Oracle® Communications Mobile Synchronization Gateway

Security Guide

Release 8.0

E56662-01

August 2016

Oracle Communications Mobile Synchronization Gateway Security Guide, Release 8.0

E56662-01

Contents

A Secure Deployment Checklist

Preface

This guide provides guidelines and recommendations for setting up Oracle Communications Mobile Synchronization Gateway in a secure configuration.

Audience

This document is intended for system administrators or software technicians who install and administer Mobile Synchronization Gateway.

Related Documents

For more information, see the following documents in the Mobile Synchronization Gateway Release 8.0 documentation set:

- *Mobile Synchronization Gateway Release Notes*: Describes the known issues and required third-party products and licensing.
- *Mobile Synchronization Gateway Installation and Configuration Guide*: Describes the requirements for installing Mobile Synchronization Gateway, installation procedures, and post-installation tasks.
- *Mobile Synchronization Gateway System Administrator's Guide*: Provides instructions for administering Mobile Synchronization Gateway.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

1

Mobile Synchronization Gateway Security Overview

This chapter provides an overview of Oracle Communications Mobile Synchronization Gateway security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

1. **Keep software up to date.** This includes the latest product release and any patches that apply to it.
2. **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
3. **Monitor system activity.** Establish who should access which system components, how often they should be accessed, and who should monitor those components.
4. **Install software securely.** For example, use firewalls, secure protocols (such as TLS), and secure passwords. See "Performing a Secure Mobile Synchronization Gateway Installation" for more information.
5. **Learn about and use Mobile Synchronization Gateway security features.** See "Implementing Mobile Synchronization Gateway Security" for more information.
6. **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security.
7. **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See "Critical Patch Updates and Security Alerts" on the Oracle Web site at:

   `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Understanding the Mobile Synchronization Gateway Environment

When planning your Mobile Synchronization Gateway implementation, consider the following:

- Which resources must be protected?

  For example:

  - Mobile Synchronization Gateway front end

  - Dependent resources, such as Oracle GlassFish Server and Oracle Directory Server Enterprise Edition

- From whom am I protecting the resources?

  In general, resources must be protected from everyone on the Internet. But should the Mobile Synchronization Gateway deployment be protected from employees on the intranet in your enterprise? Should your employees have access to all resources within the GlassFish Server environment? Should the system administrators have access to all resources and data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators, or restrict all system administrators from accessing the data or resources.

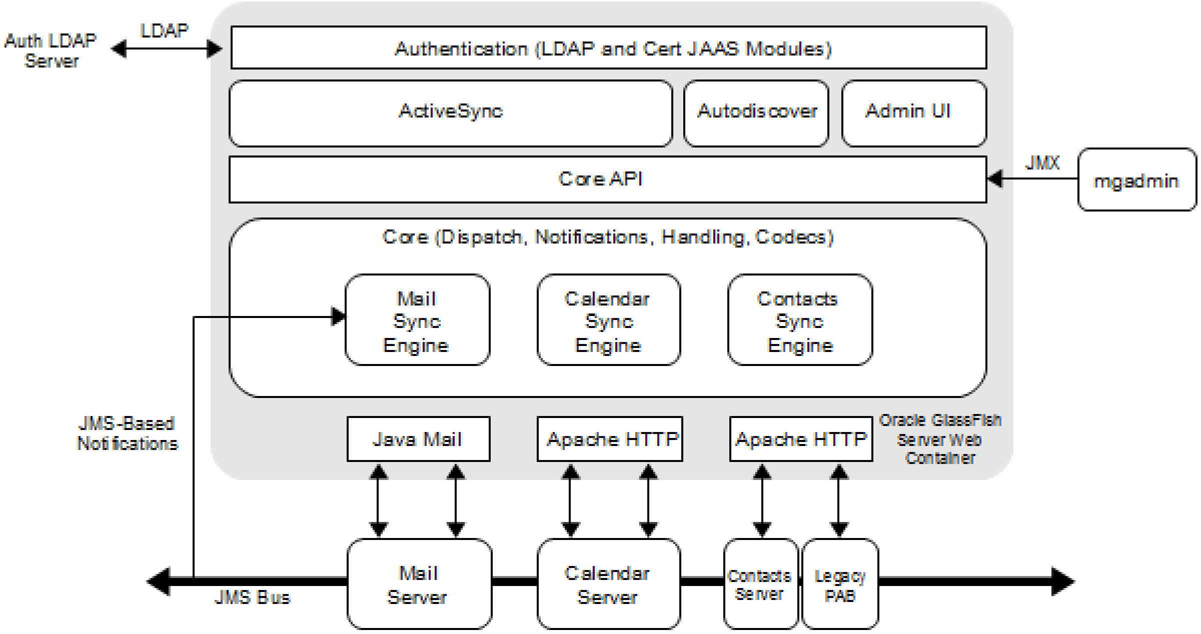
- What happens if protections on strategic resources fail?

