NOKIA

Nokia Intellisync Mobile Suite Secure Gateway Administrator's Guide

Version 9.0

Published May 2008

COPYRIGHT

Copyright © 1997 - 2008 Nokia Corporation. All rights reserved. Nokia, Nokia Connecting People, Intellisync, and Intellisync logo are trademarks or registered trademarks of Nokia Corporation. Other trademarks mentioned are the property of their respective owners.

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

IMPORTANT NOTE TO USERS

THIS SOFTWARE, HARDWARE, AND DOCUMENTATION IS PROVIDED BY NOKIA INC. AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NOKIA, OR ITS AFFILIATES, SUBSIDIARIES OR SUPPLIERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Nokia operates a policy of continuous development. Therefore we reserve the right to make changes and improvements to any of the products described in this document without prior notice.

050208

Nokia Contact Information

Corporate Headquarters

Web Site	http://www.nokia.com
Telephone	1-888-477-4566 *or* 1-650-625-2000
Fax	1-650-691-2170
Mail Address	Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA

Regional Contact Information

Americas	Nokia Inc. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: info.ipnetworking_americas@nokia.com
Europe, Middle East, and Africa	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK	Tel: UK: +44 161 601 8908 Tel: France: +33 170 708 166 email: info.ipnetworking_emea@nokia.com
Asia-Pacific	438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968	Tel: +65 6588 3364 email: info.ipnetworking_apac@nokia.com

Nokia Customer Support

Web Site:	https://support.nokia.com/		
Americas		**Europe**	
Voice:	1-888-361-5030 or 1-613-271-6721	**Voice:**	+44 (0) 125-286-8900
Fax:	1-613-271-8782	**Fax:**	+44 (0) 125-286-5666
Asia-Pacific			
Voice:	+65-67232999		
Fax:	+65-67232897		

050602

Contents

About This Guide

In This Guide

This guide is organized into the following chapters:

- Chapter 1, “Installing Secure Gateway” contains instructions for installing the Secure Gateway and provides a diagram of the recommended configuration.
- Chapter 2, “Configuring Secure Gateway” offers information for configuring the Secure Gateway after installation.
- Chapter 3, “Troubleshooting Secure Gateway” contains helpful hints for troubleshooting Secure Gateway issues.

Conventions This Guide Uses

The following sections describe the conventions this guide uses, including notices, text conventions, and command-line conventions.

Notices

Warning
Warnings advise the user that bodily injury might occur because of a physical hazard.

Caution
Cautions indicate potential equipment damage, equipment malfunction, loss of performance, loss of data, or interruption of service.

Note
Notes provide information of special interest or recommendations.

Command-Line Conventions

You might encounter one or more of the following elements on a command-line path.

Table 1 Command-Line Conventions

Convention	Description
command	This required element is usually the product name or other short word that invokes the product or calls the compiler or preprocessor script for a compiled Nokia product. It might appear alone or precede one or more options. You must spell a command exactly as shown and use lowercase letters.
Italics	Indicates a variable in a command that you must supply. For example: **`delete interface if_name`** Supply an interface name in place of the variable. For example: **`delete interface nic1`**
angle brackets < >	Indicates arguments for which you must supply a value: **`retry-limit <1–100>`** Supply a value. For example: **`retry-limit 60`**

Table 1 Command-Line Conventions (*continued*)

Convention	Description
Square brackets [ ]	Indicates optional arguments. **`delete [slot slot_num]`** For example: **`delete slot 3`**
Vertical bars, also called a *pipe* (|)	Separates alternative, mutually exclusive elements. **`framing <sonet | sdh>`** To complete the command, supply the value. For example: **`framing sonet`** or **`framing sdh`**
-flag	A flag is usually an abbreviation for a function, menu, or option name, or for a compiler or preprocessor argument. You must enter a flag exactly as shown, including the preceding hyphen.
.ext	A filename extension, such as .ext, might follow a variable that represents a filename. Type this extension exactly as shown, immediately after the name of the file. The extension might be optional in certain products.
(. , ; + * - /)	Punctuation and mathematical notations are literal symbols that you must enter exactly as shown.
' '	Single quotation marks are literal symbols that you must enter as shown.

