intellisync™
mobility unlimited.™

Intellisync Mobile Suite

Secure Gateway Administrator's Guide

Version 7.0
April 2006

PUBLISHED BY:

Nokia Enterprise Solutions
200 North Point Center East, Suite 600
Alpharetta, GA 30022

This publication is provided as is without warranty of any kind, express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This publication could include technical inaccuracies or typographical errors. Changes are made periodically to the information herein. These changes will be incorporated in new editions of the publication. Nokia may make improvements and/or changes at any time to the product(s) and/or the program(s) described in this publication.

Contents

1 Installing Secure Gateway

2 Configuring the Secure Gateway

3 Troubleshooting Secure Gateway

CHAPTER

1

Installing Secure Gateway

This chapter contains instructions for installing the Secure Gateway and provides a diagram of the recommended configuration.

Overview

Your company policy may dictate how you deploy Nokia's technology within your network configuration. There are several configuration options available; however, Nokia recommends the configuration described in this chapter using a demilitarized zone (DMZ), or screened subnet. The DMZ is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

Recommended Secure Gateway configuration

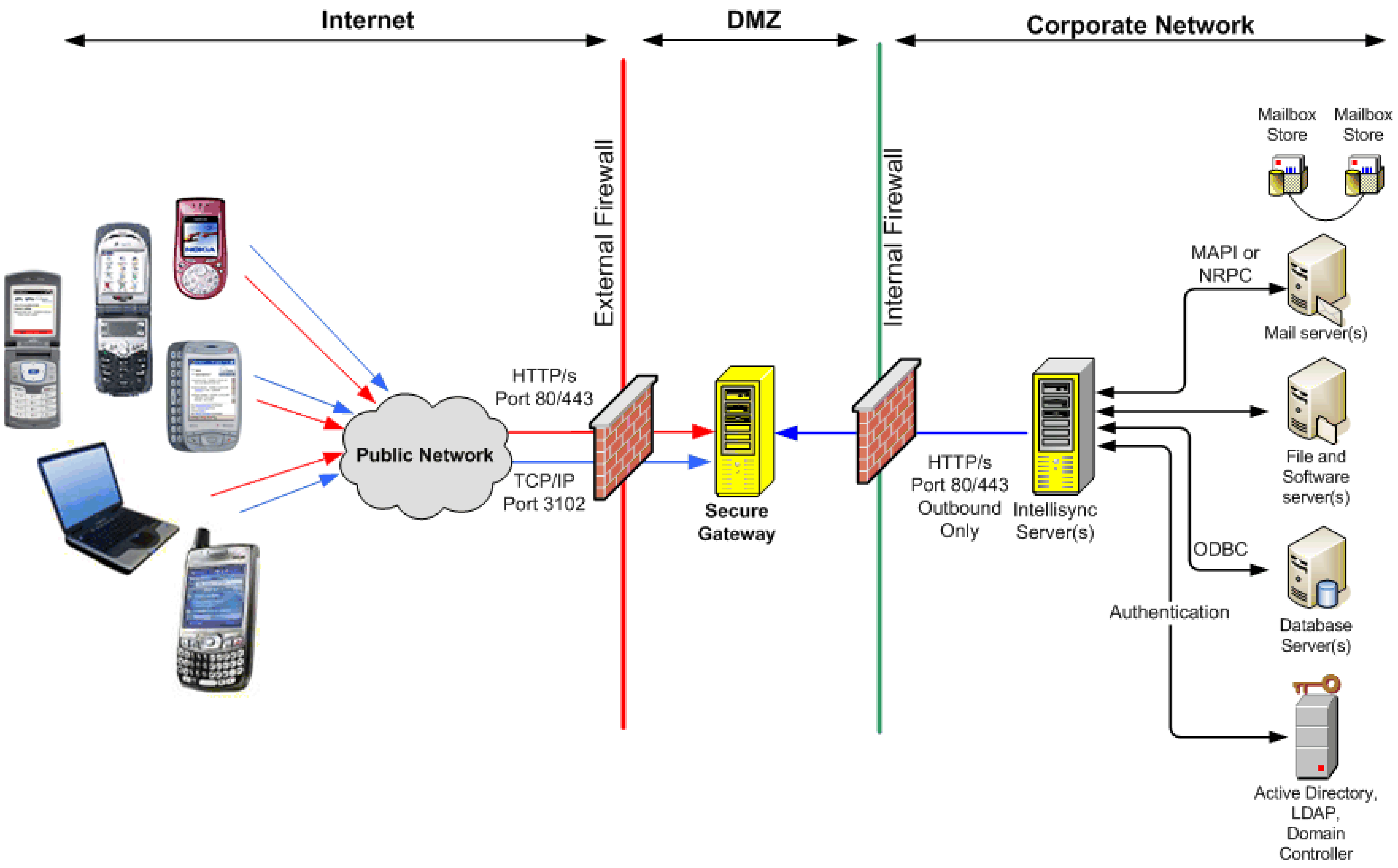
Nokia recommends using the Secure Gateway configuration within your network. The Secure Gateway offers secure and scalable communications between mobile devices and servers and consists of an HTTP listener and communications services.