  In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use Mobile Synchronization Gateway. Understanding the security ramifications of each resource help you protect it properly.

Overview of Mobile Synchronization Gateway Security

Figure 1–1 shows all the components that can comprise Mobile Synchronization Gateway, including the components to which it connects. Each installed or integrated component requires special steps and configurations to ensure system security.

Figure 1–1 Mobile Synchronization Gateway Components



Recommended Deployment Topologies

You can deploy Mobile Synchronization Gateway on a single host or on multiple hosts, splitting up the components into multiple front-end hosts and multiple back-end hosts. For more information, see the topic on planning your installation in *Mobile Synchronization Gateway Installation and Configuration Guide*.

The general recommended architecture is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture.

Operating System Security

This section lists Mobile Synchronization Gateway-specific OS security configurations. This section applies to all supported OSes.

Firewall Port Configuration

Mobile Synchronization Gateway communicates with various components on specific ports. Depending on your deployment and use of a firewall, you might need to ensure that the firewalls are configured to manage traffic for the following components:

- GlassFish Server administration server port (default 4848)
- Directory Server LDAPS port (default 636)
- The various Unified Communications Suite components in your deployment, including Oracle Communications Messaging Server, Oracle Communications Calendar Server, Oracle Communications Contacts Server, and Oracle Communications Convergence

Close all unused ports, especially non-secure ports. Opt for TLS-enabled ports, instead of non-SSL ports, for all communications (for example: HTTPS, IIOPS, t3s).

For more information about securing your OS, see your OS documentation.

Secure Communications

Secure connections between applications connected over the World Wide Web can be obtained by using protocols such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). SSL is often used to refer to either of these protocols or a combination of the two (SSL/TLS). Due to a security problem with SSLv3, Mobile Synchronization Gateway recommends the use of only TLS. However, throughout this guide, secure communications may be referred to by the generic term SSL.

In a Mobile Synchronization Gateway deployment, you can enable the use of TLS between the following components:

- GlassFish Server and client connections
- Mobile Synchronization Gateway and Directory Server
- GlassFish Server and the JMX port used by Mobile Synchronization Gateway administration utility
- Mobile Synchronization Gateway and the back-end Unified Communications Suite servers

See "Implementing Mobile Synchronization Gateway Security" for more information.

LDAP Security

To enhance client security in communicating with Directory Server, use a strong password policy for user authentication. For more information on securing Directory

Server, see the topic on security in *Oracle Directory Server Enterprise Edition Administration Guide*.

2

Performing a Secure Mobile Synchronization Gateway Installation

This chapter presents planning information for your Oracle Communications Mobile Synchronization Gateway system and describes recommended deployment topologies that enhance security.

For more information about installing Mobile Synchronization Gateway, see *Mobile Synchronization Gateway Installation and Configuration Guide*.

Installing Infrastructure Components Securely

Mobile Synchronization Gateway is deployed within Oracle GlassFish Server. When installing and configuring GlassFish Server:

- Configure HTTPS and disable HTTP.
- Configure the JMX port for GlassFish Server to use TLS.
- Configure GlassFish Server to prevent Denial of Service (DoS) attacks.

