



Software for the Open Enterprise™

> cool solutions home

AppNote: Setting up GroupWise Internet Agent for Dynamic Domains

Novell Cool Solutions: AppNote By David Stagg

Digg This - Slashdot This

Posted: 28 Oct 2004

David Stagg

Primary Support Engineer
Novell Premium Support Services
dstagg@novell.com

This paper describes how to setup and use Novell GroupWise Internet Agent (GWIA) for a Small or Home Office that is connected to the Internet using Dynamic IP addressing provided by your local Broadband (Cable, DSL, etc.) Internet Service Provider/Vendor (ISP/ISV). The material documented here is available in various online documents. It is provided here for ease of use in configuring SMTP SSL and Outbound Authentication using a 3rd party dynamic DNS service.

Contents

- Background
- Network Configuration
- External Dynamic DNS and Mail Relay Setup
- Internal DNS Configuration
- Create a SSL Certificate for GWIA
- Configuring GWIA for SSL and Outbound Authentication
- ISP/ISV's Blocking Port 25 on Inbound Email
- Conclusion

Topic:	Novell GroupWise SMTP Configuration for Dynamic DNS locations
Products:	Novell GroupWise 6.5, Novell NetWare, Novell Small Business Suite, Novell Certificate Server, Novell DNS/DHCP Services
Audience:	Small Business and Home Office Administrators and Consultants
Prerequisite Skills:	Familiarity with Novell DNS, NetWare and GroupWise administration
Tools:	ConsoleOne with Novell Certificate Server and Novell GroupWise 6.5 snapins installed

Background

Target Audience: Small Businesses and Home Offices that wish to leverage broadband access (Cable, DSL, etc) from their local ISP/ISV without requiring Static IP services and the related costs. Email use is limited to 150 or less per day. This configuration is not intended for systems connecting through dial-up links.

The Problem: ISP/ISV's assign IP addresses dynamically and charge high monthly rates for static IP Addresses. Outbound email from GroupWise is refused by some sites that subscribe to Black Lists that

include the Dynamic IP ranges your ISP/ISV assigns to your connection.

Assumptions: GroupWise 6.5 is already installed in your environment as your internal email system of choice. This may be part of NetWare Small Business Suite or on some other supported Operating System. This paper does not deal with the installation or setup of your GroupWise environment.

Network Configuration

For this paper a working environment was used that consisted of a NetWare 6.5 server connected to an Internet Router that in turn was connected to the Cable Modem provided by the local ISP/ISV. The Internet Router acquires the Dynamic IP address from the ISP/ISV for this location. The Internet Router is configured for Network Address Translation (NAT) support for all internal devices. The internal interface of the Internet Router is configured with a static IP addresses one Subnet 1. The NetWare server is configured with two Network Interface Cards, (NIC) one Public and one Private. The "Public" NIC is configured with a static IP Address on Subnet 1 (10.10.1.1) and is connected to the Internet Router. The second NIC is configured with a static IP on Subnet 2 (10.10.2.1) and is connected to an internal switch. Local workstations are connected to Subnet 2 through the switch. Workstations acquire their IP addresses from a DHCP service configured on the NetWare server.

