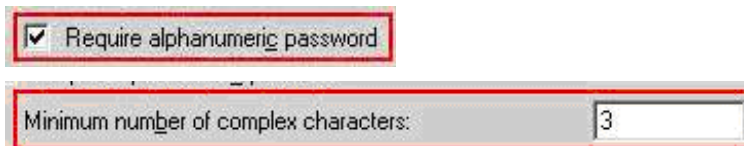
The **Minimum password length** setting specifies the minimum number of characters a device security password must contain. When enabled, the device client is required to use a password which contains a minimum of the number characters specified by the server. If the current device password does not meet the requirement, a pop-up dialog will display, prompting the user to create a sufficient password.

When the setting is disabled, the required minimum password length enforced by GO!NotifySync depends on whether or not the server requires the device client to use a security password. If the server requires the use of a security password, the device client will, by default, enforce a minimum password length of eight (8) characters. If the server does not require the use of a security password, the device client will not enforce a minimum length requirement.

Alphanumeric Password Requirement

Supported On:	Setting Label
---------------	---------------

Exchange Server 2010/2007



Exchange Server 2003



The **Require alphanumeric password** (2010/2007) and **Require both numbers and letters** (2003) settings specify whether or not the device password should consist of letters, numbers, and special characters. When enabled, the device client is required to use a “Strong Alphanumeric” password, which consists of lowercase letters, uppercase letters, numerals, and special characters (@, #, &, etc.). Collectively, these four character types are known as **complex characters**.

Exchange Server 2010/2007 has a **Minimum number of complex characters** setting which allows you to choose the number of each type of complex character which must exist in an alphanumeric device password. For example, if the minimum complex character requirement is two (2), the user will be required to create a password containing at least two (2) lowercase letters, at least two (2) uppercase letters, at least two (2) numerals, and at least two (2) special characters.

Exchange Server 2003 enforces a minimum complex character requirement of three (3). This means that the user will be required to create a password containing at least three (3) lowercase letters, at least three (3) uppercase letters, at least three (3) numerals, and at least three (3) special characters.

The one exception to this rule is in the case of when the minimum password length is less than the minimum complex character requirement multiplied by the number of complex character types. In this case, the user need only create a password with an even distribution of the complex character types that meets the minimum length.

For example, if a minimum complex character requirement of three (3) is enforced, the password will need to be at least twelve (12) characters long (3 complex characters * 4 complex character types). However, if the minimum password length is nine (9), then the user need only enter a nine-character password containing an even distribution of the complex character types. The following complex character combinations would be considered valid in this scenario:

- 3 lowercase letters, 2 uppercase letters, 2 numerals, 2 special symbols
- 2 lowercase letters, 3 uppercase letters, 2 numerals, 2 special symbols
- 2 lowercase letters, 2 uppercase letters, 3 numerals, 2 special symbols
- 2 lowercase letters, 2 uppercase letters, 2 numerals, 3 special symbols

The following complex character combinations would be considered **invalid** in this scenario, as the character types are unevenly distributed:

- 1 lowercase letter, 3 uppercase letters, 3 numerals, 2 special symbols
- 5 lowercase letters, 0 uppercase letters, 2 numerals, 2 special symbols
- 1 lowercase letter, 1 uppercase letter, 1 numeral, 6 special symbols

To further illustrate this concept, the following table provides examples of valid passwords given a minimum complex character requirement and minimum password length:

Alphanumeric Password Examples

Min. Length	Min. Comp. Chars.	Valid Password Examples
5	2	aA1!b , 7%o\$Y , 12aB# , @1AbC
10	2	aA1!bB2@cc , aaAA11!!23 , j0%73bY@Qk
15	2	aA1!bB2@cccccc , 1111111a!A1b@B2 , aaAA11!!123abc?
15	3	aA1!bB2@cC3#ddd , abcABC123!@#efg

Notice that if the minimum length exceeds the complex character requirement multiplied by the number of complex character types, the password may contain any sequence of characters in any order regardless of repetition as long as the requirement rule is met.

Inactivity Timeout

Supported On:	Setting Label
Exchange Server 2010	Maximum inactivity time lock

Exchange Server 2007



A screenshot of the Exchange Server 2007 configuration interface. It shows a checkbox that is checked, followed by the text "Time without user input before password must be re-entered (in minutes):". To the right of this text is a text input field containing the number "10". The entire control is enclosed in a red rectangular border.

Exchange Server 2003



A screenshot of the Exchange Server 2003 configuration interface. It shows a checkbox that is checked, followed by the text "Inactivity time (minutes):". To the right of this text is a text input field containing the number "5". The entire control is enclosed in a red rectangular border.