To configure and administer GlassFish Server security, see *Oracle GlassFish Server Security Guide*.

Credentials Needed to Install Mobile Synchronization Gateway Components

The installation prompts for authentication credentials for the following:

- GlassFish Server administrator
- Oracle Directory Server Enterprise Edition (Directory Server) manager (bind DN and password)
- Oracle Communications Contacts Server administrator and password
- SMTP server administrator and password
- IMAP server administrator and password
- Oracle Communications Calendar Server administrator and password
- Oracle Communications Convergence proxy administrator and password

Post-Installation Configuration

After installation, configuring Mobile Synchronization Gateway for a secure deployment involves these steps:

1. Make sure that HTTPS is configured correctly on the front-end GlassFish Server host:
   - Use a CA signed certificate.
   - Set the TLS port to the default 443 to ease client configurations.
2. Disable HTTP on the front-end GlassFish Server host.
3. Configure the JMX port for GlassFish Server to use TLS.
4. Enable LDAP TLS, if not previously done.
5. Enable secure SMTP.
6. Enable secure IMAP.
7. Enable a secure connection to Calendar Server.
8. Enable a secure connection to Contacts Server.
9. Enable a secure connection to Convergence Personal Address Book.
10. Add LDAP access control for Mobile Synchronization Gateway.

See "Implementing Mobile Synchronization Gateway Security" for more information.

3

Implementing Mobile Synchronization Gateway Security

This chapter explains the security features of Oracle Communications Mobile Synchronization Gateway and the following tasks:

- Configuring HTTPS on Front-End GlassFish Server Hosts
- Disabling SSLv3 on Front-End GlassFish Server Hosts
- Disabling HTTP on Front-End GlassFish Server Hosts
- Enabling LDAP SSL in Mobile Synchronization Gateway
- Enabling Secure Mail
- Enabling Secure Calendar
- Enabling Secure Contacts Server
- Enabling Secure Personal Address Book
- Configuring and Using Authentication
- Configuring and Using Access Control
- Making Mobile Synchronization Gateway and GlassFish Server Secure
- Detecting Possible Security Issues

About System Security in Mobile Synchronization Gateway

Security requirements arise from the need to protect data: from accidental loss and corruption, and from deliberate unauthorized attempts to access or alter that data. Secondary concerns include protecting against undue delays in accessing or using data, and against interference to the point of denial of service.

The critical security features that provide these protections are:

- Authentication
- Access control
- Secure communications

Authentication is the way in which an entity (a user, an application, or a component) determines that another entity is who it claims to be. An entity uses security credentials to authenticate itself. The credentials might be a user name and password, a digital certificate, or something else. Usually, servers or applications require clients to authenticate themselves. Additionally, clients might require servers to authenticate themselves. When authentication is bidirectional, it is called *mutual authentication*.