Text Conventions

Table 2 describes the text conventions in this guide.

Table 2 Text Conventions

Convention	Description
`monospace font`	Indicates command syntax, or represents computer or screen output, for example: `Log error 12453`
Key names	Keys that you press simultaneously are linked by a plus sign (+): Press Ctrl + Alt + Del.
Menu commands	Menu commands are separated by a greater than sign (>): Choose File > Open.
The words enter and type	Enter indicates you type something and then press the Return or Enter key. Do not press the Return or Enter key when an instruction says *type*.
Italics	• Emphasizes a point or denotes new terms at the place where they are defined in the text. • Indicates an external book title reference. • Indicates a variable in a command: `delete interface` *`if_name`*

Related Documentation

Nokia offers a common framework for the Intellisync Mobile Suite products. For this reason, there are electronic manuals and online help systems that cover the entire suite, plus additional resources for specific products.

For instructions to access documentation, see the following topics:

- "Accessing Server Documentation"
- "Accessing Client Documentation"

Accessing Server Documentation

In addition to this guide, there are several other documents in electronic format that are available.

Server Guides

The following server guides are available for Wireless Email. These documents are available on the Nokia Support Web site (https:// support.nokia.com) in Adobe Portable Document Format (PDF).

Nokia Intellisync Mobile Suite Installation Guide (InstallGdeEN.pdf) Includes the installation requirements and other information you need to install Nokia Intellisync Mobile Suite software for servers and clients. This guide applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Mobile Suite Administrator's Guide (AdminGdeEN.pdf) Includes an introduction to the suite and general information about using the suite successfully. This guide applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Device Management and File Sync Administrator's Guide (DeviceMgmtFileSyncGdeEN.pdf) Written as a companion book to the administrator's guide. Covers available functions and features with Device Management and File Sync.

Nokia Intellisync Corporate Email Connector Configuration Guide (CECConfigGdeEN.pdf) Covers system requirements and installation procedures for Corporate Email Connector installations using Lotus Domino and/or Microsoft Exchange.

Nokia Intellisync Secure Gateway Administrator's Guide (SecureGatewayGdeEN.pdf) Written as a companion book to the Nokia Intellisync Mobile Administrator's Guide (this guide). Covers administrative functions for managing the Secure Gateway.

Nokia Intellisync Mobile Suite Release Notes (ReleaseNotesEN.pdf) Includes important information you should know before you install and use Nokia Intellisync Mobile Suite. Also includes important late-breaking information that may not be included in other documentation. This document applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Server Online Help

The following online help systems are embedded in the server applications.

Nokia Intellisync Mobile Suite WebAdmin Console Help Includes information related to the managing the server using a Web browser.

Nokia Intellisync Mobile Suite (MMC) Admin Console Help – Management (ManagementHelpEN.chm) Includes information related to the Management control on the MMC console tree, such as Users, Groups, Reports, and Logs. This help system applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Mobile Suite (MMC) Admin Console Help – Profile Settings (ProfileHelpEN.chm) Includes information to help you use profile settings effectively. This help system applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Mobile Suite Device Management/File Sync Help (iSMiFDEN.chm) Includes information specific to Device Management and File Sync.

Accessing Client Documentation

The following electronic client documents are available on the Nokia Support Web site (https://support.nokia.com) in Adobe Portable Document Format (PDF).

Client Installation and Setup Guides

Each guide includes information for installing software on devices using a specific platform, setting synchronization settings, and synchronizing for the first time.