These settings specify whether or not the device client should lock the user interface after a number of minutes of inactivity. When enabled, if the user does not use the device within the specified time interval, a pop-up dialog will display, prompting the user for the security password. The dialog will remain on-screen and prohibit access to the user interface until the security password is entered correctly.

If this setting is enabled on the server, the user will be prohibited from editing all **Inactivity Timeout** options on the device client. If this setting is disabled on the server, all **Inactivity Timeout** options on the device client will be made editable to the user. If this setting is disabled on the server after having been previously enabled, the device client will automatically deactivate **Inactivity Timeout**.

Maximum Failed Unlock Attempts

Supported On:	Setting Label
Exchange Server 2010	Maximum failed password attempts

Exchange Server 2007



A screenshot of the Exchange Server 2007 configuration interface. It shows a checkbox that is checked, followed by the text "Number of failed attempts allowed:". To the right of this text is a text input field containing the number "5". The entire control is enclosed in a red rectangular border.

Exchange Server 2003



A screenshot of the Exchange Server 2003 configuration interface. It shows a checkbox that is checked, followed by the text "Wipe device after failed (attempts):". To the right of this text is a text input field containing the number "8". The entire control is enclosed in a red rectangular border.

These settings work in conjunction with **Inactivity Timeout**. The setting specifies whether or not all GO!NotifySync device databases and SD card data should be erased after a number of failed security password entry attempts. Without the enforcement of this setting, there is no limit to the number of times a user may enter the security password incorrectly.

If this setting is enabled on the server, the user will be prohibited from editing all **Wipe on Failed Unlock** options on the device client. In addition, if **Password Echo** is enabled on the device with an enforced value greater than or equal to that of **Wipe on Failed Unlock**, the enforced **Password Echo** value will be set to one unit less than the enforced **Wipe on Failed Unlock** value. For example, if the enforced **Password Echo** value is 11, and the enforced **Wipe on Failed Unlock** value is 10, the enforced **Password Echo** value will be changed to 9.

If this setting is disabled on the server, all **Wipe on Failed Unlock** options on the device client will be made editable to the user. If this setting is disabled on the server after having been previously enabled, the device client will automatically deactivate **Wipe on Failed Unlock**.

Device Encryption Requirement

Supported On:

Exchange Server 2010/2007

Setting Label



The **Require encryption on the device** setting determines whether or not all GO!NotifySync databases on the device are to be encrypted. When enforced, the device client prohibits the user from disabling encryption. In addition, if encryption was not enabled prior to enforcement, 192-bit encryption is automatically enabled. If encryption was enabled prior to enforcement, the current encryption option will remain intact.

When the setting is disabled on the server, the user is free to select any encryption algorithm, or disable encryption altogether. If the setting is disabled on the server after having been previously enabled, the current encryption option will remain intact.

Simple Password Permission

Supported On:

Exchange Server 2010/2007

Setting Label



Allow simple password is a setting which works in conjunction with numeric password enforcement. The setting determines whether or not the device password may consist of a simple pattern, such as "1111" or "1234". When enabled, the user is permitted to use a simple numeric device password. If disabled, the user is prohibited from doing so, and will be required to change the device password if the current password meets the criteria for simplicity.

Password Expiration

Supported On:

Exchange Server 2010/2007

Setting Label



The **Password expiration** setting specifies whether or not device passwords are to expire after a number of days. When enforced, once the expiration interval has passed, the device client will display a pop-up dialog, prompting the user to create a new password.


If this setting is enabled on the server, the user will be prohibited from editing all **Password Expiration** options on the device client. If this setting is disabled on the server, all **Password Expiration** options on the device client will be made editable to the user. If this setting is disabled on the server after having been previously enabled, the device client will automatically deactivate **Password Expiration**.

Password History

Supported On:

Exchange Server 2010/2007

Setting Label



Enforce password history: 4

The **Enforce password history** setting specifies how many previously-used passwords the device client is to remember. When enforced, the user is prohibited from using any passwords which are stored in password history memory. If this setting is enabled on the server, the user will be prohibited from editing all **Password History** options on the device client. If this setting is disabled on the server, all **Password History** options on the device client will be made editable to the user. If this setting is disabled on the server after having been previously enabled, the device client will automatically deactivate **Password History**.

Maximum Calendar Age Filter

Supported On:

Exchange Server 2010/2007

Setting Label



Include past calendar items: All

The **Include past calendar items** setting specifies the maximum age to which the user may set the calendar event age filter on the device client. If a maximum age is set on the server, the user will be prohibited from choosing a setting that allows the synchronization of calendar items older than this maximum.