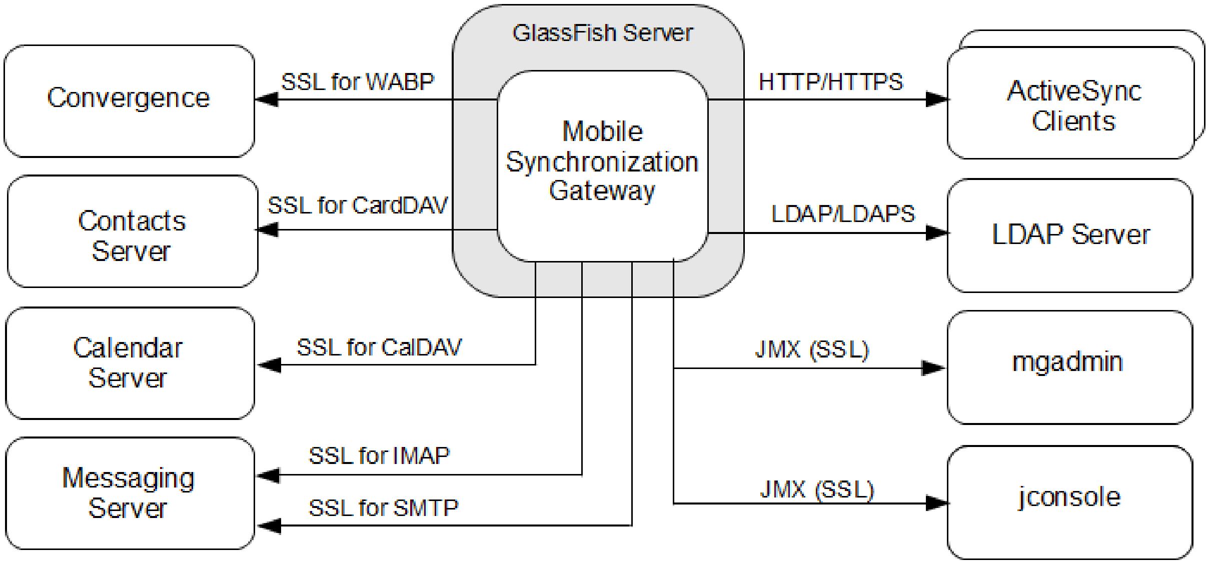
Access control, also known as authorization, is the means by which users are granted permission to access data or perform operations. After a user is authenticated, the user's level of authorization determines what operations the user can perform.

Secure communications typically means using the SSL protocol to provide encryption of data between the server and the respective components.

Mobile Synchronization Gateway supports LDAP authentication. In addition, Mobile Synchronization Gateway is able to rely on the Access Control Instructions (ACIs) used by back-end Unified Communications Suite servers to grant end users permission to search the LDAP directory for other users and resources.

Figure 3–1 shows the protocols and communication flows used by Mobile Synchronization Gateway that can be secured. The HTTPS, LDAPS, JMX, SMTPS, IMAP, CardDAV, and WABP protocols must be secured by using SSL.

Figure 3–1 Mobile Synchronization Gateway Protocol Flows



In the preceding figure, HTTPS and SSL provide encryption of data between the server and the respective components. You configure Mobile Synchronization Gateway to use SSL for SMTP, IMAP, CardDAV, CalDAV, and WABP by setting an **enablessl** parameter for each protocol. Configuring Mobile Synchronization Gateway to use SSL is covered later in this chapter.

For more information on the **enablessl** parameters, see "Mobile Synchronization Gateway Configuration Parameters" in *Mobile Synchronization Gateway Installation and Configuration Guide*.

See "Enabling LDAP SSL in Mobile Synchronization Gateway" for information on LDAPS.

Note: SSL is often used to refer to either SSL or TLS protocols or a combination of the two (SSL/TLS). Throughout this chapter, secure communications may be referred to by the generic term SSL.

Configuring HTTPS on Front-End GlassFish Server Hosts

To configure HTTPS on the front-end Oracle GlassFish Server host, perform the following tasks:

- Installing an Official Certificate
- Setting SSL Default Port to 443

Installing an Official Certificate

The default GlassFish Server installation comes with a self-signed certificate, which is incompatible with production usage. To install an official certificate, see the topic on configuring GlassFish Server to use a Certificate Authority issued certificate in *Calendar Server System Administrator's Guide*.

Setting SSL Default Port to 443

Most clients assume that the GlassFish Server is running on the default SSL port number (443). If you did not set the GlassFish Server default SSL port to 443 during installation, perform this task to do so.