The Secure Gateway intercepts the HTTP requests from mobile devices to the Intellisync Mobile Suite server and can route the requests in three ways:

- Push requests through TCP/IP port 3102
- Sync requests through ports 80 and 443
- Web requests through ports 80 and 443

The following diagram illustrates the recommended configuration for the Secure Gateway. In this scenario, all Intellisync Mobile Suite components and enterprise servers are behind the corporate inner firewall.

Recommended Secure Gateway Configuration



The following table shows the default port settings. Your port settings may be different depending on your network configuration.

Table 1: Default ports for communication from devices

Communication Protocol	Default Port
HTTP • Sync traffic • Web tunneling	80 (configurable)
HTTPS • Sync traffic • Web tunneling	443 (configurable)
TCP/IP • Push traffic	3102 (configurable)

Installing the Secure Gateway

To install and configure the Secure Gateway, follow these steps:

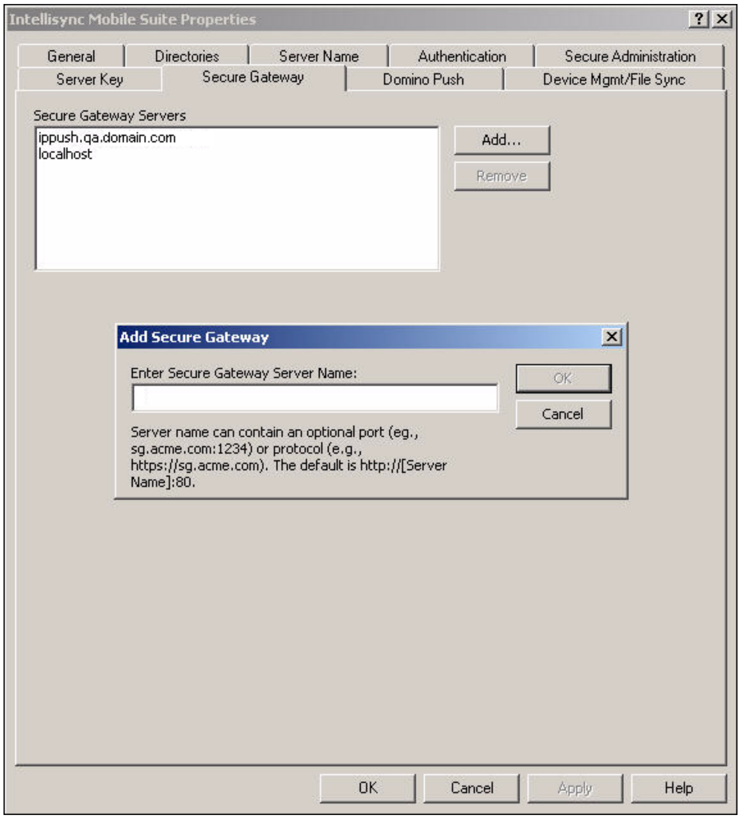
1. From the installation source folder, double-click the setup.exe file. The Secure Gateway Setup starts and prepares the wizard application for the installation.
2. On the Secure Gateway Welcome screen, click **Next**. The Destination Folder screen appears.
3. To install to a location other than the default folder, click **Change**. Otherwise, click **Next**. The Secure Gateway Service User screen appears.
4. Complete the following fields:

   Username. Enter the name for the specified user.

