GO!NotifyLink

Enterprise Server System Security Guide

The goal of this document is twofold.

First, it will provide an understanding of the layers of security built into the GO!NotifyLink system. These layers ensure the confidentiality and integrity of wirelessly transmitted information from behind the firewall to wireless devices in the field.

Second, the document includes administrative guidelines for implementing or modifying settings governing the security measures that shield both servers and mobile wireless devices.

Securing Your Valuable Corporate Data

Mobile devices are capable of giving users real-time access to corporate information. The wireless handheld has become a type of mobile computing device and should be treated as such in your security policy. Since losing a phone can be as problematic as losing a laptop, efforts should be made to educate corporate employees in the proper use of mobile phones in regard to security.

GO!NotifyLink strives to give the IT professional the tools needed to insure that mobile devices in the enterprise meet the stipulations of your corporate security policy.

Table of Contents

Architecture

The *GO!NotifyLink Enterprise Server* (GO!NLES) is comprised of three components. These components exist for a *GO!NotifyLink On-Premise* system and apply to the *GO!NotifyLink On-Demand* system as well.

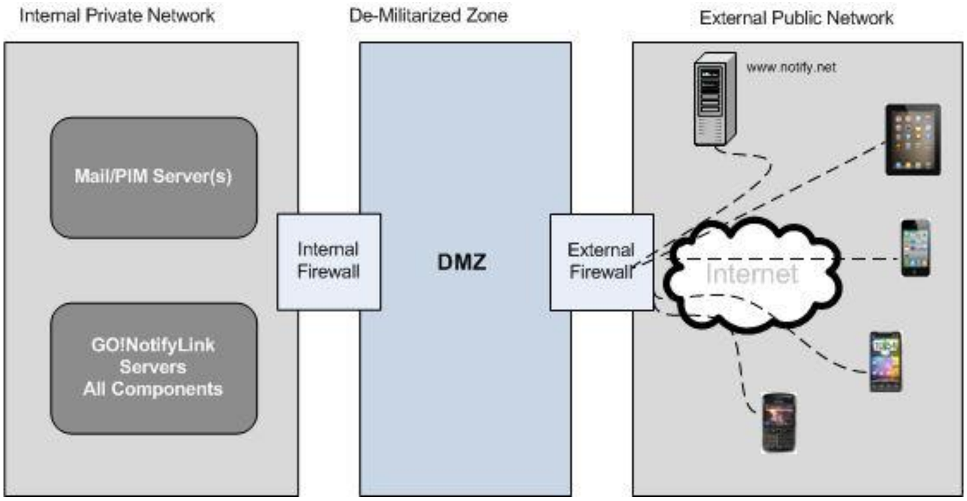
1. **HTTP(s)/Web Component** - Used for product key registration and validation and administration and user management webs.
2. **Database Component** – Relational databases used for storing administration information along with user information like filters, message formats, etc. Presently, this is Microsoft SQL Server 2000, 2005, and 2008.
3. **Messaging Engines Component** – Interfaces to Email and PIM (calendar, contacts and tasks). Includes messaging engines as well as support engines for leasing, monitoring, etc.

All three components may be installed on the same server or each component can be installed on a separate server. The architecture you choose will depend on system size and complexity.

Network Configuration Scenarios

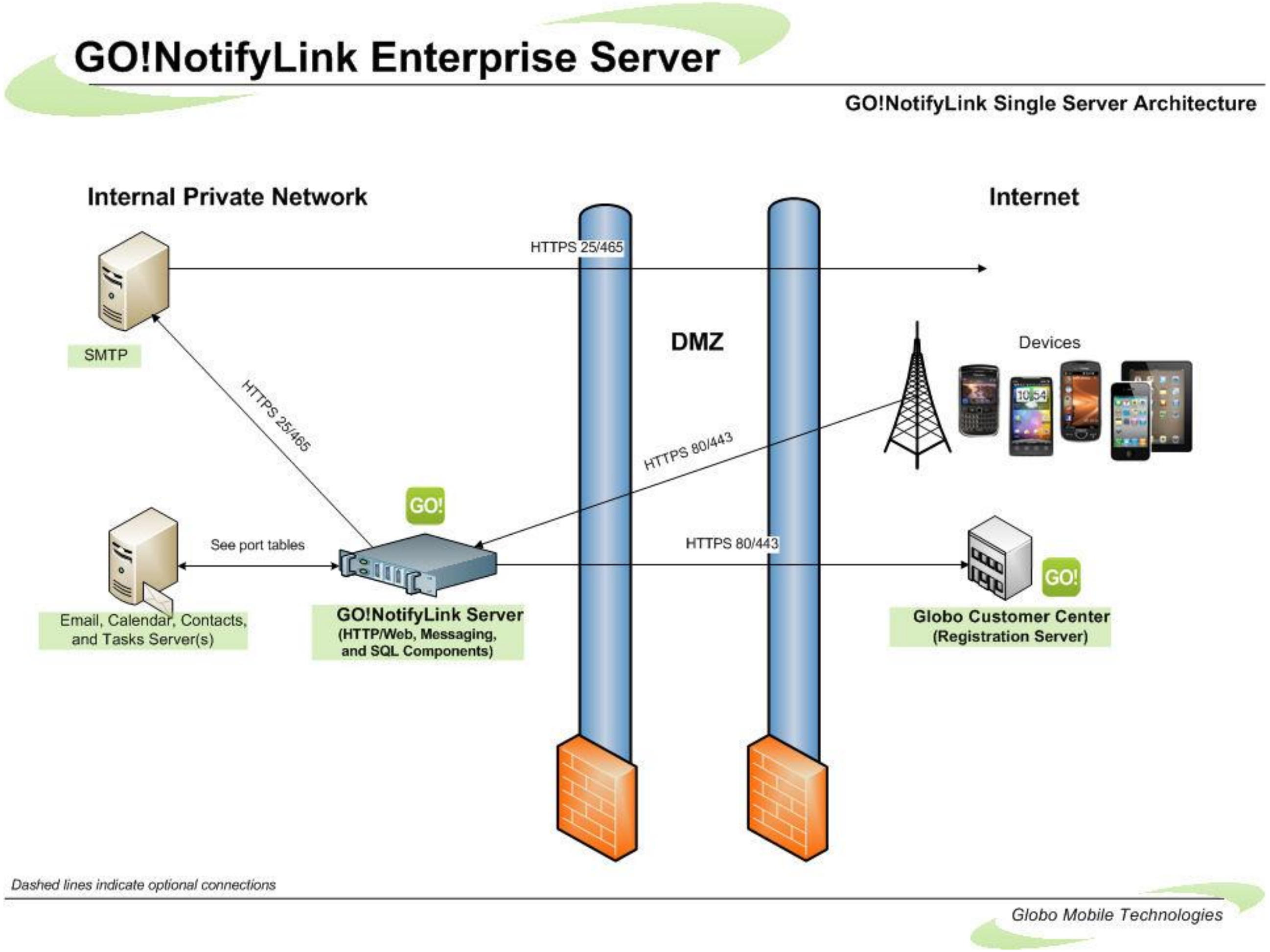
Several configuration scenarios are supported which gives the user some flexibility in choosing a method of deployment.