Maximum Email Age Filter

Supported On:

Exchange Server 2010/2007

Setting Label



Include past e-mail items: All

The **Include past e-mail items** setting specifies the maximum age to which the user may set the email message age filter on the device client. If a maximum age is set on the server, the user will be prohibited from choosing a setting that allows the synchronization of email items older than this maximum.

HTML Email Permission

Supported On:

Exchange Server 2010/2007

Setting Label



The **Allow HTML formatted e-mail** setting specifies whether or not the device client is permitted to receive email messages in HTML format. When enabled, the user can choose between receiving email in Text and HTML formats on the device client. If disabled, the device client receives email in Text format only.

Enable Password Recovery

Supported On:

Exchange Server 2010/2007

Setting Label

Enable Password Recovery

This option enables password recovery for the mobile device. Users can generate a temporary recovery password from the device if they have forgotten its unlock password. They can look up the recovery password using Outlook Web Access (OWA). In addition, an administrator can look up the recovery password via the Exchange Management Console (EMC).

This feature requires ActiveSync protocol version 12.0 or 12.1.

To enable this feature in Exchange

From the EMC, select the **Client Access** node under **Organization Configuration** in the navigation tree. Right click on the policy and choose **Properties**, then choose the **Password** tab. Check the **Enable Password Recovery** option.

Autodiscover Service Configuration

What is Autodiscover

Autodiscover is a technology that allows clients to discover services automatically without having to know the exact location of the server hosting the services. The *Microsoft Exchange Server* Autodiscover feature supports discovery for a number of services including the ActiveSync server address and is generally available in the default installation of Exchange 2013/2010/2007.

GO!NotifySync uses Autodiscover to automatically find the ActiveSync server address so that users do not have to manually enter it during the *GO!NotifySync* registration process.

Benefits

Autodiscover has been incorporated into the *GO!NotifySync* registration process in order to provide a more streamline experience for end users as they configure a *GO!NotifySync* user account on the device. The goal for the Autodiscover feature is to automatically determine a user's ActiveSync server address given the user's email address and ActiveSync account credentials. In this way, the burden of knowing or obtaining the ActiveSync server address is removed from the end user.

The Autodiscover Process

There are two steps to the Autodiscover process. The first step consists of finding the Autodiscover service and the second step includes querying the Autodiscover service for the desired services. Since Microsoft Exchange is the Autodiscover service as well as the ActiveSync server, the Autodiscover process consists of the device first connecting to the Autodiscover service to submit the query for the ActiveSync server address and then using the ActiveSync server address for all future communication with the server.

Multiple connections are used (as opposed to just generating the ActiveSync server address based on the email address domain) because it is often required that a very specific server address value is used when using SSL to protect communication between the device and the ActiveSync server. This server address may not always match the email address domain, which would make it impossible for the device to locate the server automatically.

Autodiscover Location Discovery

GO!NotifySync uses the email address domain to try to determine the location of the Autodiscover service. Possible URLs are generated using the email domain from the email address entered in the first step of the GO!NotifySync registration process. The URLs generated depend on the Autodiscover method used for the connection attempts. See Section 2.2: *Connecting to the Autodiscover service* for details on the two different Autodiscover methods.

Direct Connection Generated Autodiscover URLs

1. <https://DOMAIN/Autodiscover/Autodiscover.xml>
2. <https://autodiscover.DOMAIN/Autodiscover/Autodiscover.xml>

Where “DOMAIN” is the domain from the email address entered.

Indirect Connection Generated Autodiscover URLs

1. <http://DOMAIN/Autodiscover/Autodiscover.xml>
2. <http://autodiscover.DOMAIN/Autodiscover/Autodiscover.xml>

Where “DOMAIN” is the domain from the email address entered.

Connecting to the Autodiscover Service

GO!NotifySync uses two different methods of connecting to the Autodiscover service. The Direct Connection method is attempted first and the Indirect Connection method is used if the Direct Connection method is unsuccessful. User authentication credentials entered during the first step of the GO!NotifySync registration process are used when querying the Autodiscover service for the ActiveSync server address.