   Password. Enter the password for the specified user.
5. Click **Next**. A confirmation screen appears.
6. Click **Install**. The installation program installs the Secure Gateway components into the specified location. When the installation is complete, the InstallShield Wizard Completed screen appears.
7. Click **Finish**. The Secure Gateway wizard closes.

After the installation, you must specify the name of the Secure Gateway computer on the Intellisync Mobile Suite server. To do so, complete the following steps:

1. From the Windows **Start** menu on the Intellisync Mobile Suite server, choose **Programs**, **Intellisync Mobile Suite**, and then choose **Admin Console**. The Intellisync Mobile Suite control appears.
2. Select Intellisync Mobile Suite in the console tree.
3. From the **Action** menu, choose **Properties**. The Intellisync Mobile Suite Properties dialog box appears.
4. Click the **Secure Gateway** tab. The Secure Gateway panel appears.
5. Click **Add**. The Add Secure Gateway dialog box appears.

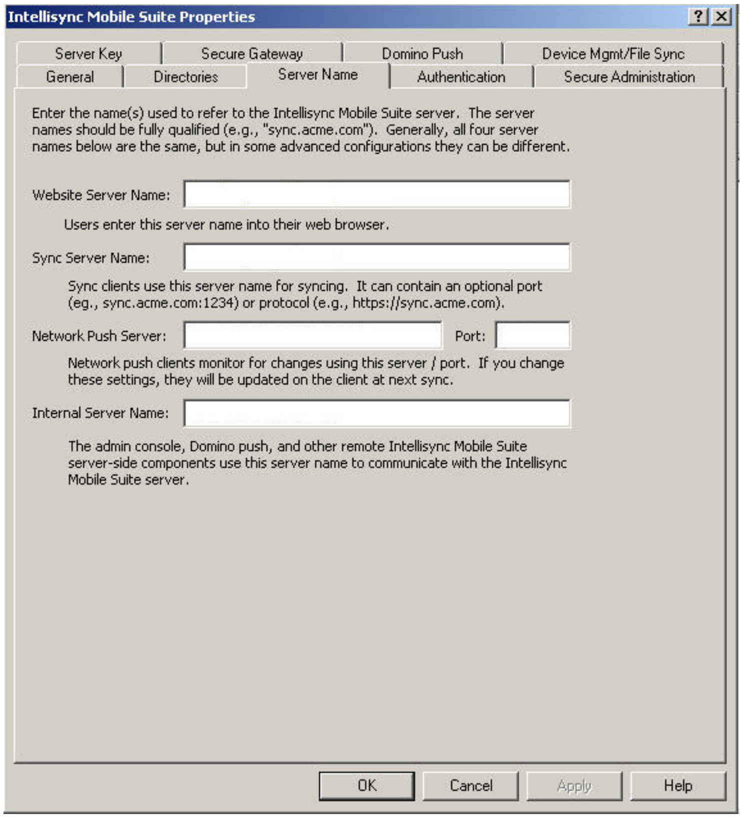


ippush.qa.domain.com
localhost

Server name can contain an optional port (eg., sg.acme.com:1234) or protocol (e.g., https://sg.acme.com). The default is http://[Server Name]:80.

6. Enter the name or IP address of the Secure Gateway server in the field and click **OK**. The Secure Gateway dialog box closes, and the server name appears in the Secure Gateway Servers field.
7. Click the **Server Name** tab.

8. Enter the Secure Gateway server name in the following fields:
   - Website Server Name
   - Sync Server Name
   - Network Push Server (this applies only to the IMS server)



Enter the name(s) used to refer to the Intellisync Mobile Suite server. The server names should be fully qualified (e.g., "sync.acme.com"). Generally, all four server names below are the same, but in some advanced configurations they can be different.

Website Server Name:

Users enter this server name into their web browser.