Single Server – This is the simplest installation scenario. All three components of *GO!NotifyLink* reside on a single server.   However, because the individual components of *GO!NotifyLink* have varying resource requirements, you must choose a server that meets the resource requirements of all three components.

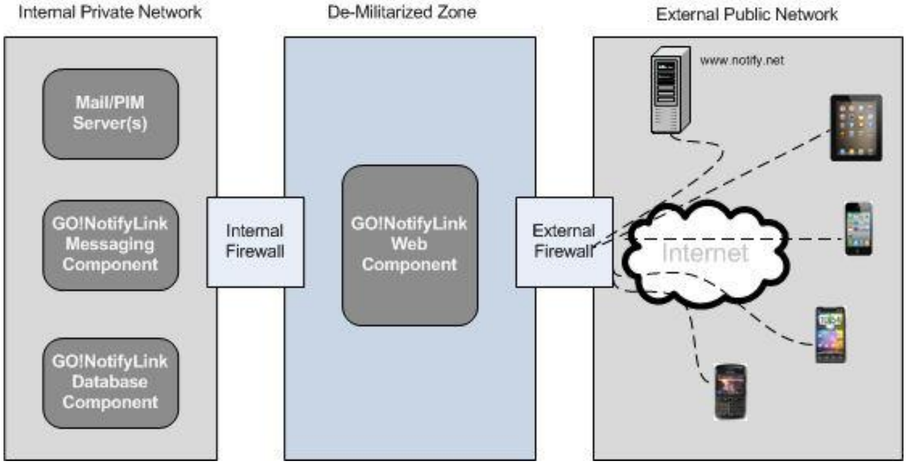


Single Server Configuration Diagram

Typical configuration suitable for general-purpose deployment where a single server meets all the requirements needed for installation.

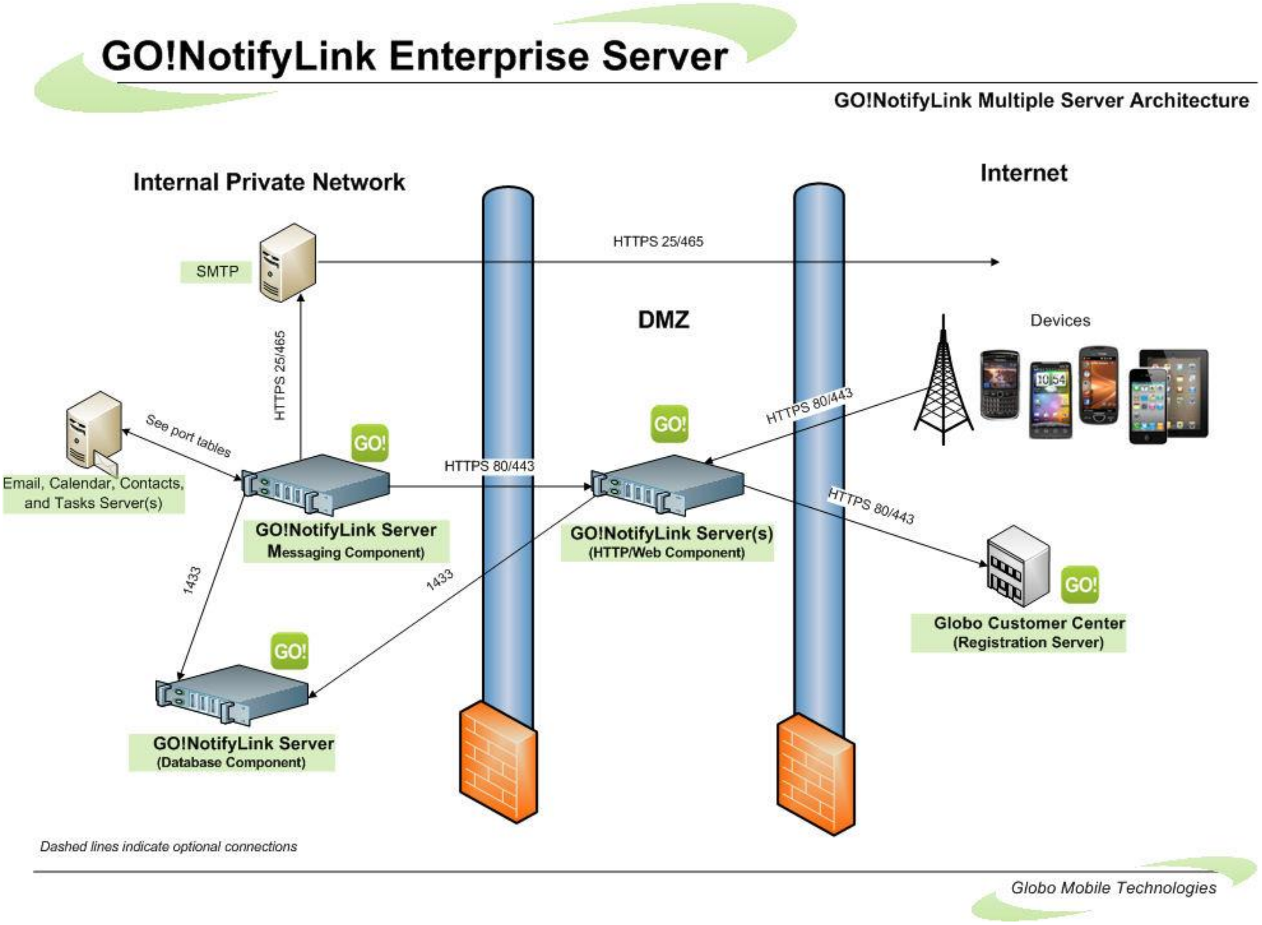

GO!NotifyLink Enterprise Server
GO!NotifyLink Single Server Architecture
Internal Private Network
Internet
HTTPS 25/465
SMTP
DMZ
Devices
HTTPS 25/465
HTTPS 80/443
GO!
See port tables
HTTPS 80/443
Email, Calendar, Contacts, and Tasks Server(s)
GO!NotifyLink Server (HTTP/Web, Messaging, and SQL Components)
GO!
Globo Customer Center (Registration Server)
Dashed lines indicate optional connections
Globo Mobile Technologies

Multiple Server – The Multiple Server installation configuration makes for a more flexible deployment, allowing each of the GO!NotifyLink components to be installed onto servers configured specifically for that component. Each component can be installed to either a pre-existing server (SQL or IIS based) without further configuration needed, or to servers configured for the individual component. This is particularly useful in deployments where a single server cannot meet all the requirements for each of the GO!NotifyLink components.



Multiple Server Configuration Diagram

Deployment options for larger more complex deployments where a single server does not meet all the requirements needed for installation.


GO!NotifyLink Enterprise Server
GO!NotifyLink Multiple Server Architecture
Internal Private Network
Internet
SMTP
HTTPS 25/465
HTTPS 25/465
DMZ
Devices
See port tables
Email, Calendar, Contacts, and Tasks Server(s)
GO!
HTTPS 80/443
HTTPS 80/443
HTTPS 80/443
GO!NotifyLink Server Messaging Component)
GO!NotifyLink Server(s) (HTTP/Web Component)
1433
1433
Globo Customer Center (Registration Server)
GO!NotifyLink Server (Database Component)
Dashed lines indicate optional connections
Globo Mobile Technologies

The Secure Layers

To simplify a description of the *GO!NotifyLink Enterprise* security system, we have grouped the security features into several categories, which we refer to as the “layers” of security.