Table 3 Client Guides

Name	File Name
Nokia Intellisync Mobile Suite Client Guide - Palm OS Platform	PalmUsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - Pocket PC Platform	PPCUsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - Smartphone Platform	SmartphoneUsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - S60 3rd Edition Platform	Symbian60_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - S80 Platform	Symbian80_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - UIQ Platform	SymbianUIQ_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - UIQ 3rd Edition Platform	SymbianUIQ3_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - J2ME Platform	J2ME_UsersGuideEN.pdf

Note
The client guides are *not* installed as part of the client installation. You decide whether to provide this documentation to your users.

Client Online Help

The following online help systems are embedded in the Wireless Email client application.

Nokia Intellisync Mobile Suite PC Client Help Includes information about using the Nokia Intellisync Mobile Suite Client on a PC.

Nokia Intellisync Mobile Suite Web PIM Help Includes information about using the Nokia Intellisync Mobile Suite Client on a PC.

1 Installing Secure Gateway

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

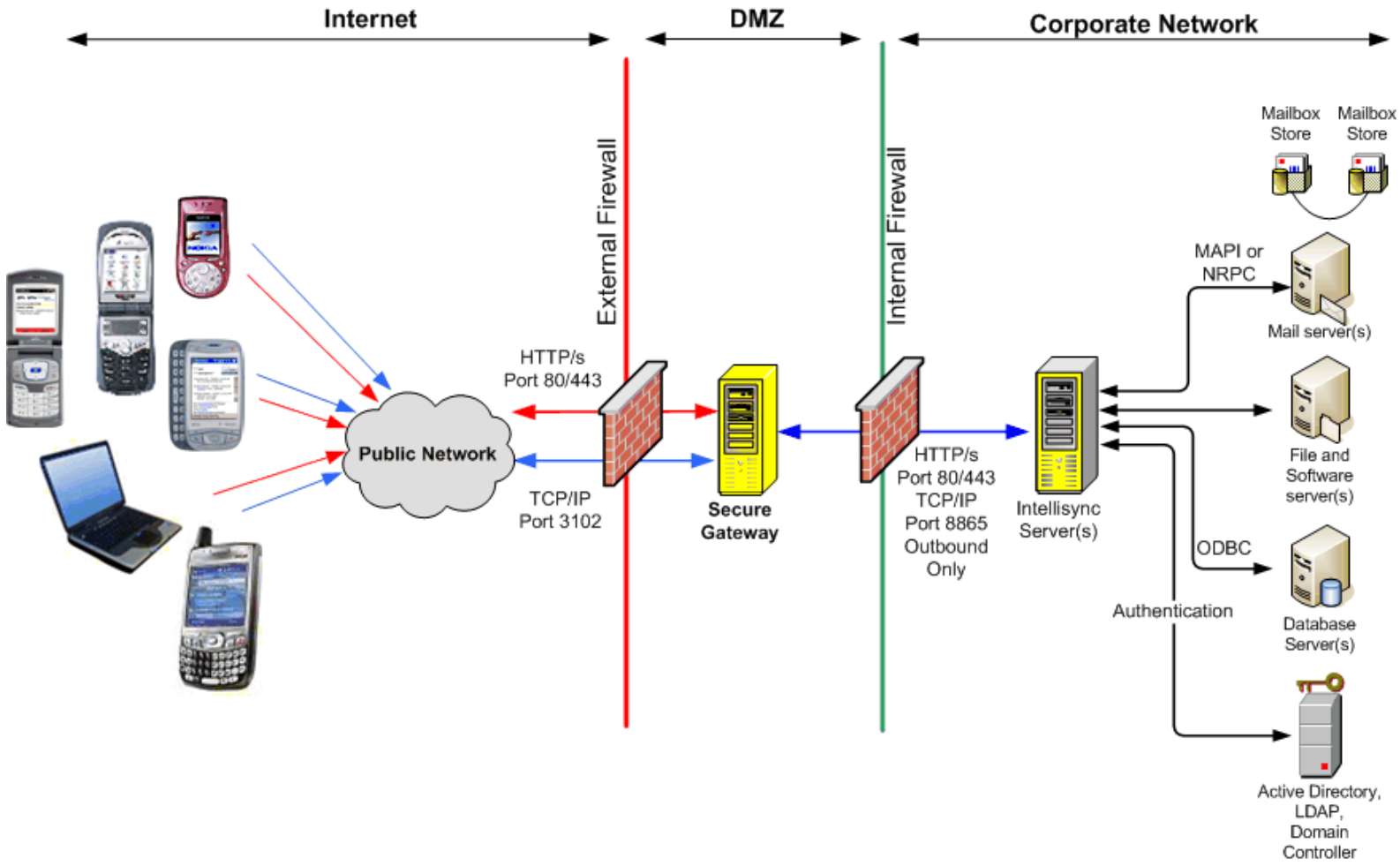
Nokia recommends using the Secure Gateway configuration within your network. The Secure Gateway offers secure and scalable communications between mobile devices and servers and consists of an HTTP listener and communications services.