Sync Server Name:

Sync clients use this server name for syncing. It can contain an optional port (eg., sync.acme.com:1234) or protocol (e.g., https://sync.acme.com).

Network Push Server: Port:

Network push clients monitor for changes using this server / port. If you change these settings, they will be updated on the client at next sync.

Internal Server Name:

The admin console, Domino push, and other remote Intellisync Mobile Suite server-side components use this server name to communicate with the Intellisync Mobile Suite server.

9. Click **OK**. The Intellisync Mobile Suite Properties dialog box closes and the Secure Gateway Admin Console appears.
10. Restart the Intellisync Mobile Suite service for your changes to take effect.

Setting up a Secure Gateway cluster

You can set up multiple Secure Gateways in a cluster. A Secure Gateway cluster can provide redundancy to decrease the probability of system downtime in case one Secure Gateway server should fail.

Installing a Secure Gateway cluster

1. Install Secure Gateway on the additional server(s) you want to add to the cluster. Refer to “Installing the Secure Gateway” on page 1-4 for installation steps.
2. Choose a fault-tolerant location to store a shared path since other Secure Gateway servers in the cluster will access this location.
3. This shared path will contain a file, sgsharedprop.properties, which contains the cluster server names. This file is automatically created after you have added each server(s) to the cluster.

Modifying the securegateway.properties file

After you install Secure Gateway on each server, you must modify the securegateway.properties file on each server. To do so, complete the following steps:

1. From the C:\Program Files\SecureGateway\CommSvr\conf directory, open the securegateway.properties file.
2. Define the Secure Gateway shared path for the cluster by entering the following property:

   SecureGatewaySharedPropertiesPath=\\\\<DNS hostname or IP address>\\<drive>\\<path>\\

   This path is the fault-tolerant location for the shared properties file.
3. Restart the Secure Gateway server. If the shared properties file does not exist, it is automatically created in the shared path.
4. Repeat steps 1-3 for each server in the cluster.

Adding Secure Gateway servers to the cluster

To add the servers to the Secure Gateway cluster, complete the following steps:

1. From the shared properties path, open the sgsharedprop.properties file.
2. Define the Secure Gateway cluster servers by entering the following property fore each server:

   SecureGatewayAddress<*1-N*>=<*DNS hostname or IP address*>
3. Restart the Secure Gateway service on each server in the cluster.

   A locked copy of the shared properties file is loaded on each server in the cluster.

▶ If you are setting up a cluster outside of the shared network, you must copy the sgsharedprop.properties to each server. Any changes to the sgsharedprop.properties file will have to be manually updated on each server.

● ● ● ● ● ● ● ● ●

CHAPTER

2

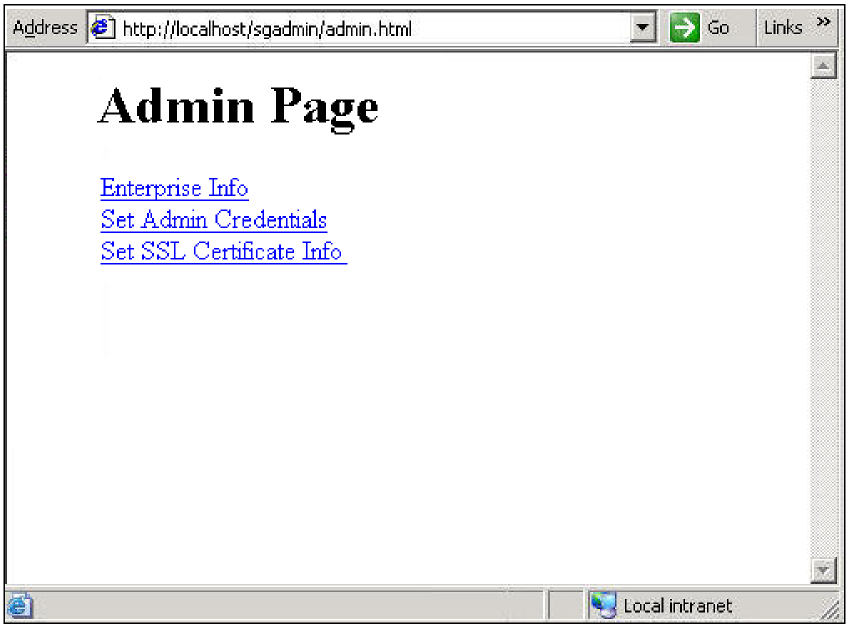
Configuring the Secure Gateway

This chapter offers information for configuring the Secure Gateway after installation.