- Message Content Security
- Server to Server Communication Security
- Database Security: Data-at-Rest Encryption
- Device to Web/Http Server Authentication
- Device Security
- Server Log File Security

Message Content Security

Whether information originates on the device or server, *GO!NotifyLink* transmits “data-in-motion” in an encrypted tunnel so it is secure in transit.

AES / TDES Encryption *GO!NotifyLink Enterprise Server (GO!NLES)* supports Triple Data Encryption Standard (TDES) and Advanced Encryption Standard (AES) algorithms for encrypting message content delivered from GO!NLES to wireless devices. Since *GO!NotifyLink* supports both protocols, it is up to the administrator to choose which is used.

Each unique user encryption key is 256 bits in size and is shared by the server and device. The key can be set by the administrator, the end user (if *IT Policy* permissions are granted), or can be generated randomly. It can be sent over the air.

Every message retrieved from the mail server is encrypted behind the corporate firewall and decrypted only when it reaches the correct handheld. The reverse process is true as well. When information originates on the device (replies, changes, new information), it is encrypted before leaving the device and decrypted at the *GO!NotifyLink Enterprise Server*.

SSL Encryption Additionally, communication between the *GO!NotifyLink* Web/Http server and the device can be encrypted using SSL (HTTPS) to protect messages traveling over the Internet, thus providing a second layer of security for data-in-motion.

Implementation Guidelines: Message Content

1. Encryption Settings

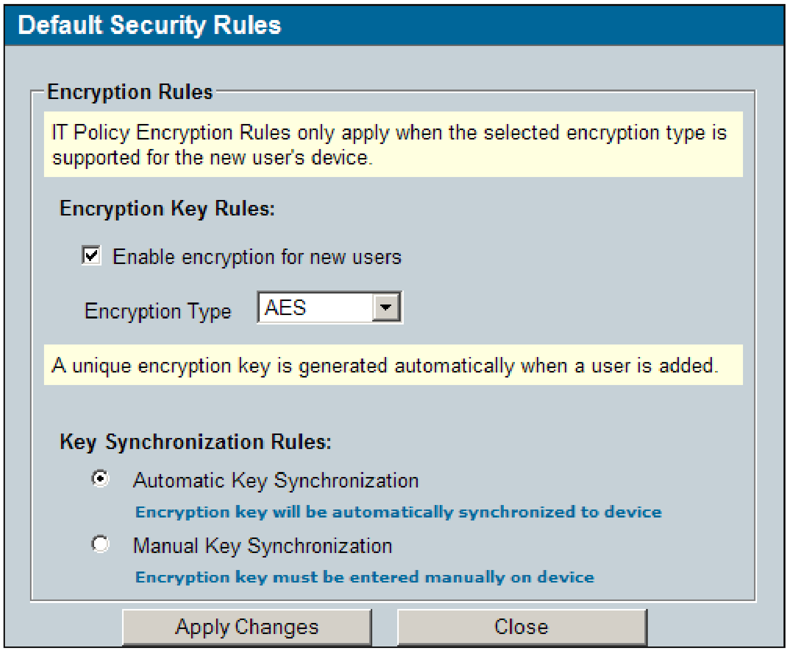
Encryption protocol for message content is set via the Administrative Web console on the *Default Security Rules* page shown below.

After installing *GO!NotifyLink Enterprise Server* components and before adding user accounts, access the Administrative Web console to set these Security parameters:

-Select ***IT Policy Management*** > select a policy and click the ***Edit IT Policy*** button > ***Security Rules***

- Enable encryption settings for new users
- Select the encryption algorithm type (AES or TDES)

An encryption key will be automatically generated for each new user added to the system. Keep in mind that the global encryption type you choose will only apply if a user's device supports the protocol. The setting can be individualized for a user whose device does not support the global encryption type. (From the admin web, select *User Administration* > select a user and click the *Edit User Policy* button > *Security Rules*.)



Default Security Rules

Encryption Rules

IT Policy Encryption Rules only apply when the selected encryption type is supported for the new user's device.

Encryption Key Rules:

☑ Enable encryption for new users

Encryption Type: AES

A unique encryption key is generated automatically when a user is added.

Key Synchronization Rules:

● Automatic Key Synchronization

Encryption key will be automatically synchronized to device

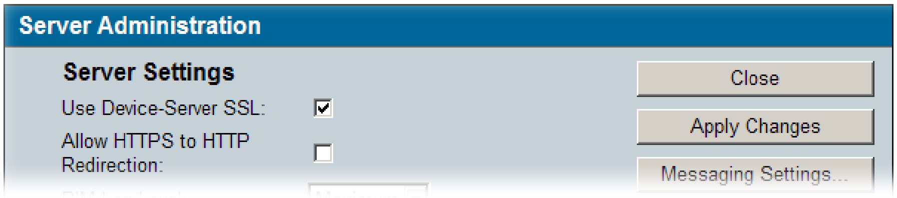
○ Manual Key Synchronization

Encryption key must be entered manually on device

AES vs. TDES Triple DES was the standard FIPS compliant encryption algorithm until 2001. Then the AES encryption algorithm became the standard. GO!NotifyLink supports both protocols and each is an effective encryption method for protecting information in transit. Government grade security is available, however, by implementing the National Institute of Standards and Technology (NIST) FIPS compliant AES encryption algorithm.

2. Enabling SSL

Enable SSL for device to Web/Http server communication.



Server Settings

Use Device-Server SSL: ☑

Allow HTTPS to HTTP Redirection: □

-Select ***Server Administration***

- Check the ***Use Device-Server SSL*** box.

-Install an SSL certificate on your Web/Http server and enable SSL in IIS/Apache.

-Instruct users, whose device O/S supports SSL, to enable it.

- On the device: ***GO!NotifyLink Preferences*** > ***Account Settings***

Server to Server Communication Security

GO!NotifyLink Messaging Component to Mail/PIM Servers

GO!NotifyLink's messaging engines can access email and PIM in a secure manner using Secure Socket Layers (SSL) or Transport Layer Security (TLS) if the mail server supports it.

GO!NotifyLink Web/Http Component to Registration Servers

GO!NotifyLink's Web/Http component will communicate to the GO!NotifyLink product key registration server using Secure Socket Layers (SSL). Communication between these servers occurs when license keys are added, when users are added, or when users are deleted.

Implementation Guidelines: Server to Server

GO!NotifyLink Messaging Component to Mail/PIM Servers

SSL/TLS use for communication between the GO!NotifyLink Messaging component and your mail server is enabled on Edit Mail Protocol page via the Administrative Web console as shown below.