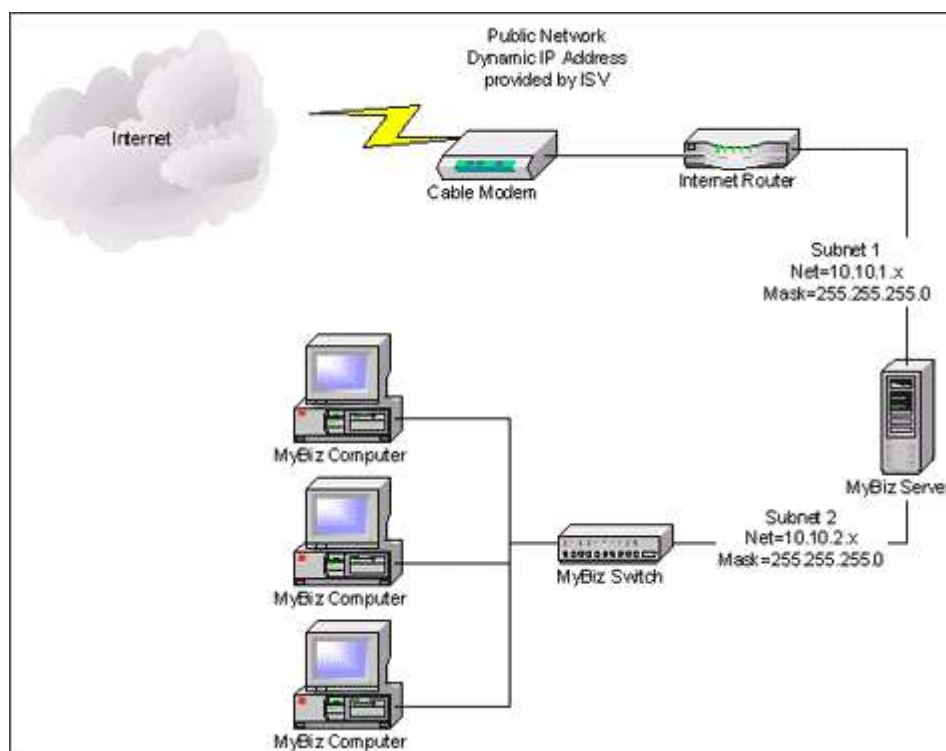


Diagram of MyBiz Internal Network

Note: The Internet Router will require additional configuration to properly forward Port 25 (SMTP) to your GWIA service. The steps required for this will depend on the actual Internet Router device you have and it's specific configuration process. Read the documentation for your device to properly configure this.

External Dynamic DNS and Mail Relay Setup

To handle the dynamic nature of the IP address provided by your ISP/ISV and still enable access to mail and other possible services, the services from <http://www.dyndns.org/> were used. This included setting up an Account, a Dynamic DNS Domain and MailHop Outbound services.

Note: At the time of this writing other Dynamic services were not explored or validated. With the exception of the MailHop Outbound services, DynDNS.org currently offers these services for free. The MailHop Outbound service is available for an annual fee. The author of this paper neither recommends, warranties, supports or makes any specific claims for or against <http://www.dyndns.org/>This paper simply documents the use of the services available from this organization at the time of writing. Visit www.dyndns.org to identify conditions for using the services that are available and may be of use to you in supporting your environment.

1. Create an account with Dynamic Domain provider. To create a new account with DynDNS.org at <https://www.dyndns.org/account/create.html> you need to provide a "username", "E-mail Address" and a "Password".

2. Select and Register your Dynamic Domain and assign your current dynamic IP Address as assigned by your ISP/ISV. By selecting the "Enable Wildcard" option all hosts for your domain will be directed to your server.

Many Dynamic Domains can be selected from DynDNS.org. The example here uses mydomain.dyndns.biz for the MyBiz network.

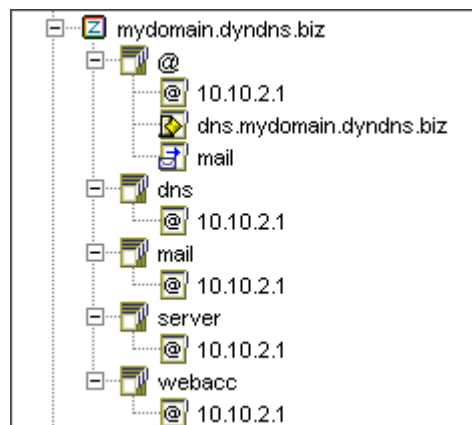
3. Sign up for MailHop Outbound service. This is a fee service so additional details will have to be provided to activate the service.



Internal DNS Configuration

Internally DNS services are provided by a DNS service configured on the NetWare server. The internal DNS server is Authoritative for the Domain so that internal DNS requests are correctly resolved to internal services. This is also required to be setup properly so that any outbound emails that generate error messages are returned to the sender properly. If not done correctly these messages can end up looping at the GWIA.

The sample internal DNS setup to the right shows the records created using the Novell DNS/DHCP Management console. This domain matches the dynamic domain selected when setting up the Dynamic Domain above. As this is a single server all of the A records are pointing to the same IP Address. CNAME records could be used for the various services but the entry that the MX (Mail Exchange) record points to must be an A record and not a CNAME record.