To set the default SSL port to 443:

1. List all the HTTP listeners. For example:

```
asadmin list-http-listeners
http-listener-1
http-listener-2
admin-listener
Command list-http-listeners executed successfully.
```

2. Determine which SSL listener (which will have an attribute of **security-enabled=true**). For example:

```
asadmin get
server.network-config.protocols.protocol.http-listener-1.security-enabled
server.network-config.protocols.protocol.http-listener-1.security-enabled=fals
e
Command get executed successfully.

asadmin get
server.network-config.protocols.protocol.http-listener-2.security-enabled
server.network-config.protocols.protocol.http-listener-2.security-enabled=true
Command get executed successfully.

asadmin get
server.network-config.protocols.protocol.admin-listener.security-enabled
server.network-config.protocols.protocol.admin-listener.security-enabled=false
Command get executed successfully.

asadmin get
server.network-config.network-listeners.network-listener.http-listener-2.port
server.network-config.network-listeners.network-listener.http-listener-2.port=
8181
Command get executed successfully.
```

3. Set the port number of the SSL listener to 443. For example:

```
asadmin set
server.network-config.network-listeners.network-listener.http-listener-2.port=
443
```

```
server.network-config.network-listeners.network-listener.http-listener-2.port=
443
Command set executed successfully.
```

This change does not require you to restart GlassFish Server.

Disabling SSLv3 on Front-End GlassFish Server Hosts

Identify the http-listener for the publicly accessible port that has SSL/TLS enabled (**security-enabled=true**) on which requests for Mobile Synchronization Gateway are received. Ensure that SSLv3 is disabled for this listener by setting the option **ssl3-enabled** to **false**.

1. Identify the HTTP listeners that have SSL/TLS enabled (**security-enabled=true**) and verify whether SSLv3 is enabled on that listener (**ssl3-enabled=true**).

```
asadmin get configs.config.server-config.network-config.protocols.protocol.* |
grep http-listener.*security-enabled=true
configs.config.server-config.network-config.protocols.protocol.http-listener-2
.security-enabled=true

asadmin get
configs.config.server-config.network-config.protocols.protocol.http-listener-2
.ssl.ssl3-enabled
configs.config.server-config.network-config.protocols.protocol.http-listener-2
.ssl.ssl3-enabled=true
Command get executed successfully.
```

2. Disable those HTTP listeners.

```
asadmin set
configs.config.server-config.network-config.protocols.protocol.http-listener-2
.ssl.ssl3-enabled=false
configs.config.server-config.network-config.protocols.protocol.http-listener-2
.ssl.ssl3-enabled=false
Command set executed successfully.
```

3. Restart GlassFish Server.

Disabling HTTP on Front-End GlassFish Server Hosts

Disable non-SSL HTTP access to prevent any unsecured communications with Mobile Synchronization Gateway.

1. List all the HTTP listeners and note the ones that do not have security enabled. For example:

```
asadmin get
configs.config.server-config.network-config.network-listeners.network-listener
.http-listener-1.enabled
configs.config.server-config.network-config.network-listeners.network-listener
.http-listener-1.enabled=true
Command get executed successfully.
```

2. Disable those HTTP listeners. For example:

```
asadmin set
configs.config.server-config.network-config.network-listeners.network-listener
.http-listener-1.enabled=false
configs.config.server-config.network-config.network-listeners.network-listener
```

```
.http-listener-1.enabled=false
Command set executed successfully.
```

This change does not require you to restart GlassFish Server.

Enabling LDAP SSL in Mobile Synchronization Gateway

If you specified to use an LDAPS URL during the Mobile Synchronization Gateway initial configuration, the changes described in this section were already performed by the **init-config** script.

You must have already enabled the back-end Oracle Directory Server Enterprise Edition host for SSL, either with a CA-signed certificate or self-signed certificate.

To configure Mobile Synchronization Gateway to communicate with Directory Server over SSL:

1. Copy the **cert8.db** and **key3.db** files to the *MobileSyncGateway_home*/**lib/** directory.
2. Create a text file, for example, **usessl.txt**, with the following content:

   ```
   base.ldapinfo.authldap.ldapport=port_number
   base.ldapinfo.authldap.ldapusessl=true
   base.ldapinfo.ugldap.ldapport=port_number
   base.ldapinfo.ugldap.ldapusessl=true
   ```

   Change the *port_number* values to the LDAP SSL port value in your deployment.
3. Run the **mgadmin config** command to make the configuration change:

   ```
   mgadmin config -u admin -f usessl.txt
   ```

   Warning messages appear that tell you to restart GlassFish Server.
4. Restart GlassFish Server:

Enabling Secure Mail

You can secure both SMTP and IMAP email communication with Mobile Synchronization Gateway. If you specified to use SSL during the Mobile Synchronization Gateway initial configuration, the changes described in this section were already performed by the **init-config** script.