Mail Servers

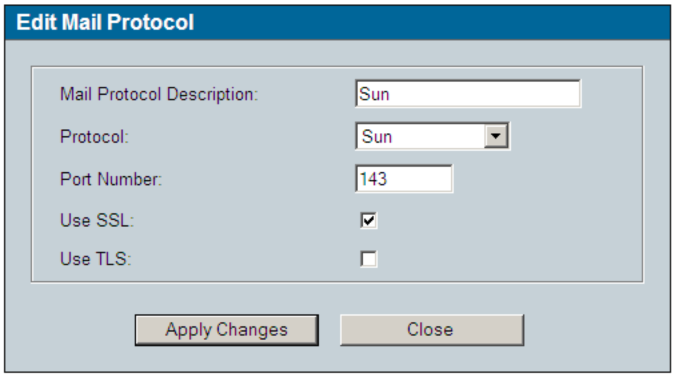
-Select *Server Administration* > *Mail Servers*

-Highlight the server you are using and click *Edit Mail Protocols*

-Highlight the protocol you wish to use and click *Edit Mail Protocol*

-Check the box beside *Use SSL* or *Use TLS*

-Install an SSL certificate on your mail server and enable SSL in IIS/Apache.



Mail Protocol Description: Sun

Protocol: Sun

Port Number: 143

Use SSL: ☑

Use TLS: ☐

PIM Servers

-Select ***Server Administration*** > ***PIM Servers***

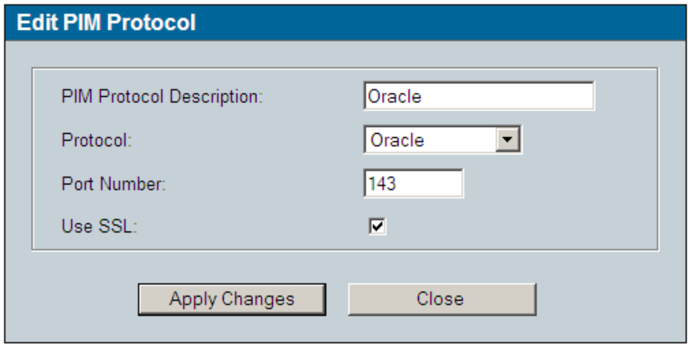
-Highlight the server you are using and click ***Edit PIM Protocols***

-Highlight the protocol you wish to use and click ***Edit PIM Protocol***

-Check the box beside ***Use SSL***

- Install an SSL certificate on your PIM server and enable SSL in IIS/Apache.

Note: *Some collaboration suite software use proprietary encryption protocols and do not require SSL*



PIM Protocol Description: Oracle

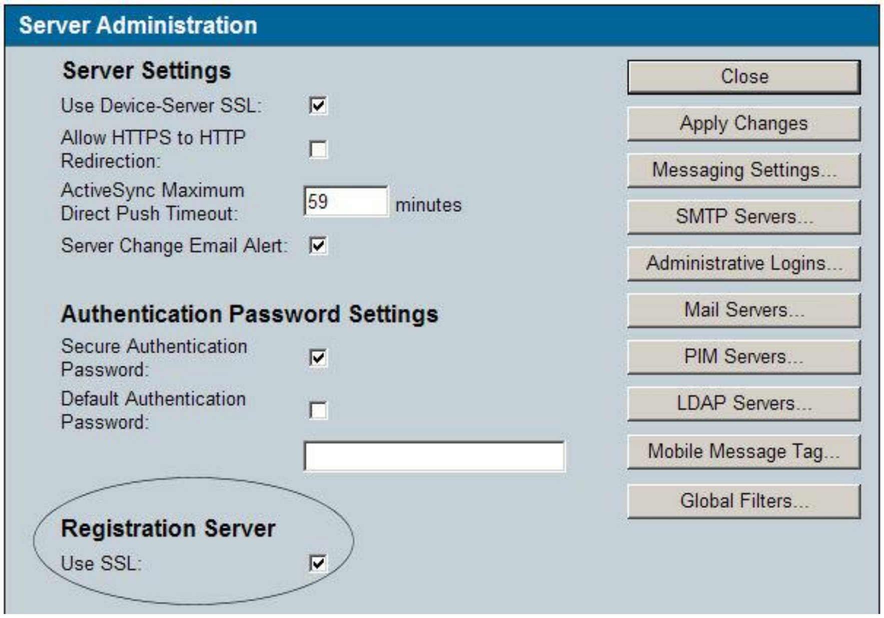
Protocol: Oracle

Port Number: 143

Use SSL: ☑

GO!NotifyLink Web/Http Component to Registration Servers

The GO!NotifyLink registration server is equipped with an SSL certificate. Enabling the use of SSL for communication between the server housing your GO!NotifyLink Web/Http Component and the registration server is done on the ***Server Administration*** page of the Administrative Web console as shown below.



Server Administration

Server Settings

Use Device-Server SSL: ☑

Allow HTTPS to HTTP Redirection: □

ActiveSync Maximum Direct Push Timeout: 59 minutes

Server Change Email Alert: ☑

Authentication Password Settings

Secure Authentication Password: ☑

Default Authentication Password: □

Registration Server

Use SSL: ☑

Check the **Use SSL** box located under ***Registration Server***.

Database Security: Data-at-Rest Encryption

Sensitive data-at-rest is secured in the GO!NotifyLink database using AES encryption algorithms. The seed, from which the database encryption key is generated, is stored in a database table. Starting with version 4.7.0, GO!NotifyLink Enterprise Servers use a 256 bit encryption key size to encrypt user information in the database.

Encrypted database information includes:

- Passwords
- User Encryption Key
- Authentication Password
- Email, Calendar, Contacts, and Task content

The GO!NotifyLink database component itself is secured using built-in SQL Server security features. By default, GO!NotifyLink creates a single SQL Server login with access to the GO!NotifyLink database. Permissions can be set within SQL Server, as desired, to access the database by other SQL Server logins or by using Windows Authentication.

Device to Web/HTTP Server Authentication

Authentication

Authentication ensures that a device is “who” it claims to be each time it communicates with the Web/Http Server.

On the server side, device authentication is automatically enabled upon installation of the *GO!NotifyLink Enterprise Server*. The server generates an 8 character authentication password for each user when they are added to the GO!NLES server. When the user registers a device he/she is prompted for that authentication password. The password is stored on both the server and the device. At registration and each time the device initiates a query for email and PIM, the password serves as a seed from which an AES encryption key is generated. Authentication elements communicated between device and Web/Http server are, therefore, encrypted using the AES algorithms.

The authentication password can be changed at any time through the Administrative or Client portion of the GO!NotifyLink web interfaces. A new random password can be generated by the server or can be typed in manually. If the authentication password is changed, the device will not be able to send/receive email until the password is updated on the device. Until the passwords match, the user will be prompted for the new password each time the device tries to connect to the server.

Should a user change devices or need to reregister an existing device, an administrator or the client must manually release new registration messages by implementing the *Synchronize Device* option from the administrative or client web. This insures that unauthorized users do not register a device against an GO!NLES user account that does not belong to them.

Detail of the Authentication Steps Between Device and Server

Device

The device uses the authentication password (seed) to generate an AES encryption key used to encrypt authentication elements sent to the server.

The device encrypts the elements to be sent to the server and also sends an encryption SHA-1 hash of the unencrypted characters.

The device does not store the authentication encryption key on the device, only the authentication password is stored (the key is generated each time it is needed).

Server

When the Web/Http server receives an authentication request from the device it decrypts the request and the SHA-1 hash portion of the request, using an AES encryption key generated from the authentication password stored on the server.

The server verifies that the request decrypted successfully and that the decrypted SHA-1 sent in the request matches the SHA-1 hash of the decrypted request.