Using the Secure Gateway Admin Console

The Secure Gateway Admin Console is a management utility located on the Secure Gateway server. To access the Secure Gateway Admin Console, enter the following URL or enter `sgadmin` from a local server:

- http://localhost/sgadmin/admin.html or localhost/sgadmin



Address http://localhost/sgadmin/admin.html

Admin Page

Enterprise Info
Set Admin Credentials
Set SSL Certificate Info

Secure Gateway Admin Console

The Secure Gateway Admin Console allows the following:

- **Enterprise Info**. Shows enterprise servers currently connected to the Secure Gateway.
- **Set Admin Credentials**. Sets up the administrator user name and password to access the Secure Gateway.
- **Set SSL Certificate Info**. Configures an SSL certificate for Secure Gateway including SSL key name and SSL key password.

Configuring the Secure Gateway properties file

You can manage your Secure Gateway configuration using the securegateway.properties file. With this file, you can configure authentication, logging, HTTP server, Web tunneling, and properties. When you modify the securegateway.properties file, you must restart the Secure Gateway service for changes to take effect.

Authentication and encryption

The following properties define and manage authentication and encryption for Secure Gateway (default values shown):

Property	Description
WebAuthenticationType=1	Sets Secure Gateway authentication type. Set value to 0 (zero) for no challenge. Set value to 1 for basic challenge.
WebCommonDomainName=	Shares authentication session credentials for multiple DNS names. If this property is not set, every DNS name is challenged. For example, test.acme.com and test2.acme.com would use WebCommonDomainName=acme.com. Used in conjunction with WebAuthenticationType when property is set to 1 (basic challenge).
AdminForceSecureConnection=0	Forces Secure Admin Console requests to be SSL when value is set to 1.
AdminTimeoutMinutes=15	Defines how long a browser-authenticated administrator session (Secure Admin Console) can remain inactive before it expires and re-authenticates.
EncryptMobileGatewayConnection=0	Turns on another layer of AES encryption between Mobile Gateway and Secure Gateway servers. Set value to 1 if Secure Gateway server is outside the corporate firewall. Regardless of this setting, all communication between the IMS server to devices is always encrypted.

Debugging and logging

The following properties define and manage debugging and audit logging for Secure Gateway (default values shown):

Property	Description
LoggingLevel=0	Sets debugging logging for Secure Gateway. Logging will appear in a file <secure_gateway_mm_dd_yyyy_n.log> located in the default installation log directory. The Secure Gateway server automatically picks up the change in two minutes. LoggingLevel property can be set from 1 (basic information) to 10 (detailed information).
SecureGatewayLogExpirationDays=8	Specifies the number of days to keep logs before deletion.

HTTP server

The following properties define and manage HTTP server settings for Secure Gateway (default values shown):

Property	Description
HttpIPAddress=	Defines the IP address to listen for HTTP connections. Defaults to all IP addresses for server.
HttpPort=80	Defines the port to listen for HTTP connections (includes Mobile Gateway servers and devices). Set to zero (0) to not listen.
SecureGatewayPort=80	Defines the port to listen for TCP connections from Mobile Gateway servers.
HttpSSLPort=443	Defines the port to listen for HTTPS connections (includes Mobile Gateway servers and devices). Set to zero (0) to not listen.

Secure Gateway cluster configuration

The following properties define and manage settings for a Secure Gateway cluster configuration (default values shown):

Property	Description
SecureGatewaySharedPropertiesPath=	Defines the path of the sgsharedprops.properties file. Used for Secure Gateway clusters.

For more information on Secure Gateway clusters, refer to “Installing a Secure Gateway cluster” on page 1-7.