Direct (Single) Connection Method

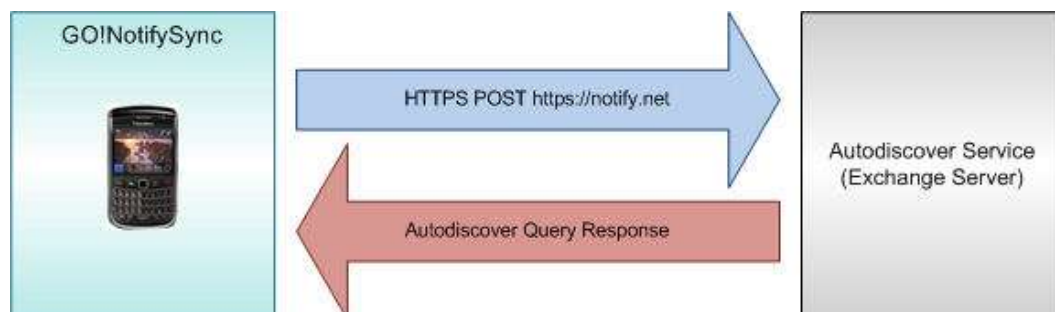
The direct connection method is used in a single-server environment where all ActiveSync users use the same URL to connect to the ActiveSync server. If the email domain matches the external address of the server (see example 1) no additional network configuration is required. If the email domain does not match the external address of the server (see example 2) you need to configure your network so that GO!NotifySync can properly find the Autodiscover service. A domain or subdomain must be configured to match one of the URLs that the device generates from the email address domain (identified in section 2.1.1).

GO!NotifySync connects to the Autodiscover service sending the query for the ActiveSync server address and expects the Autodiscover query response in return. The connection is over HTTPS using an HTTP POST request to the generated Autodiscover service URLs (identified in section 2.1.1).

Example 1: Exchange Server Address Matches Email Domain

Exchange Server Address: notify.net

ActiveSync User Email Address: user@notify.net

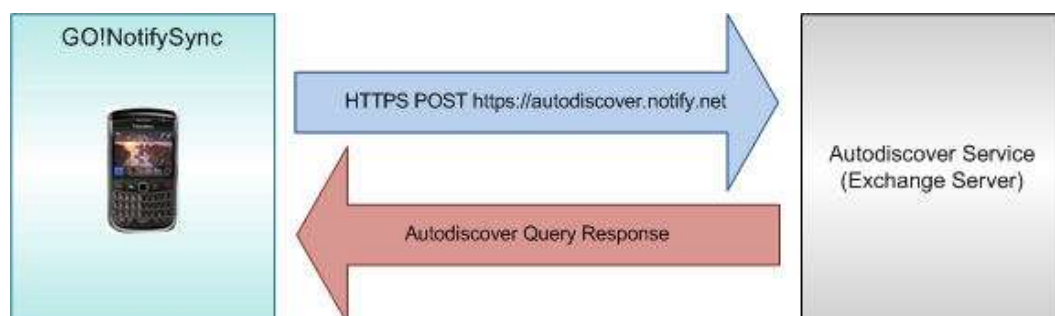


No network configuration is required in order for GO!NotifySync to find the Autodiscover service using the URLs generated from the email domain (identified in section 2.1.1).

Example 2: Exchange Server Address Does Not Match Email Domain

Exchange Server Address: eas.notify.net

ActiveSync User Email Address: user@notify.net



Network configuration is required so that "autodiscover.notify.net" resolves to the same location as "eas.notify.net". This will make it possible for GO!NotifySync to find the Autodiscover service using the URLs generated from the email domain (identified in section 2.1.1).

Indirect (Multiple) Connection Method

The indirect connection method can be used in environments with multiple Exchange servers. An independent web service is used to redirect Autodiscover requests to the appropriate Autodiscover service, usually based on the user credentials. The address of the independent web service must match one of the URLs generated from the email address entered in the first step of the GO!NotifySync registration process (identified in section 2.1.2).

Two transactions are required to locate the Autodiscover service using this method. GO!NotifySync connects over HTTP using an HTTP GET request to the generated Autodiscover service URLs expecting an HTTP redirect response. The location specified in the redirect response is assumed to be the Autodiscover service. GO!NotifySync uses the Direct Connection method for the second transaction using the location specified in the redirect response. See section 2.2.1 for details on the Direct Connection method.