If decryption is successful and the SHA-1 matches, then the request is processed by the server and a response is sent to the client.

If decryption is unsuccessful or the SHA-1 hash does not match, then the server responds with a message indicating that authentication failed, and the user is prompted for their authentication password.

ActiveSync Device Authentication

Users who register ActiveSync (AS) devices against an GO!NLES user account also use an authentication password. It is entered on the device at registration and must match the authentication password associated with the GO!NLES user account on the server.

Since there is no device application installed on ActiveSync devices, the registration process is somewhat different. In addition to requiring the authentication password at registration, the server captures and stores the unique device ID. This prevents unauthorized users from registering a device against an GO!NLES user account that does not belong to them. Should a user change devices or need to reregister an existing device, an administrator or the client must manually implement the *Clear Registration* option from the administrative or client web. This clears the unique identifier stored for the device and allows the device to reconnect and send updated information to the server.

Further Measures for Securing the Web/Http Server

To further secure the Web/Http server, you can lock down the virtual directories except for those pages accessed by the mobile devices. For a list of the php pages needing to be left open, contact the Globo Mobile Technologies Technical Support at technical@globoplc.com

Device Security

GO!NotifyLink device security implements proactive features that can help deter security breaches. It also includes reactive security options that can be implemented when a device is lost or stolen and therefore more vulnerable to a breach.

This section highlights *GO!NotifyLink's* core device security features. For a more comprehensive listing of device security features, see the Device IT Policy Comparison chart.

Proactive Device Security Options

Device Data-at-Rest Encryption

Data-at-rest encryption for the email database on the device storage disk is supported by several device types.

GO!NotifyLink Device Application

- BlackBerry – With *GO!NotifyLink for BlackBerry* v4.7 or greater, use the device application preferences *(General Security Settings)* to choose from three encryption key lengths.
    - Secure (128-bit)
    - More Secure (192-bit)
    - Most Secure (256-bit)

ActiveSync Solution Devices

- Android with TouchDown – encrypts TouchDown data only
    - Versions 5.1.0026 - 6.4.x – TDES 168-bit
    - Versions 6.5 and higher – AES 256-bit

- Android (Native) devices - OS version 3.0; manufacturer/model dependent for OS versions less than 3.0
- iPhone 3GS and 4 with iOS 4, iPod touch 3rd and 4th generation with iOS 4, and iPad device models – AES 256 bit
- Nokia S60 3rd edition devices – 256 bit
- webOS – AES 128-bit
- Windows Mobile 6.1 and 6.5 – AES 128-bit
- Windows Phone 7 – *This device does not currently support Data-at-Rest encryption.*

Device Rules: Lock Rules

Inactivity Timeout

- *BlackBerry*
  The GO!NotifyLink Lock Timeout setting always respects the native timeout interval. Turning off the device or letting the native inactivity timer turn off the device will not cause the password prompt when turning the device back on unless the GO!NotifyLink timeout interval has expired. Soft reset always triggers the password prompt to be displayed.
- *iPhone/ iPod touch/ iPad, Windows Mobile, Palm webOS, Symbian, Android Native, Android with TouchDown™, and Windows Phone 7 platforms using GO!NotifyLink ActiveSync Solution*
  Lock interval is based on native lock interval and can be set on the device or can be enforced by security rules sent from the *GO!NotifyLink* server.

Challenge Timeout

- *BlackBerry*
  The GO!NotifyLink Challenge Timeout lock is initiated regardless of inactivity and is intended to challenge the use of the device if it is lost or stolen. It must be greater than the *Inactivity Timeout*.
- *iPhone/ iPod touch/ iPad, Windows Mobile, Palm webOS, Symbian, Android Native Android with TouchDown™, and Windows Phone 7 platforms using GO!NotifyLink ActiveSync Solution* – Not supported

Duress Notification

- *BlackBerry*
  If enabled, this option allows the user to activate the duress notification if he/she is forced to unlock the device under duress by entering the password in an altered format (shift all characters to the left). EX: If lock password is “guarddog”, the duress password is “uarddogg”.

  A high priority Email notification is sent to the specified Email address with the Subject: “GO!NotifyLink Duress Notification.” The notification is completely hidden from view. It does not appear in the Outbox, Sent Items, or Deleted Items folders.
- *iPhone/ iPod touch/ iPad, Windows Mobile, Palm webOS, Symbian, Android Native Android with TouchDown™, and Windows Phone 7 platforms using GO!NotifyLink ActiveSync Solution* – Not supported

Device Rules: Password Rules

Device Password Expiration

- *BlackBerry*
  If enabled, fifteen days prior to the expiration, user is reminded that the password will expire in 15 days. When the password expires, the device locks. The user must unlock it with the current password and then create a new password at the prompt. Expiration can range from 30 to 365 days.
- *iPhone/ iPod touch/ iPad, Windows Mobile, Symbian, Android Native(some models), Android with TouchDown*^{TM}*, and Windows Phone 7 platforms using GO!NotifyLink ActiveSync Solution also support this policy.*
  Not supported on *Palm webOS* devices.

Device Password History

- *BlackBerry*
  If enabled, this feature prevents users from reusing passwords too soon. Can configure device to store anywhere from 10 to 100 passwords. EX: If the number of stored passwords is 10, you will not be able to use the past ten passwords. When you create the 11th password, the oldest stored password becomes available for use again.
- *iPhone/ iPod touch/ iPad, Windows Mobile, Symbian, Android Native(some models), Android with TouchDown*^{TM}*, and Windows Phone 7 platforms using GO!NotifyLink ActiveSync Solution also support this policy.*
  Not supported on *Palm webOS* devices.

Device Rules: ActiveSync Rules

ActiveSync Rules allow administrators to enforce or disable security policies on *ActiveSync* devices.

When enabled this rule will enforce security policies that are set on the *GO!NotifyLink* server and are supported by *ActiveSync* devices. The rule is enabled by default.

Security policies supported on *ActiveSync* devices vary by device platform, but may include:

- Minimum Password Length
- Allow Simple Password
- Require Alphanumeric Password
- Minimum Number of Complex Characters
- Maximum Inactivity Timeout
- Wipe on Failed Unlock Attempts
- Remote Wipe
- Password Expiration
- Password History
- Require Storage Card Encryption
- Require Device Encryption
- Allow Camera

Reactive Device Security Options

GO!NotifyLink supports remote WIPE and LOCK executions and local (device) WIPE executions (where applicable). Remote WIPE and LOCK are controlled via the GO!NotifyLink Administrative Web and work when wireless is on.

Clear Device - The wipe trigger deletes Email and PIM and locks the device, enabling a password prompt. (Where applicable, SD card wipe is an option as well.)

Lock Password - The LOCK trigger locks the device, enabling a password prompt, but does not delete Email/PIM.

Remove Mailbox - *GO!NotifyLink* supports a third remote device security execution that removes the mailbox information from the device and puts *GO!NotifyLink* into a pre-registration state.

Remote Wipe - This option appears in place of *Clear Device* and *Remove Mailbox* when the device associated with the user's account is an ***ActiveSync device***.