To enable secure email communication for Mobile Synchronization Gateway:

1. To use SSL with SMTP, set the **smtp.enablessl** configuration parameter to **`true`** and set the **smtp.port** configuration parameter to the SMTP SSL port, typically 465.

   ```
   mgadmin config modify -o smtp.enablessl -v true
   mgadmin config modify -o smtp.port -v 465
   ```

2. To use SSL with IMAP, set the **imap.enablessl** configuration parameter to **`true`** and set the **imap.port** configuration parameter to the IMAP SSL port, typically 993.

   ```
   mgadmin config modify -o imap.enablessl -v true
   mgadmin config modify -o imap.port -v 993
   ```

Enabling Secure Calendar

You can secure Oracle Communications Calendar Server communication by using SSL transport. If you specified to use SSL during the Mobile Synchronization Gateway initial configuration, the changes described in this section were already performed by the **init-config** script.

To enable secure Calendar Server communication for Mobile Synchronization Gateway:

- Set the **caldav.enablessl** configuration parameter to **`true`** and set the **caldav.port** configuration parameter to the SSL port.

```
mgadmin config modify -o caldav.enablessl -v true
mgadmin config modify -o caldav.port -v port
```

Enabling Secure Contacts Server

You can secure Oracle Communications Contacts Server communication by using SSL transport. If you specified to use SSL during the Mobile Synchronization Gateway initial configuration, the changes described in this section were already performed by the **init-config** script.

To enable secure Contacts Server address book communication for Mobile Synchronization Gateway:

- Set the **carddav.enablessl** configuration parameter to **`true`** and set the **carddav.port** configuration parameter to the SSL port.

```
mgadmin config modify -o carddav.enablessl -v true
mgadmin config modify -o cardav.port -v port
```

Enabling Secure Personal Address Book

You can secure Oracle Communications Convergence Personal Address Book (PAB) communication by using SSL transport. If you specified to use SSL during the Mobile Synchronization Gateway initial configuration, the changes described in this section were already performed by the **init-config** script.

To enable secure PAB communication for Mobile Synchronization Gateway:

- Set the **wabp.enablessl** configuration parameter to **`true`** and set the **wabp.port** configuration parameter to the SSL port.

```
mgadmin config modify -o wabp.enablessl -v true
mgadmin config modify -o wabp -v port
```

Configuring and Using Authentication

For information on Mobile Synchronization Gateway and LDAP authentication, see the topic on provisioning users in *Calendar Server System Administrator's Guide*.

Configuring and Using Access Control

For information on configuring access control, see the topic on administering access in *Calendar Server System Administrator's Guide*.

Making Mobile Synchronization Gateway and GlassFish Server Secure

To make GlassFish Server more secure for Mobile Synchronization Gateway, perform the following tasks:

- Preventing Denial of Service Attacks on GlassFish Server
- Configuring JMX Port for GlassFish Server to Use SSL

Preventing Denial of Service Attacks on GlassFish Server

Using GlassFish Server, you can prevent a Denial of Service (DoS) attack against the server by:

- Limiting the size of a POST request
- Specifying a request timeout value
- Creating a blacklist of host names, IP addresses, or both

For more information, see the topic on DoS prevention in *Calendar Server System Administrator's Guide*.

Configuring JMX Port for GlassFish Server to Use SSL

GlassFish Server does not enable the JMX port with SSL by default. If you want to make the JMX communications secure, you must enable security for GlassFish Server, either through the Administration Console, or through the **asadmin** command.