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

- Push requests through TCP/IP port 3102
- Sync requests through ports 80 and 443
- Web requests through ports 80 and 443
- SMS Push requests through port 25

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.

Figure 1 Recommend Secure Gateway Configuration



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

Communication Protocol	Default Port
HTTP • Sync traffic • Web tunneling	80 (configurable)
HTTPS • Sync traffic • Web tunneling	443 (configurable)
TCP/IP Push traffic	3102 (configurable)
SMS Push	25

The following table shows the default port settings for communication from the Intellisync Mobile Suite server. Your port settings may be different depending on your network configuration.

Communication Protocol	Default Port
HTTP Outbound traffic	80 (configurable)
HTTPS Outbound traffic	443 (configurable)
TCP/IP Outbound traffic	8865 (configurable)

Note
If your security or firewall policies restrict outbound traffic to the Internet, ask your IT department to establish an outbound rule to allow HTTPS connections over the TCP 443 port to https://ccds.nokia.com.

System Requirements

The following table shows the Nokia Intellisync Mobile Suite Secure Gateway minimum requirements.

HARDWARE	
Processor	Pentium III 900MHz
Hard Disk Space	5 GB free disk space
Memory	1 GB RAM
SOFTWARE	
Operating System	Windows Server 2003 (SP1)
Browser	Microsoft Internet Explorer, v 6.0 or later
Other	MS TCP/IP Protocol network environment
OTHER REQUIREMENTS	
Permissions	Local Admin
Open port 80/443	Open port 80/443 inbound for synchronization and browser request
Open port 3102	Open port 3102 for device push connections

Installing the Secure Gateway

To install and configure the Secure Gateway

1. From the Secure Gateway folder in 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. Enter the name and 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 server on the Intellisync Mobile Suite server.

To specify the name of the Secure Gateway server

1. On the Intellisync Mobile Suite server, choose Start > Programs >Intellisync Mobile Suite > Admin Console.

   The Intellisync Mobile Suite control appears.

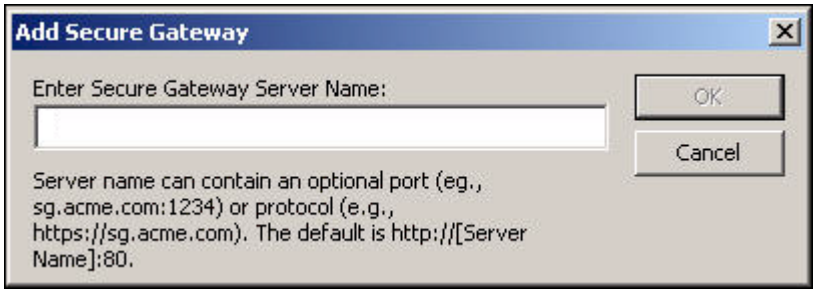
2. Select Intellisync Mobile Suite in the console tree.

3. Choose Action > Properties.

   The Intellisync Mobile Suite Properties dialog box appears.