Clear Device / Remote WIPE* (Sent from the *GO!NotifyLink* Administrative or Client Web)

- BlackBerry devices – Email and PIM are deleted
- iPhone/ iPod touch/ iPad, Windows Mobile, Palm webOS, Symbian, Android Native*,* Android with TouchDown*TM,* and Windows Phone 7 ActiveSync devices – Email, PIM and mailbox account are deleted and the device enters a pre-registration state. The specifics of how Remote Wipe operates may vary by the model and operating system version of the device. See device user guides for details.

*Where applicable, the SD card can be wiped as well (*Clear Device and Cards*)

Local WIPE, based on failed unlock attempts when Lock is on (device)

- BlackBerry devices– When the password is entered incorrectly after 10 consecutive tries device issues the wipe, which deletes the Email and PIM.
- Symbian S60, 3rd Edition OS devices using *GO!NotifyLink ActiveSync Solution* – When the password in entered incorrectly after 10 consecutive tries the device issues the wipe, which deletes Email and PIM and removes the *GO!NotifyLink* account.
- Windows Mobile devices using *GO!NotifyLink ActiveSync Solution* – Uses the native security measures. Native security may do a local wipe, but this depends on what security implementations the OEM customized into the firmware.
- iPhone/ iPod touch/ iPad devices using *GO!NotifyLink ActiveSync Solution* – Uses the native security measures and does a local wipe based on password attempts for iPhone OS version 3.0 or later. Device settings reset to their defaults and all information and media is removed by overwriting the data stored in the device. For iPhone OS version 2.2.1, the device does not actually wipe, but imposes time delays and eventually locks the device, requiring reauthorization through iTunes.
- Palm webOS devices using *GO!NotifyLink ActiveSync Solution* – Uses the native security measures and does a local wipe based on password attempts. The wipe deletes all personal information, such as messages, contacts, calendar events and tasks, the Microsoft Exchange ActiveSync account, and any third party applications added.
- Android devices with TouchDownTM using *GO!NotifyLink ActiveSync Solution* – Uses the native security measures and does a local wipe based on password attempts. The wipe deletes the GO!NotifyLink account created via TouchDown and all data synchronized by TouchDown.
- Android devices (Native) using *GO!NotifyLink ActiveSync Solution* – Uses the native security measures and does a local wipe based on password attempts. The wipe deletes all data, accounts, and applications from the device, but will not erase the SD card.
- Symbian S60, 3rd Edition devices using *GO!NotifyLink ActiveSync Solution* – Uses the native security measures and does a local wipe based on password attempts. The wipe deletes all data, accounts, and applications from the device and the SD card.
- Windows Phone 7 devices using *GO!NotifyLink ActiveSync Solution* – Uses the native security measures and does a local wipe based on password attempts. The wipe deletes all data, accounts, and applications from the device, but will not erase the SD card.

Remote Removal of GO!NotifyLink Mailbox (Sent from the *GO!NotifyLink* Administrative or Client Web)

- BlackBerry devices– Email and account information are wiped from the device
- iPhone/ iPod touch/ iPad, Windows Mobile, Palm webOS, Symbian, Android Native, Android with TouchDown*TM*, and Windows Phone 7 devices using the *GO!NotifyLink ActiveSync Solution* – Mailbox removal is not a separate option. The *Remote Wipe* option removes the mailbox account along with Email and PIM.

Remote LOCK (Sent from the *GO!NotifyLink* Administrative Web)

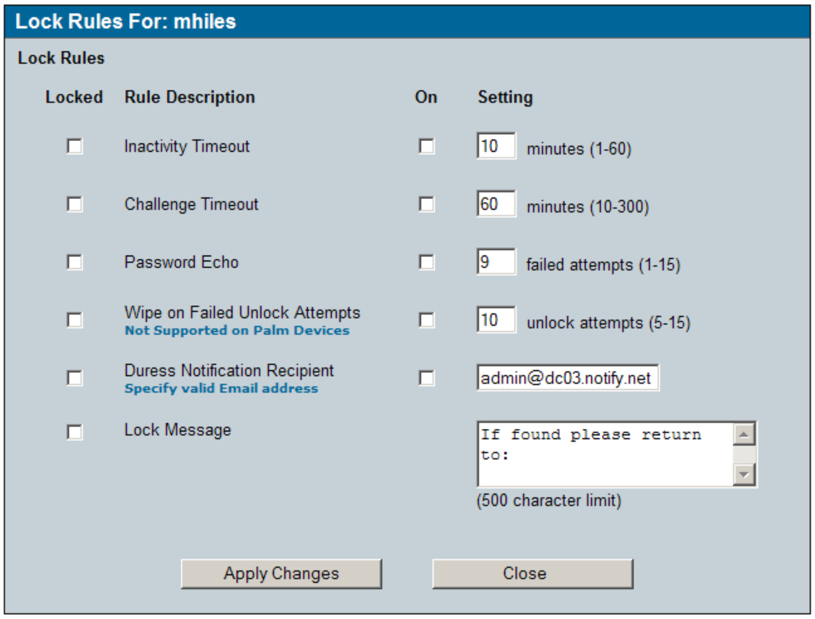
Device platforms which support remote lock use the password set in GO!NotifyLink's *Device IT Policy*: *Lock Settings* as the LOCK password.

- BlackBerry devices – The entire device is locked by the GO!NotifyLink application. The native BlackBerry security is not used.
- iPhone/ iPod touch/ iPad, Windows Mobile, Palm webOS, Symbian, Android Native, Android with TouchDown*TM*, and Windows Phone 7 devices using *GO!NotifyLink ActiveSync Solution* – Not supported.

Implementation Guidelines: Preventing/Managing Device Breaches

Lock settings are managed from the Administrative Web.

-Select ***User Administration*** > select a user and click the ***Edit User Policy*** button > ***Lock Rules***



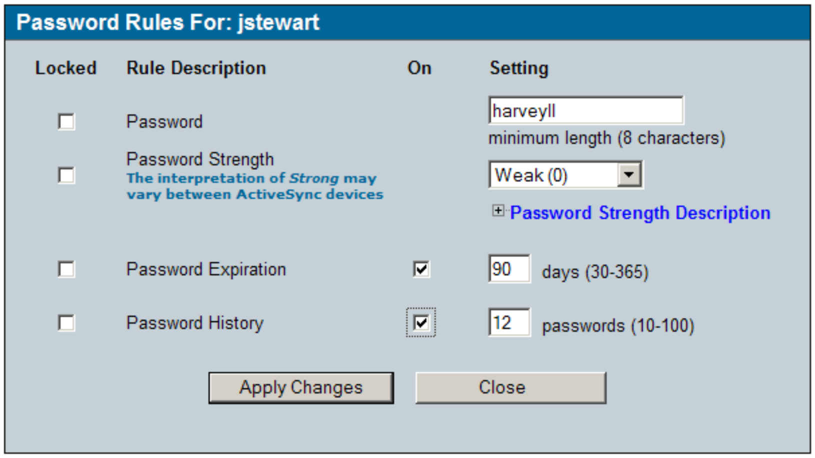
Lock Rules For: mhiles

Lock Rules

Locked	Rule Description	On	Setting
□	Inactivity Timeout	□	10 minutes (1-60)
□	Challenge Timeout	□	60 minutes (10-300)
□	Password Echo	□	9 failed attempts (1-15)
□	Wipe on Failed Unlock Attempts Not Supported on Palm Devices	□	10 unlock attempts (5-15)
□	Duress Notification Recipient Specify valid Email address	□	admin@dc03.notify.net
□	Lock Message		If found please return to: (500 character limit)

Password settings are managed from the Administrative Web.