Create a SSL Certificate for GWIA

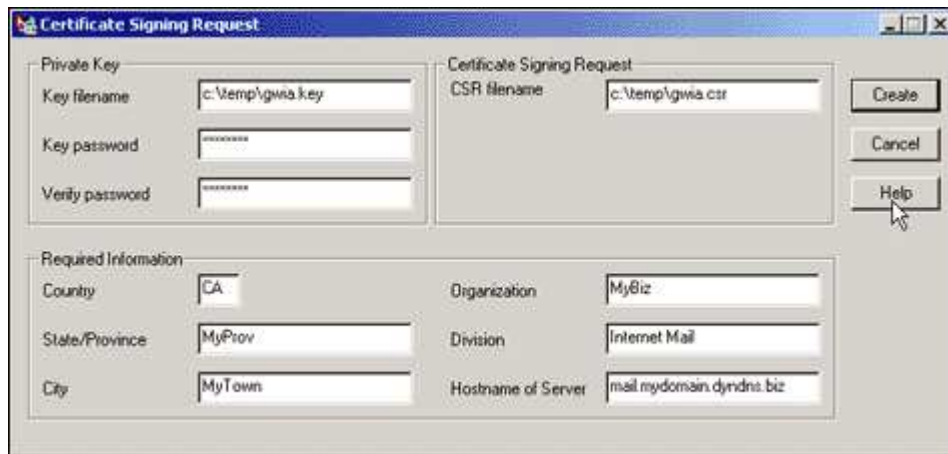
Outbound Authentication is required to be able to use the DynDNS Mailhop services. Although SSL connections are not required, your user name and password are sent in clear text to the Mailhop service without SSL connections configured. The next steps walk through the process required to create a SSL Certificate that your GWIA can use for SSL connections. This is based on using the Novell Certificate Server which is included as part of a Novell NetWare installation.

1. Create a Certificate CSR using GWCSRGEN.EXE found in the \admin\utility\gwcsrgen subdirectory in the GroupWise Software Distribution directory.

In this example two files are created, "gwia.key" and "gwia.csr", using the information provided in the Required Information section. The "gwia.csr" file will be used to create a signed Certificate and the "gwia.key" will be used with the Certificate for SSL configuration of the GWIA.

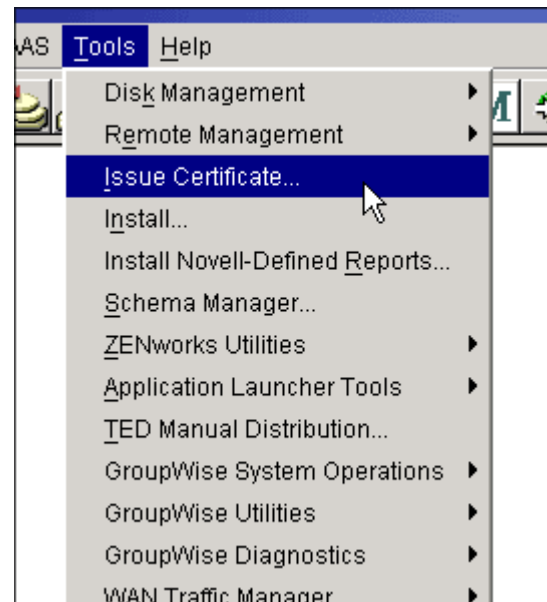
Fill in each field with the required information and then click Create to create the gwia.key and gwia.csr files.

Additional information on the various fields is available in Help for the GWCSRGEN utility.