4. Click the **Secure Gateway** tab. The Secure Gateway panel appears.

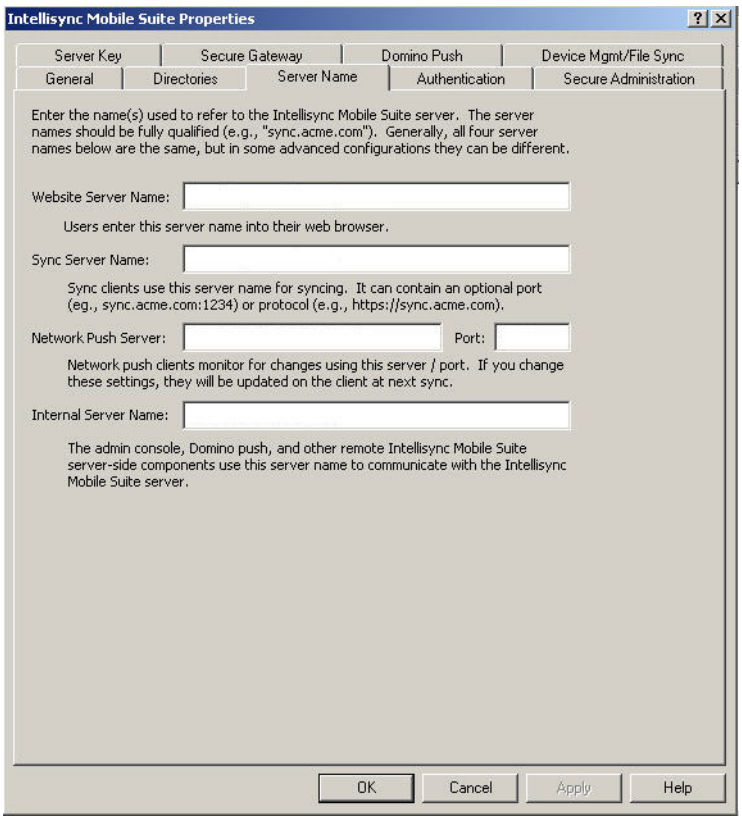
5. Click **Add**. The Add Secure Gateway dialog box appears.



6. Enter the name or IP address of the Secure Gateway server in the field and click OK. The server name can contain an optional port and/or protocol. For example: tcp://sg.acme.com:8865, sg.acme.com:1234, http://sg.acme.com:80
   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).



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:
    - Choose Start > Programs >Administrative Tools > Services.
    - Select the Intellisync Mobile Suite service.
    - Choose Action > Start.

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.

To install a Secure Gateway cluster

1. Install Secure Gateway on the additional server(s) you want to add to the cluster. For the procedure, see "System Requirements" on page 18.
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, that contains the cluster server names. This file is automatically created when you add 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 modify the securegateway.properties file

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

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.

Note
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.

2 Configuring Secure Gateway

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`

The Secure Gateway Admin Console allows the following:

Field	Description
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 Intellisync Mobile Suite service for changes to take effect. Refer to step 10 on page 20 for instructions on restarting the service.

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 "Setting Up a Secure Gateway Cluster" on page 20.

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

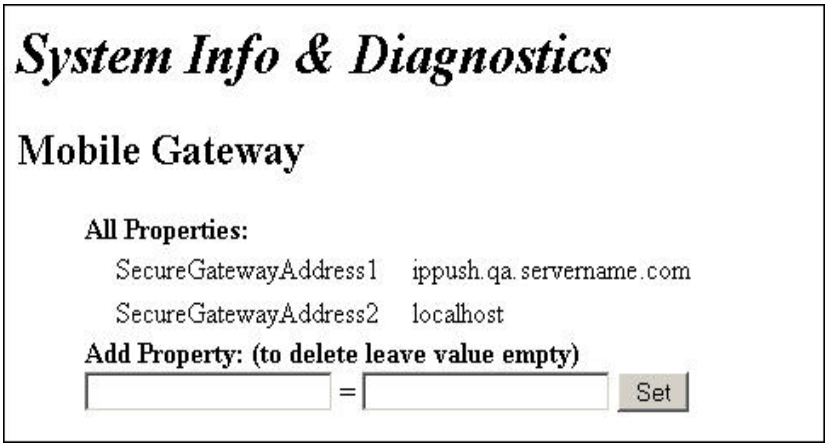
If you want to use the Secure Gateway to route HTTP requests through the firewall, you must define routing destinations.