Web tunneling

Secure Gateway acts as an authenticated reverse-proxy and enables you to route HTTP requests to the Mobile Gateway behind the firewall. These requests are then mapped to the correct destination by the Mobile Gateway and sent. This setup works only in the single enterprise model.

The following properties define and manage Web tunneling settings for a Secure Gateway (default values shown):

Property	Description
WebTunnelingSupported=1	Allows tunneling of Web requests to the Mobile Gateway for dispatching.
GALLookupTunnelingSupported=1	Allows tunneling of global address list (GAL) lookup Web requests to the Mobile Gateway for dispatching. Used in conjunction with the WebTunnelingSupported property. Set this property to 0 (zero) to disallow all Web traffic except GAL lookup when the WebTunnelingSupported property value is set to 1.
WebInactiveMinutes=60	Defines how long a browser-authenticated session can remain inactive before it expires and re-authenticates.
SyncMLWebTunnelingSupported=1	Handles HTTP(S) SyncML requests differently than other Web requests. Set this value to zero (0) for SyncML device requests to be routed to the default Web handler.

Property	Description
SyncMLDenyAccess=0	Allows SyncML requests as unauthenticated. Set value to 1 to disallow SyncML requests. Used in conjunction with the SyncMLWebTunnelingSupported property. To block SyncML access, set value to 1 when SyncMLWebTunnelingSupported property value is set to 1.
SyncMLForceSecureConnection=0	Forces SyncML requests to be SSL when value set to 1. Used in conjunction with the SyncMLWebTunnelingSupported property when value is set to 1.

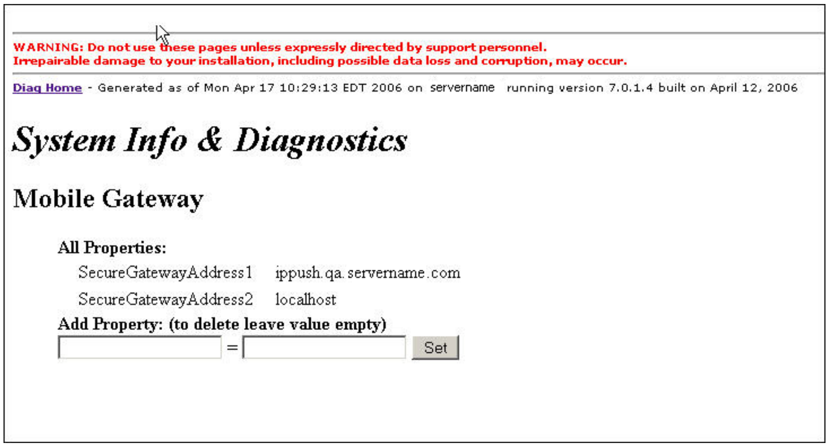
Configuring Secure Gateway to route HTTP requests

If you want to use the Secure Gateway to route HTTP requests through the firewall, you must define routing destinations.

Routing destinations are entered on the Mobile Gateway diagnostic page. These destinations control how the requests are interpreted and where the requests should be delivered.

To access the Mobile Gateway diagnostic page, complete the following steps:

1. From the Intellisync Mobile Suite Admin Console, launch WebAdmin.
2. Enter the Administrator name and password, and then click **Login**.
3. Enter the URL http://localhost/admin/diag/, and then click the **Mobile Gateway** link. The Mobile Gateway System Info and Diagnostics page appears.



WARNING: Do not use these pages unless expressly directed by support personnel.
Irrepairable damage to your installation, including possible data loss and corruption, may occur.

Diag Home - Generated as of Mon Apr 17 10:29:13 EDT 2006 on servername running version 7.0.1.4 built on April 12, 2006

System Info & Diagnostics

Mobile Gateway

All Properties:

SecureGatewayAddress1	ippush.qa.servername.com
SecureGatewayAddress2	localhost

Add Property: (to delete leave value empty)

Routing destinations can be defined two ways. The first is DNS-based, where each different destination has its own unique DNS name. The second is URL-based, where the request URL is examined and the request is routed based on the folder names in the URL.