The **mgadmin** command uses the JMX protocol to connect to GlassFish Server. This section describes how to create secure communications between the **mgadmin** command and the Mobile Synchronization Gateway host over SSL. To do so, you need to create a **trustStore** file for **mgadmin**. If you are using SSL for communicating with GlassFish Server, you must also configure JMX to use SSL.

To create secure communications between **mgadmin** and Mobile Synchronization Gateway:

1. Export the server certificate that GlassFish Server is using for SSL.

   Depending on the GlassFish Server version, you might use the Java **keytool** command or the Network Security Services (NSS) **certutil** command to export the certificate.

   In these examples, the current directory is the GlassFish Server configuration directory and the certificate is named **s1as**.

   - Example **keytool** command:

     ```
     keytool -exportcert -keystore keystore.jks -storetype JKS -alias s1as -rfc
     -file /tmp/s1as.txt
     ```

   - Example **certutil** command:

     ```
     /usr/sfw/bin/certutil -L -d . -n s1as -a > /tmp/s1as.txt
     ```

2. Import the GlassFish Server certificate into a Java **keystore** for use by the **mgadmin** command with the **-s** option.

   For example:

   ```
   keytool -importcert -alias s1as -file /tmp/s1as.txt -keystore
   /var/opt/sun/comms/mobile/config/mgtruststore -storetype JKS
   ```

3. Modify the **/var/opt/sun/comms/mobile/config/mgservercreds.properties** file to reflect the new **trustStore** file created in the previous step.

   Add the following line:

   ```
   secure=/var/opt/sun/comms/mobile/config/mobiletruststore
   ```

   Alternately, you could specify the explicit path to the **trustStore** file in the **mgadmin** command with the **-s** option.

   For example:

   ```
   mgadmin config modify -o parameter -v value -s /my_home/my_truststore
   ```

4. In the GlassFish Server Administration Console, enable secure JMX.

   a. Navigate to **Configurations**.

   b. Navigate to **server-config**.

   c. Navigate to **Admin Service**.

   d. On the **JMX Connector** tab, select the **Enabled** box for Security.

   e. On the **SSL** tab, set the **Certificate Nickname** to the certificate's alias that you used when you created the certificate.

Detecting Possible Security Issues

You can use the Mobile Synchronization Gateway log files to look for security problems. This section lists a few security-related log messages.

Login errors resemble the following:

```
INFO [2014-01-08T11:20:44.529-0600] <...LDAPLoginModule.lookupUser> Error while
retrieving user info for user User: No results found
```

If you have the log level set to FINEST, then you see messages resembling the following when a login error occurs:

```
FINEST [2014-01-08T11:36:56.304-0600] <...WCAPServlet.service> failed login or
session timeout
```

If a user is trying to bypass the data parsing, you see warnings such as the following:

```
FINE [2014-01-08T11:39:53.426-0600] <...RESTServlet.service> Got a non standard
condition: failed to parse - Error at line 4:Illegal property [BEGI]
```

An unusually high number of requests (REQ) from the same IP address shows up as the following in the commands log file:

```
Sample request log entry....
[2014-01-07T03:39:05.454-0700] <3887> NabServlet [REQ] REPORT
/nabserver/principals/jsmith IP_address server:port
```

A

Secure Deployment Checklist

This appendix provides guidelines to help you secure Oracle Communications Mobile Synchronization Gateway and its components.

Secure Deployment Checklist

The following security checklist provides guidelines to help you secure Mobile Synchronization Gateway and its components.

- Install only the components you require.
- Lock and expire default user accounts.
- Use a strong LDAP password policy for user authentication.
- Restrict, control, and revisit user privileges:
  - Grant only the necessary privileges to each user.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Enforce access controls effectively and authenticate clients stringently.
- Restrict network access by doing the following:
  - Use firewalls.
  - Never leave an unnecessary hole in a firewall.
  - Password-protect the Oracle listener against remote access.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Restrict system access by IP addresses.
  - Encrypt network traffic.
- Apply all security patches and workarounds.
- Encrypt sensitive information.