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

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.



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.

Note
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.

Configuring the Secure Gateway for SSL entails the following procedures:

1. To create a keystore file.
2. To generate a CSR.
3. To import the digital certificate.
4. To configure the SSL Properties for Secure Gateway.

To create a keystore file

1. Generate the keystore file by running the keytool utility with the following parameters where **<**`keystore_name`**>.**`cer` and **<**`keystore_name`**>.**`key` are the file names you define:

   ```
   C:\Program Files\Intellisync Mobile Suite\jre\bin>keytool -import -alias
   www.syncube.jp -trustcacerts -file keystore_name.cer -keystore
   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.

To generate a CSR

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

   ```
   C:\Program Files\Secure Gateway\jre\bin\keytool -certreq -alias <Web server name> -keyalg RSA -file <name>.csr -keystore <name>.key
   ```

2. Send the CSR file to a CA via email. The CA authenticates the certificate requestor and returns a .cer file, a digitally signed certificate, via email.

To 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\jre\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\jre\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.

To 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.

Configuring Secure Gateway for OMA DM Edition

To configure the Secure Gateway to route Open Mobile Alliance (OMA) Device Management traffic to the OMA Device Management Edition server, you must add some routing information to the Mobile Gateway configuration.

Before You Begin

Consider the following important information before you begin configuring the Secure Gateway for the OMA Device Management Edition.

- You must know the OMA Device Management Edition server name.
- Because the OMA Device Management server uses SSL, it must have a valid certificate. If the OMA DM server does *not* have a trusted certificate, set the Mobile Gateway property as follows: WebRoutingAllowUnknownSSLCertificates=0.
- Secure Gateway authentication must be disabled if OMA Device Management Edition traffic is being routed through the Secure Gateway. To do this, open the Secure Gateway properties file and set the Web Authentication property to WebAuthenticationType=0.

To configure the Secure Gateway for OMA DM Edition

1. Using a web browser, type the following URL:
   `http://IMSServername/admin`
2. Log onto the Mobile Suite WebAdmin application.
3. Type the following URL and press Enter:

   `http://IMSServername/admin/diag.`

   A diagnostic page appears for custom configuration.
4. Under Cluster Wide Settings, choose Mobile Gateway. The All Properties field lists the existing Mobile Gateway configuration settings.

5. Under Add Property, edit the appropriate fields to add or modify the following entries so that Mobile Gateway can route the OMA Device Management traffic to the OMA Device Management server.
   - Substitute your OMA Device Management server name where you see <OMA_DM_ServerName>.
   - Substitute `<port>` with the port number used for OMA Device Management Edition traffic.

First Edit Field	Second Edit Field
`WebURLRoutingOmaDmEndUser`	`oma-dm-enduser,https://<OMA_DM_ServerName>:<port>,0`
`WebURLRoutingOmaDmConnector`	`oma-dm-connector,https://<OMA_DM_ServerName>:<port>,0`
`WebURLRoutingOmaDmMobileDev`	`mobile-dev,https://<OMA_DM_ServerName>:<port>,0`

6. Restart the Intellisync Mobile Suite service for changes to take effect. Refer to step 10 on page 20 for instructions on restarting the service.

3 Troubleshooting Secure Gateway

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, including the following:

- To verify server name values and connections
- To verify network configuration on Intellisync server(s)
- To verify network configuration on Secure Gateway server(s)
- To verify firewall router configuration
- To test network connections

To verify server name values and connections

1. From the Windows Start menu on the Intellisync Mobile Suite server, choose Programs > Intellisync Mobile Suite > 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 verify that the Sync Server Name value and Network Push Server value are correct.

To 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.

To 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 Lookupsetting 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.

To 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.

To 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.