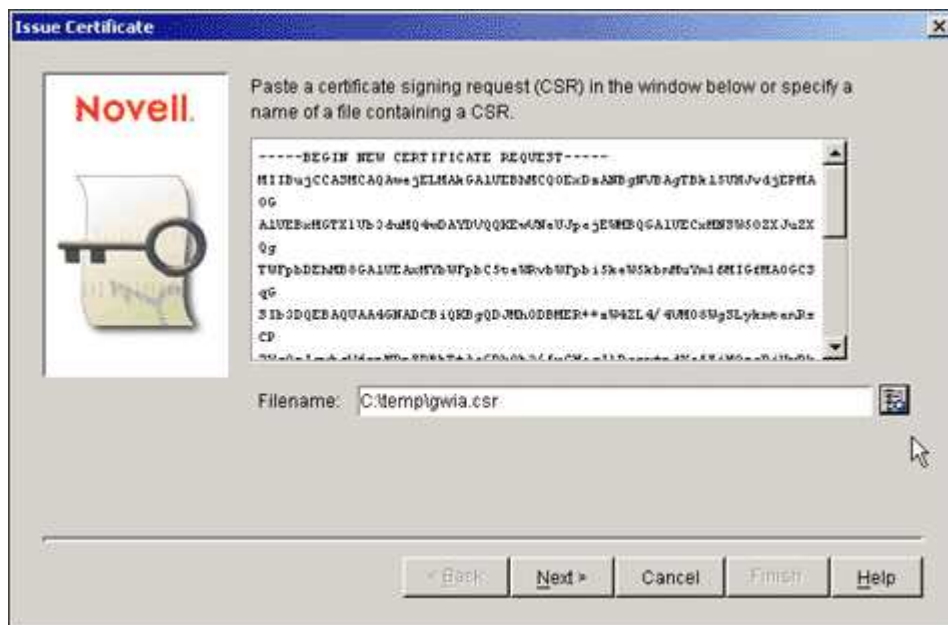


The screenshot shows a Windows-style dialog box titled "Certificate Signing Request". It is divided into two main sections. The top section, "Private Key", contains three text boxes: "Key filename" with the value "c:\temp\gwia.key", "Key password" with a masked password, and "Verify password" with a masked password. The bottom section, "Certificate Signing Request", contains one text box: "CSR filename" with the value "c:\temp\gwia.csr". To the right of these sections are three buttons: "Create", "Cancel", and "Help". Below these sections is a "Required Information" section with several text boxes: "Country" (CA), "Organization" (MyBiz), "State/Province" (MyProv), "Division" (Internet Mail), "City" (MyTown), and "Hostname of Server" (mail.mydomain.dyndns.biz).

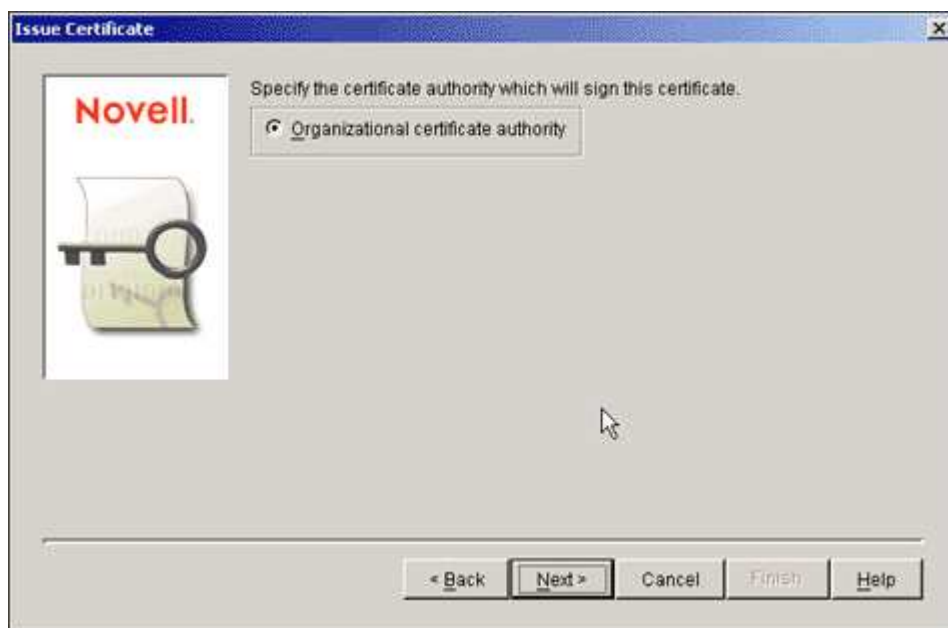
2. Create the Signed Certificate using Novell Certificate Server by selecting the "Issue Certificate" option in the Tools menu of ConsoleOne.