By default, if the routing destination is SSL, and the certificate is not trusted, the Mobile Gateway will return an error to the Secure Gateway and to the Web browser.

You can set the following property to override this error:

Property	Description
WebRoutingAllowUnknownSSLCertifications	Overrides a SSL routing destination and processes the request.

To set this property enter the following:

```
WebRoutingAllowUnknownSSLCertifications = 1
```

DNS routing destinations

```
WebDNSRouting[uniqueNumber]=source,destination
```

is defined as the following:

- `source` is the Secure Gateway DNS address
- `destination` is defined as [protocol]address[:port]

Examples:

```
WebDNSRouting1=webpim.securegateway.com,localhost:8840
```

webpim.securegateway.com routes to http://localhost:8840

```
WebDNSRouting2=intranet.securegateway.com,intranet
```

intranet.securegateway.com routes to http://intranet:80

URL routing destinations

```
WebURLRouting[uniqueNumber]=source,destination,flag
```

is defined as the following:

- `source` is the first folder in the URL
- `destination` is defined as [protocol]address[:port]
- `flag` is used for specifying this is a virtual folderName and the name should be stripped from the URL before being routed

Examples:

```
WebURLRouting1=/,http://localhost:8840,0
```

http://www.securegateway.com/ routes to http://localhost

```
WebURLRouting2=en,http://localhost:8840,0
```

http://www.securegateway.com/en/login.asp routes to http://localhost/en/login.asp

```
WebURLRouting3=intranet,http://intranet,1
```

http://www.securegateway.com/intranet routes to http://intranet

Configuring Secure Gateway for SSL

SSL support is available in Secure Gateway and provides a default key file; however, you can override this value by using a provided keytool Java utility, which enables you to administer public/private key pairs and associated certificates. The keytool utility stores the keys and certificates in a keystore. The default implements the keystore as a file. It protects private/public keys with a password. These properties help configure Secure Gateway for SSL.

When you define your keystore file, you can generate a Certification Signing Request (CSR). With this CSR, you can obtain a digital certificate from a Certification Authority (CA), such as Verisign. After you have created your keystore file, you can use the Secure Gateway Admin Console to insert the encrypted values into the securegateway.properties file.

► For more information about Java Key and Certification Management keytool, refer to http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html for documentation.

To configure Secure Gateway for SSL, complete the following steps:

Create a keystore file

1. Generate the keystore file by running the keytool utility with the following parameters where <*name*>.key is a the keystore file you define:

   C:\Program Files\Secure Gateway\jre1.5.0_01\bin\keytool -genkey -keyalg RSA -alias <*Web server name*> -keystore <*name*>.key
2. Enter your keystore password, and then enter the information at the following prompts:
   - What is your first and lastname?
   - What is the name of your organizational unit?
   - What is the name of your organization?
   - What is the name of your City or Locality?
   - What is the name of your State or Province?
   - What is the two-letter country code for this unit?
3. Confirm the information entered by entering “Yes” at the prompt.
4. Enter the password for <*Web server name*>, or press return if this password is the same as your keystore password.

Generate a CSR

1. **Generate a CSR.** Run the keytool utility located with the following parameters where <*name*>.csr is the name of the CSR (for sending to a CA):

   C:\Program Files\Secure Gateway\jre1.5.0_01\bin\keytool -certreq -alias <*Web server name*> -keyalg RSA -file <*name*>.csr -keystore <*name*>.key.
2. Send the CSR file to a CA via e-mail. The CA authenticates the certificate requestor and returns a .cer file, a digitally signed certificate, via e-mail.

Import the digital certificate

1. **Import the .cer file.** Run the keytool utility with the following parameters where <*name*>.cer is the digital certificate received from the CA:

   C:\Program Files\Secure Gateway\jre1.5.0_01\bin\keytool -import -alias <*Web server name*>-trustcacerts -file <*name*>.cer -keystore <*name*>.key
2. Enter your keystore password at the prompt. The .cer file imports and a confirmation message appears.