-Select ***User Administration*** > select a user and click the ***Edit User Policy*** button > ***Password Rules***



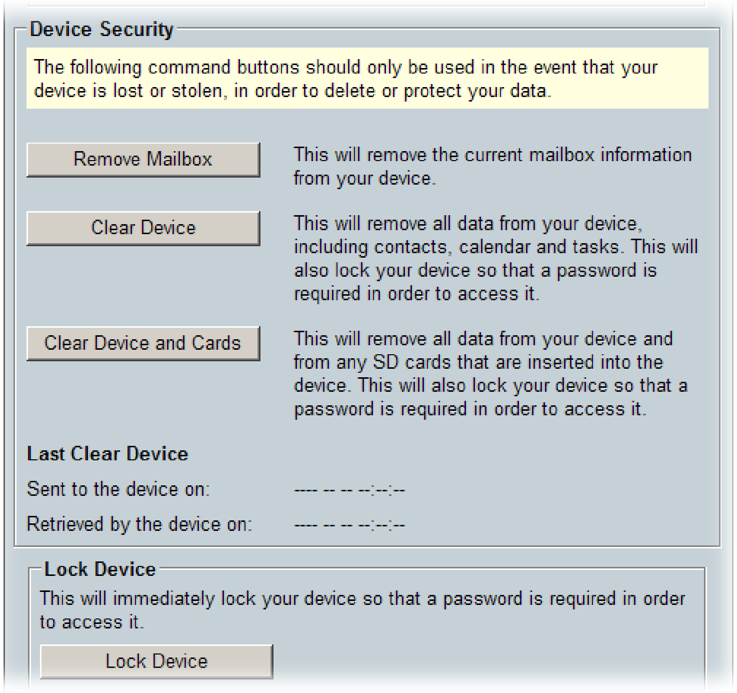
Password Rules For: jstewart

Locked	Rule Description	On	Setting
☐	Password		harveyll minimum length (8 characters)
☐	Password Strength The interpretation of *Strong* may vary between ActiveSync devices		Weak (0) ⊞ Password Strength Description
☐	Password Expiration	☑	90 days (30-365)
☐	Password History	☑	12 passwords (10-100)

Clear Device, Remote wipe, and Lock commands are issued from the Administrative Web.

-Select ***User Administration*** > select a user and click the ***Edit User Policy*** button > ***Security Rules***

Devices synchronizing with GO!NotifyLink



Device Security

The following command buttons should only be used in the event that your device is lost or stolen, in order to delete or protect your data.

Remove Mailbox — This will remove the current mailbox information from your device.

Clear Device — This will remove all data from your device, including contacts, calendar and tasks. This will also lock your device so that a password is required in order to access it.

Clear Device and Cards — This will remove all data from your device and from any SD cards that are inserted into the device. This will also lock your device so that a password is required in order to access it.

Last Clear Device

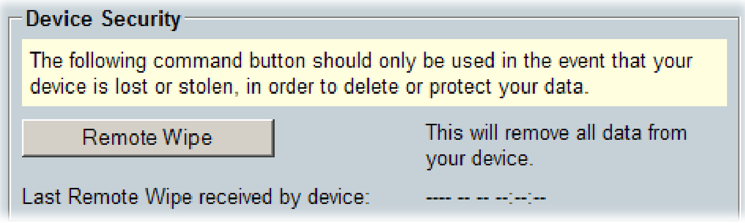
Sent to the device on: ---- -- -- --:--:--

Retrieved by the device on: ---- -- -- --:--:--

Lock Device

This will immediately lock your device so that a password is required in order to access it.

Devices synchronizing through an ActiveSync Server



Device Security

The following command button should only be used in the event that your device is lost or stolen, in order to delete or protect your data.

This will remove all data from your device.

Last Remote Wipe received by device: ---- -- -- --:--:--

Recommended Follow Up Practices When Remotely Clearing Devices

The success of the clear device and remote wipe options depends on timing and whether or not the wireless device connects in order to receive the message.

There are maintenance settings within the server system that will eventually remove the clear message from the database. If this happens before the device connects and receives the message, the device will not be cleared.

Therefore, administrators are advised to **execute '*best practice*' measures** to ensure that no further data gets to the device. The best practice is to remove the user from the *GO!NotifyLink* server.

From the *User Administration* page, select the user and click the **Remove User** button.

Server Log File Security

GO!NotifyLink Enterprise Server error logging is intended to be used as a diagnostic tool by Technical Support staff. Files may be set to log varying degrees of detail as needed or logging may be disabled in accordance with security laws or policies.

Servers where the log files reside should, of course, be secured. In addition, when logging *is* enabled, administrators should limit access to the directory where the logs are contained.

A further security measure would be to limit the amount of information sent to the log files by reducing log levels. Logging is enabled and set at level 2 by default. The log levels can be adjusted, however, to levels 0 through 4 (4 logs the highest level of detail; 0 logs only errors).

You may wish to reduce the logging level to 0 (errors only) in database files containing potentially sensitive user information:
In the database, set *GeneralConfig.DebugLogLevel* to 0

You may wish to totally disable logging in the registry:
In the registry on the Web/Http component server, set

HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES AirSyncServer\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES InternetMsgService\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES ValidateLeaseService\EnableLogging to 0

In the registry on the Messaging component server, set
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES AttachmentService\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES AvailableUsers\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES GleanerController\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES NotificationController\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES PIMService\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES ResponseHandler\EnableLogging to 0
HKEY_LOCAL_MACHINE\Software\Notify Technology Corporation\NLES SyncMLServer\EnableLogging to 0

GO!NotifyLink On Demand Security

GO!NotifyLink On Demand is the outsourced solution chosen by many organizations not wanting to manage a *GO!NotifyLink* server on premise. It is a simple solution to immediate mobility needs, and offers the flexibility of migration to an On Premise solution should growth require it.

The On Demand service provides mobile users with secure, real-time, wireless synchronization of Email/PIM equal to that of On Premise systems for BlackBerry, iPhone/ iPod touch/ iPad, Palm webOS, Symbian S60 3, Windows Mobile and Windows Phone 7 devices.

This section of the document describes the standards in place for securing the On Demand service.

Data Center Architecture

GO!NotifyLink On Demand is hosted in a state-of-the-art, hardened data facility located in Youngstown, Ohio.

Data center physical features include:

- Multi-layered security control procedures: non-descript building with no public access, 24/7 closed-circuit video and alarm monitoring, biometric entry system, locked server cage area
- Uninterruptible redundant AC and DC power, onsite backup power generators
- HVAC redundant design for maximum temperature and humidity control
- Smoke detection and dry-pipe fire suppression systems

Physical and logical security of *GO!NotifyLink On Demand* servers:

- Dual redundant firewalls
- Load balanced and redundant gateway server clusters
- Servers fed by dual power sources
- Virus protection, antivirus signatures updated daily
- Authentication logic implemented which includes username/password and other authentication methods described in this document, see Device to HTTP/Web Server Authentication

Data Center Access and System Maintenance Policies:

- Access restricted to key personnel, role based access control is used, root access is given and other privileges are only assigned on an as needed basis
- Login IDs are not shared; remote access is only conducted by key personnel and over a virtual private network
- Passwords are made up of complex patterns and are changed on a regular basis
- Automatic backups are performed several times a day and are not done by a third party
- Timely upgrades are performed to secure and provide optimum operations. Patches and updates are applied regularly to conform to current patch and release levels described by Globo Mobile Technologies and by manufacturers of third party software used by Globo Mobile Technologies. This generally occurs within two weeks from the time the patch is available.