Example: Multiple Users and Multiple Exchange Servers

Independent Web Service Address: autodiscover.notify.net

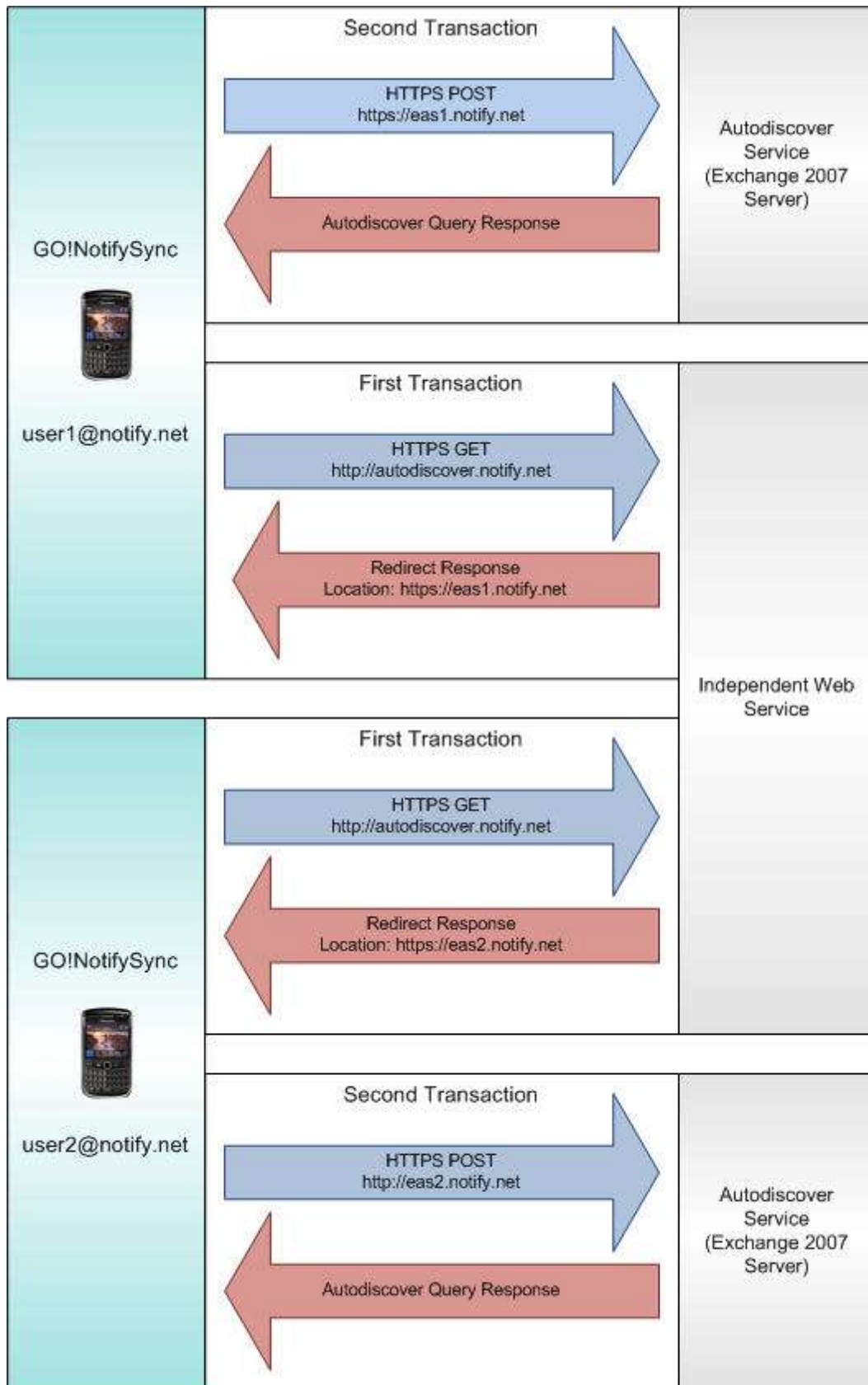
Exchange Server 1 Address: eas1.notify.net

Exchange Server 2 Address: eas2.notify.net

ActiveSync User 1 Email Address: user1@notify.net

ActiveSync User 2 Email Address: user2@notify.net

The independent web service returns a redirect response, redirecting *GO!NotifySync* to one of the Autodiscover services to allow *GO!NotifySync* to complete the Autodiscover query.



Microsoft Exchange Autodiscover Configuration

The Autodiscover service is usually enabled in a default installation of Exchange 2013, 2010, or 2007. However, you must configure the service so that it can send the ActiveSync server address in the Autodiscover response. Reference the Microsoft TechNet articles listed below for instructions on how to do this.

Managing the Autodiscover Service 2013 / 2010

<http://technet.microsoft.com/en-us/library/bb124251.aspx>

Managing the Autodiscover Service 2007

<http://technet.microsoft.com/en-us/library/aa995956.aspx>

<http://technet.microsoft.com/en-us/library/aa998277.aspx>

Additional Reference:

[MS-OXDISCO]: Autodiscover HTTP Service Protocol Specification

Version 2.0

<http://msdn.microsoft.com/en-us/library/cc307725.aspx>

[MS-ASCMD]: ActiveSync Command Reference Protocol Specification

Version 1.02

<http://msdn.microsoft.com/en-us/library/cc307725.aspx>