3. **Verify your certificate.** Run the keytool utility with the following parameters where <*name*>.key is the filename you define:

   C:\Program Files\Secure Gateway\jre1.5.0_01\bin\keytool -list -v -alias <*Web server name*>-keystore <*name*>.key
4. Enter keystore password and verify the digital certificate, which includes owner, issuer, serial number, and certificate fingerprints.

Configure the SSL properties for Secure Gateway

1. Place the keystore file into the following directory or the location of your securegateway.properties file.

   C:\Program Files\Secure Gateway\Commsvr\conf
2. Log in to the Secure Gateway Admin Console by entering the following URL or entering `sgadmin` from a local server:

   /localhost/sgadmin/admin.htm
3. Select the **Set SSL Certification Info** link.
4. Enter the key file name (information located in the commsvr/conf directory).
5. Enter the password, and then enter it again in the Repeat Password field.
6. Select **Save**. The properties are added to the securegateway.properties file with the values encrypted.
7. Restart the Secure Gateway service.

● ● ● ● ● ● ● ● ●

CHAPTER

3

Troubleshooting Secure Gateway

This chapter contains helpful hints for troubleshooting Secure Gateway issues.

Troubleshooting Secure Gateway issues

This section provides steps to follow to help identify, isolate, and resolve sync or push related issues with Intellisync Mobile Suite and Secure Gateway.

Verify server name values and connections

1. From the Windows **Start** menu on the Intellisync Mobile Suite server, choose **Programs**, **Intellisync Mobile Suite**, and then choose **Admin Console**. The Intellisync Mobile Suite control appears.
2. Select Intellisync Mobile Suite in the console tree.
3. From the **Action** menu, choose **Properties**. The Intellisync Mobile Suite Properties dialog box appears.
4. Click the **Server Name** tab.
5. Verify that Sync Server Name and Network Push Server are set to the external DNS/IP address that resolves to the Secure Gateway server. (To view information on the Secure Gateway server, click the **Secure Gateway** tab.)
6. Click **OK**.
7. From the Intellisync Mobile Suite server, use Telnet to verify you can connect to the Secure Gateway.
8. From a computer connected to the Internet, use Telnet to verify you can connect to the following:
   - <SyncServerName> 80
   - <NetworkPushServer> 3102
9. Install the Intellisync Mobile Suite client on a test device and the verify that the Sync Server Name value and Network Push Server value are correct.

Verify network configuration on Intellisync server(s)

1. Add all IP addresses bound to all NICs to the hosts file, resolving to the hostname.
2. Add any IP addresses for Secure Gateway servers to the hosts file, resolving to the hostname (only required if the hostname was specified in the Intellisync Mobile Suite Admin Console).
3. If possible, verify and set the Speed and Duplex values for all NICs.
4. Verify that "ipconfig /all" returns correct and expected values.
5. Verify that "netstat -a" returns correct and expected values.

Verify network configuration on Secure Gateway server(s)

1. Add all IP addresses bound to all NICs to the hosts file, resolving to the hostname.
2. Remove all registered DNS server entries on all NICs.
3. Disable the "Register this connection's addresses in DNS" setting on all NICs.
4. Remove all registered WINS server entries on all NICs.
5. Disable the "Enable LMHOSTS lookup" setting on all NICs.
6. Set the "NetBIOS" setting to "Disable NetBIOS over TCP/IP" on all NICs.
7. Verify that "ipconfig /all" returns correct and expected values.
8. Verify that "netstat -a" returns correct and expected values.

Verify firewall router configuration

1. Verify that any nodes (usually firewalls and load balancers) between the Internet and the Secure Gateway server allow idle connections on port 80 and 3102 to stay active for longer than 15 minutes.
2. Verify that no IDS or packet inspection devices modify data on port 80 or 3102.

Test network connections

1. From a computer connected to the Internet, use a browser to verify you can access the Intellisync Mobile Suite Web site.
2. From a test device, use the browser to verify you can access the Intellisync Mobile Suite Web site.
3. Run SocketLife on the Secure Gateway server and verify that a Palm device can consistently connect to port 80 and 3102 with a Seed Time value of 1, 5 and 15. You can obtain a copy of the SocketLife program from Intellisync Technical Support.