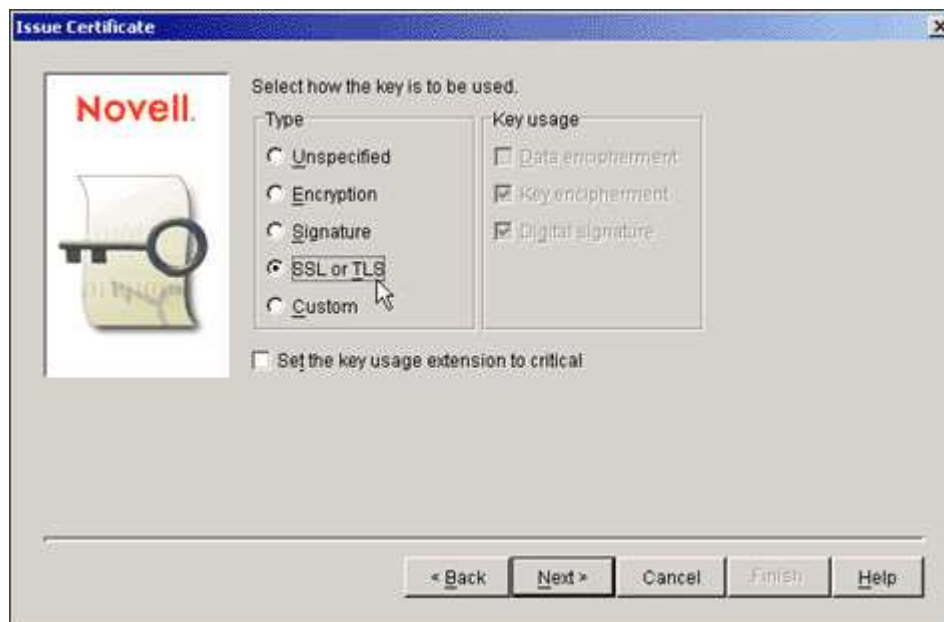
An object in the Tree (Tree Root or lower) has to be selected for the Tools > Issue Certificate... option to be available.



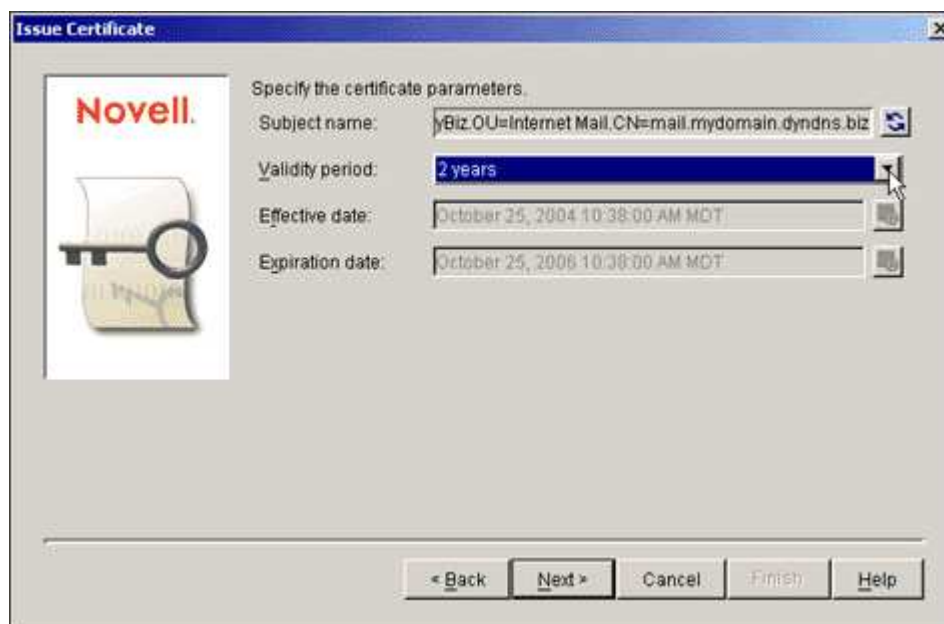
3. Browse and select the CSR file that was created previously and click Next.



4. Click Next



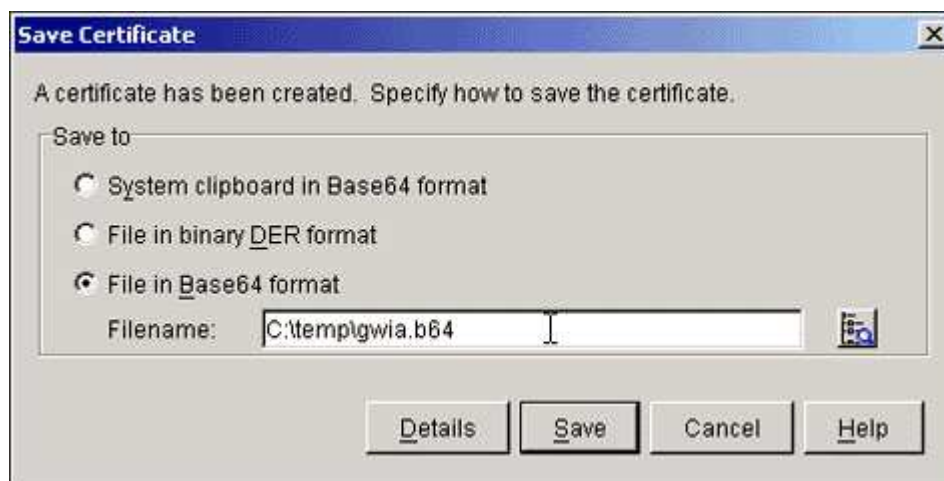
5. Select SSL or TLS for the Certificate Type and click Next