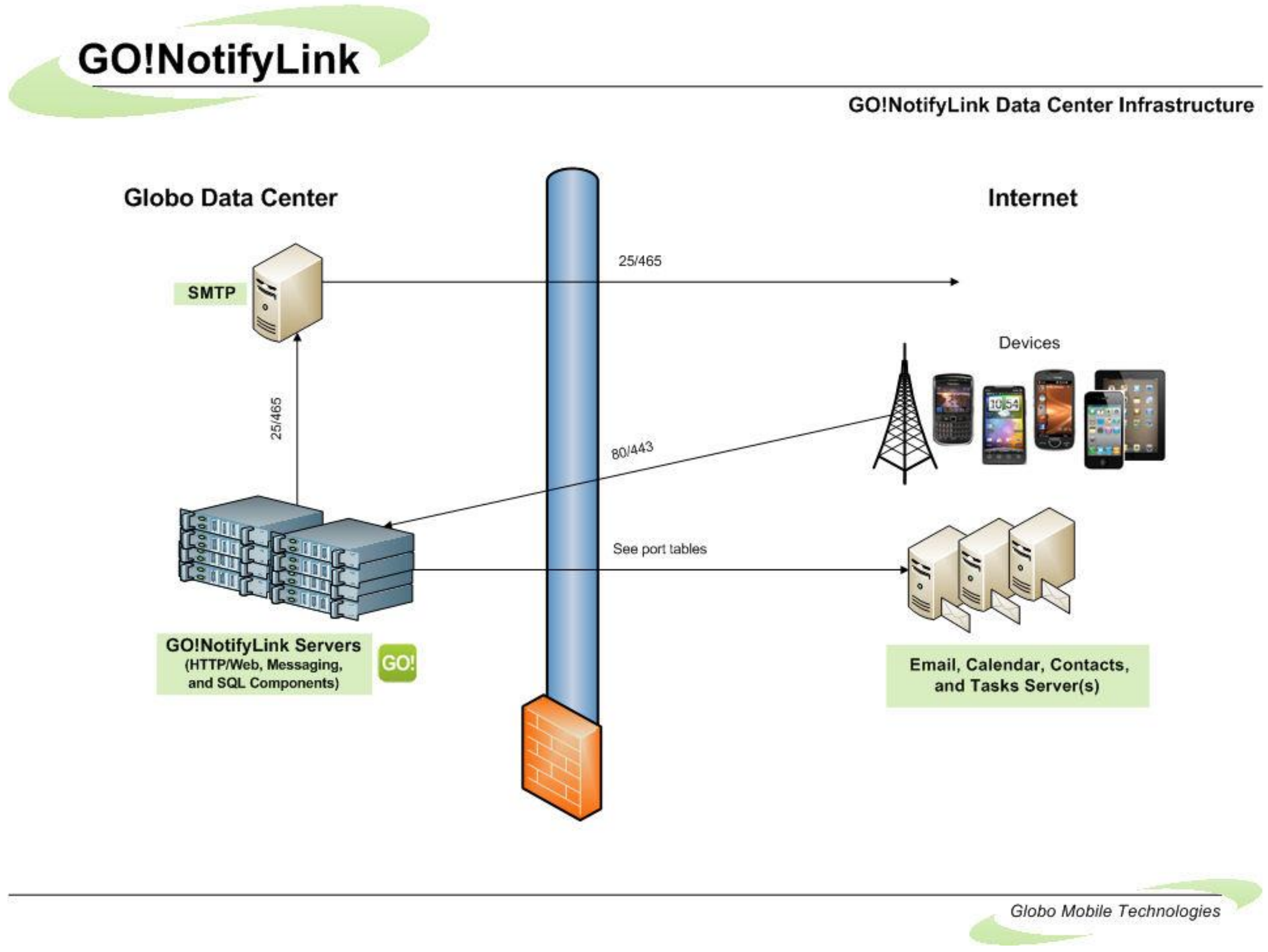
Network Security

The network topology is illustrated in the diagram below. More complete information on system architecture is included in the beginning of this document under Architecture and in the *Enterprise Server Installation Guide* found on the Globo Mobile Technologies software portal page. *(Access that portal at* http://gonotifylink.globoplc.com/Portal.asp, *then click on Server Installation and User Guides.)*

The *GO!NotifyLink* system is protected by a firewall. The only ports/protocols allowed incoming are 80/443 (HTTP/HTTPS). If the *Remote Lookup* option to an address book is used then 389/636 (LDAP/LDAPS) is needed. Outgoing ports are specific to each groupware server type and are listed in the charts below.

The *GO!NotifyLink* system uses AES, TDES with key length of 256 bits. It also uses SSL public key of 128 bytes.

Data Center Infrastructure


GO!NotifyLink
GO!NotifyLink Data Center Infrastructure
Globo Data Center
Internet
SMTP
25/465
25/465
Devices
80/443
See port tables
GO!NotifyLink Servers
(HTTP/Web, Messaging, and SQL Components)
GO!
Email, Calendar, Contacts, and Tasks Server(s)
Globo Mobile Technologies

Firewall Rules/Policies

Source	Destination	Port	Service
Devices	GO!NotifyLink Http/Web	80 or 443	HTTP or HTTPS
Messaging	IMAP4 server	143 or 993	IMAP or IMAP SSL
HTTP/Web	LDAP server	389 or 636	LDAP* or LDAPS*

Email/PIM Servers

Source	Destination	Port	Service
CGP	IMAP4 Server	143 or 993	IMAP or IMAP SSL
Exchange	Exchange PIM Server	80 or 443	HTTP or HTTPS
FirstClass	PIM Server	80 or 443	HTTP or HTTPS
GroupWise	GroupWise: PO	1677	GW Api
Kerio	PIM Server	80 or 443	HTTP or HTTPS
MDaemon	PIM Server (SyncML)	3000 or HTTPS Port	HTTP or HTTPS
Meeting Maker	PIM Server	8080 or 8443	HTTP or HTTPS
Mirapoint	Mirapoint Message Server	80 or 443	HTTP or HTTPS
Oracle	Oracle PIM Server	7779 or 4445	HTTP or HTTPS
Oracle Beehive	Beehive PIM Server	7777 or 4443	HTTP or HTTPS
Scalix	PIM Server	80 or 443	CalDAV
Sun	Sun Calendar Express	3080 or 4445	HTTP or HTTPS
Sun	Sun Contact Server (Communications Express)	80 or 443	HTTP or HTTPS
Sun	Sun CalDAV Server	8080 or 8443	CalDAV
Zimbra	Zimbra PIM Server	80 or 443	HTTP or HTTPS