6. Select the "Validity period" that you prefer and click Next



7. Verify the Certificate parameters and then click Finish.



8. Change the "Save to" format to Base64 and enter the path and file name to save the Certificate. Once the option and pathname is correct click Save.
9. Put the Certificate files in place for the GWIA to use.

In this configuration the subdirectory SYS:SYSTEM\GWagent was used for the GroupWise Agent files. A new subdirectory SYS:SYSTEM\GWagent\MailCert was created to hold the new SSL Certificate files. It is important to note that the 0.subdirectories in the path to the Certificate files must be in the 8.3 format. Long subdirectory names will generate an error and SSL will not work.

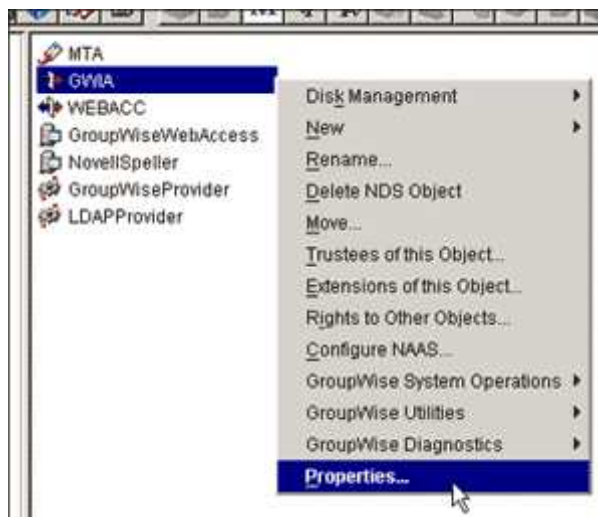
Copy the files GWIA.KEY and GWIA.B64 to SYS:\SYSTEM\GWagent\MailCert, or a directory of your choice where they will be available to the GWIA agent.

Configure GWIA for SMTP SSL connections

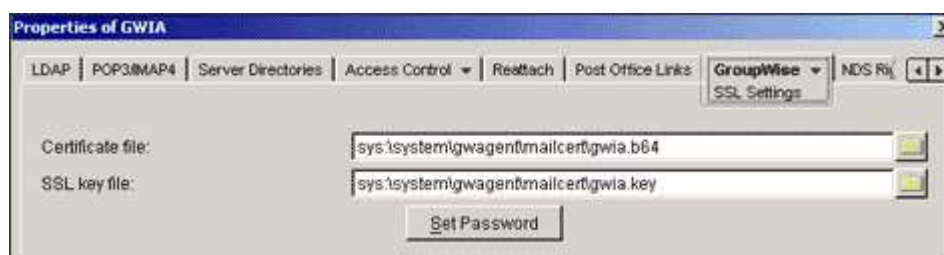
The following steps are also documented in online documentation for GroupWise. Search for Securing Internet Agent connections Via SSL in the GroupWise documentation.

1. Define the Certificate File for the Internet Agent. The SMTP process requires a SSL Certificat file for the SSL converstations

2. In ConsoleOne, right-click the Internet Agent Object, then click Properties.



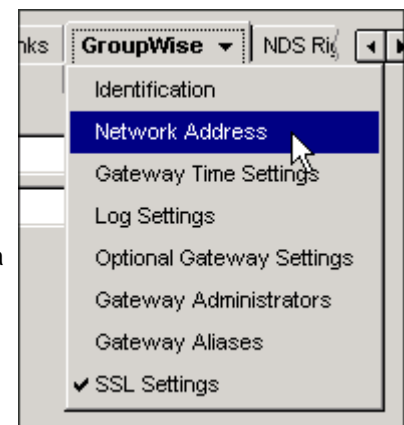
3. Click GroupWise > SSL Settings to display the SSL Setting page.



4. Type in the paths to the gwia.b64 and gwia.key files using the full pathnames to the location on the server. If you use the browse button you will have to edit the path to use the VOL:\path notation for a NetWare server. The wrong path syntax will prevent SSL from working correctly.
5. Click the "Set Password" button field to enter the password for the gwia.key file. This is the password that was used earlier when setting up the files using the GWCSRGEN utility.

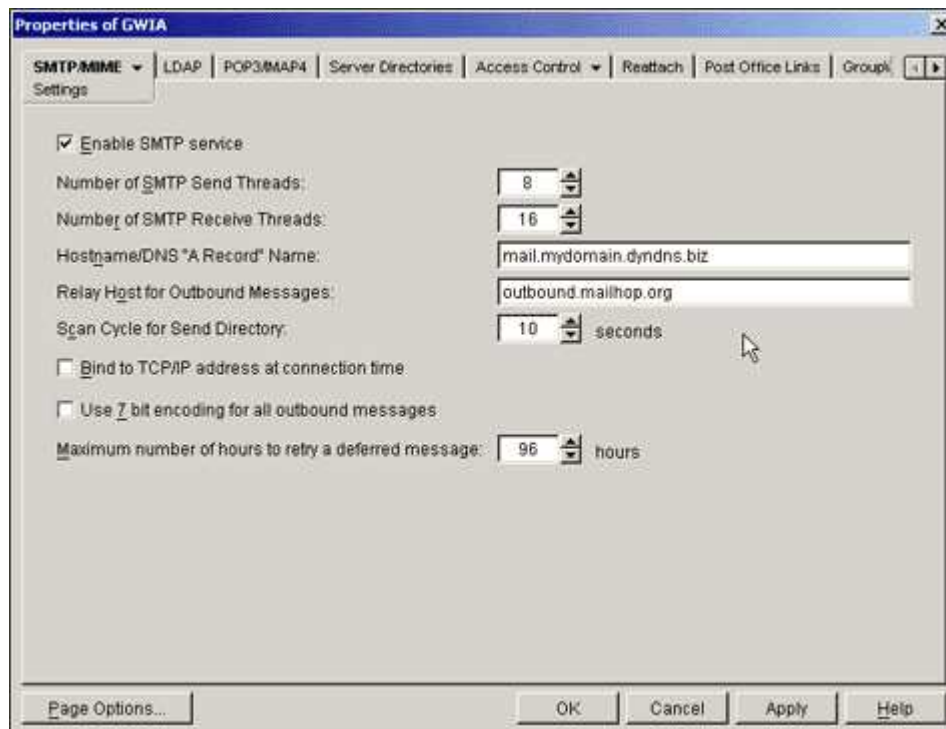
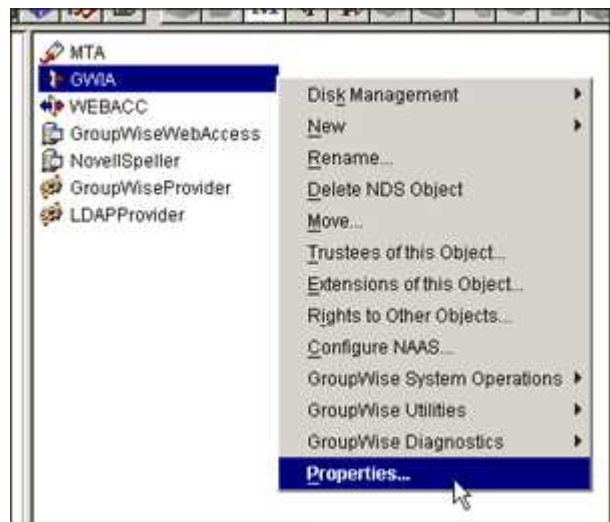


6. Once the password is entered click Set Password
7. Then click Apply to save your SSL Settings.
8. Enable SSL for SMTP is required so that the SMTP service will attempt to communicate using SSL first. If a conversation via SSL is not possible then a normal connection will be established.
9. Switch to the GroupWise Network Address page
10. Set the SMTP SSL option to Enabled and then click OK to save the settings



Configure GWIA for SMTP Outbound Authentication

1. Setup GWIA with your DNS domain information that was selected earlier when setting up your Dynamic Domain.
2. In ConsoleOne right-click the Internet Agent object and select Properties
3. Then select the SMTP/MIME > Settings tab



4. If it is not already configured, enter the Hostname information. In this example we used mail.mydomain.dyndns.biz. Use the correct Hostname that matches your domain and DNS configuration.
5. Configure the "Relay Host for Outbound Messages" with "outbound.mailhop.org" to forward outbound email through the MailHop Outbound service that you setup earlier in this process. See the previous screen shot for details.
6. Click OK to save your SMTP/MIME settings.
7. Setup SMTP Host Authentication by editing the "gwauth.cfg" file located in the Internet Agent's gateway directory. The directory is located under the Domain's "wpgate" directory. In this example that was "wpgate\gwia". Three fields are required in this file: domain_name, authuser and authpassword. These are the values required for the Internet Agent to authenticate to the MailHop Outbound service. The authuser and authpassword values for MailHop Outbound are the username and password used when you created the Account at DynDNS.org. Check with your chosen dynamic DNS service for the required Authentication values.

8. Open the wpgate\gwia\gwauth.cfg file in notepad and add a line to the end providing the required information. In this example the contents of gwauth.cfg look like:

```

GWIA AUTH configuration file
-----
domain          AuthID          password
Example
remotehost.com  AuthUserID     AuthPassword
-----
outbound.mailhop.org  mybiz  password

```

Note: The password value is clear text in this file so ensure that you have appropriate security on your domain directories.

9. Once all the Internet Agent settings have been configured restart the Internet Agent by using the F6 option on the Internet Agent Console screen.

ISP/ISV's Blocking Port 25 on Inbound Email

Setting up and testing for this paper did not encounter the situation where ISP/ISV's are now starting to block port 25 for inbound email to your system. If your ISP/ISV is blocking Port 25 you will have to setup the Internet Agent on a different Port and have a Smart Host relay the mail to you on that port. DynDNS.org has a MailHop Relay service that may work for your environment. This information is provided simply for your reference as the author has not setup or tested that service.

Conclusion

Setting up your Novell GroupWise Internet Agent in a Dynamic DNS environment allows you to control your own email environment and gain the benefits of your own private GroupWise system for mail handling. This paper has demonstrated how to effectively configure SMTP with SSL and Authentication for Outbound mail services for minimal costs.

Reader Comments


- good solution.
- Handy and well explained ;)
- I personally have done much of what you say but in a much simpler fashion. Basically All I did was to get a Dynamic DNS provided. Forward them my domain so that they are now hosting my zone records. On the local side of my network I have a server behind a Linksys Router (I am not thrilled with Linksys ... just for the record. They are slow and a bit klunky) and port forwarded the port 25 to my server. While its not in heavy use and infact is only used occasionally I have not seen any problems since I started with the DDNS provider and I am behind a Comcast network. Am I missing something important? Did I create an unseen problem that will bite me later?

From David: When I started digging into it I found that some mail systems subscribe to Black Lists that include the Dynamic IP Address Ranges provided by various ISP's. The Dynamic Range that I sit in was one of those that was being Black Listed by default. The only way around this was to get a static IP for lots more money, or look to some service that could receive my outbound email and forward from a valid host system. The choice that I documented required Outbound Relay and SSL Authentication for Security. Since the various pieces were documented in different manuals I had to work through a number of issues pulling the details together. The result is the published article. I


made indirect reference to my situation near the start of the article where I stated: **"The Problem:"**. If you are not experiencing any blocking on your outbound email to any site, then you do not need this full solution. What you are doing is enough at this time. It may be that the Dynamic Range you are provided by Comcast is not currently on the Black Lists. If they are added in the future you may need to use this solution fully then. Until then save your money and enjoy.

- Great Article. I'll look into the dynamic portion of mine as well. My ISP has not changed any IP addresses since I got the account a year and a half ago. My solution to being blocked was this - set up my smarthost as the ISP SMTP server as the recommend for your mail clients. Once I set that up in my smarthost SMTP field, emails flowed to all addresses again. Thanks again for the article.
Regards, Paul Paul M. Muhlbach, A+, CNA, MCSA


Like what you see?

Sign up for our weekly newsletter. 


Want to contribute?

It could earn you a nano!
Learn more. 

Like Wikis?

Join the Cool Solutions Wiki.


**Interested?**

Request a sales call


*Novell Cool Solutions (corporate web communities) are produced by WebWise Solutions.
www.webwiseone.com*

© 2006 Novell, Inc. All Rights Reserved.