Oracle® Communications Services Gatekeeper

Security Guide

Release 5.1

E36134-01

June 2013

ORACLE®

Oracle Communications Services Gatekeeper Security Guide, Release 5.1

E36134-01

Contents

4 Securing Partner Accounts and Services

Preface

This guide explains concepts and tasks necessary to securely implement Oracle Communications Services Gatekeeper (Services Gatekeeper).

Audience

This document is intended for system administrators and system integrators who secure services in a Services Gatekeeper implementation.

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 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.

Related Documents

For more information, see the following documents in the Oracle Communications Services Gatekeeper Release 5.1 documentation set:

- *Oracle Communications Services Gatekeeper Concepts Guide*
- *Oracle Communications Services Gatekeeper Installation Guide*
- *Oracle Communications Service Gatekeeper Administrator's Guide*
- *Oracle Communications Service Gatekeeper OAuth Guide*

Services Gatekeeper is partially based on the Oracle WebLogic Server, and these Oracle Fusion Middleware documents are also useful:

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*

See the Oracle WebLogic documentation at: http://docs.oracle.com/cd/E24329_01/index.htm

1

Services Gatekeeper Security Overview

This chapter provides an overview of the Oracle Communications Services Gatekeeper (Services Gatekeeper) security features and considerations.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date**. This includes the latest product release and any patches that apply to it.
- **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.
- **Monitor system activity**. Establish who should access which system components, and how often, and monitor those components.
- **Install software securely**. For example, use firewalls, secure protocols such as SSL and secure passwords. See "Performing a Secure Services Gatekeeper Installation" for details.
- **Learn about and use the Services Gatekeeper runtime security features**. See "Administering Services Gatekeeper Security" for more information.
- **Use secure development practices**. For example, take advantage of existing database security functionality instead of creating your own application security. See "Securing Partner Accounts and Services" for more information.
- **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 the "Critical Patch Updates and Security Alerts" Web site:

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

Overview of Services Gatekeeper Security

It is useful for you to read through the *Oracle Communications Services Gatekeeper Concepts Guide* before reading this manual to get an understanding of how Services Gatekeeper works.

Services Gatekeeper is a hardened extension of WebLogic Server 11g that you use to serve TCP/IP applications (services) on telephony networks. It includes tools to connect to telephony networks, and make these services available to subscribers using these networks. These services are generally third-party applications that external developers provide, and Services Gatekeeper provides a Partner Manager Portal that

developers (partners) use to manage their services. Services Gatekeeper relies on a database to maintain information about Services Gatekeeper.

Services Gatekeeper can function as a single point of contact for access to the functionality of the underlying network, providing common authentication, authorization, and access control procedures for all applications, both internal and partner-provided.

Services using SOAP-based interfaces can leverage the flexible security framework of Oracle WebLogic Server 11gR1PS2 to provide robust system protection. Applications can be authenticated using plaintext or encrypted (digest) passwords, X.509 certificates, or SAML 1.0/1.1 tokens.

Service requests can use XML encryption based on the W3C standards, for either the whole request message or specific parts of it. And, to ensure message integrity, requests can be digitally signed, using the W3C XML digital signature standards.

Services using RESTful interfaces can leverage HTTP basic authentication: username/password and SSL protection.

Implementing a secure Services Gatekeeper implementation falls generally in to these categories:

- Pre-installation tasks, that include installing a database and creating database users.
- Perform a secure installation of Services Gatekeeper by:
  - Installing a database and create and authorize database users.
  - Installing Services Gatekeeper in a clustered deployment (separate application and networking tiers) so that the individual components are easier to defend.
  - Creating Services Gatekeeper administrative users to administer Services Gatekeeper and any third-party services developers.
  - Securing the WebLogic server.
  - Securing JDBC with database credentials.
  - Securing domains with RDBMS security.
  - Obtaining and installing firewalls between the tiers for protection.
  - Controlling access to Services Gatekeeper Oracle Access Manager MBeans that control OAM functionality.
  - Securing your web services, and ensure that your partners do the same.
  - Securing Oracle Service Bus and the Service Oriented Architecture Facades.
  - Securing geographically redundant deployments.
  - Adding a custom password validator (optional).
  - Obtaining and install a custom password validator (optional).
  - Obtaining and install Java Cryptography Extension (optional).
- Administer your Services Gatekeeper implementation securely by:
  - Creating and maintaining administrative users with just the authorization levels that they require.
  - Monitoring Services Gatekeeper and the underlying WebLogic server for security attacks.

  - Assigning administrative users to monitor partner activity and approve their accounts.
  - Assigning a security contact to create and administer Services Gatekeeper Service Level Agreements (SLAs) that define access to Services Gatekeeper.
  - Backing up your Services Gatekeeper implementation.
- Set up the Services Gatekeeper Partner Portals to allow partner to securely create accounts for themselves and register their services.
- Educate partners to:
  - Enable security for communication services, including using SLAs for authorization and protocol security for authentication. SOAP-based, RESTful, and native (M7, SMPP, and UCP) all have their own secure interfaces.
  - Service interceptors can also shop secure communication services.
  - Use Oracle OAuth to manage access to secured resources (such as pictures or secured URLs).
  - Administer your partners with Partner Manager Portal. This includes:
    * Recording their Partner Portal credentials somewhere safe.
    * Changing their automatically-generated application IDs as soon as possible because they are is predictable

These tasks are explained in the chapters that follow.

About the Services Gatekeeper Environment

When planning your Services Gatekeeper implementation, consider the following:

- Which resources need to be protected?
  - You must protect subscriber data, such as credit-card numbers.
  - You must protect internal data, such as the MBeans that control Services Gatekeeper.
  - You must protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?**

  For example, you must protect partner data from other partners, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, a system administrator might manage your system components without needing to access the system data.
- **What will happen if protections on a strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly

Security Standards and Specifications

See the discussion on security standards and specifications in *Oracle Communications Services Gatekeeper Concepts Guide* for a list of the security-related standards that Services Gatekeeper supports.

2

Performing a Secure Services Gatekeeper Installation

This chapter explains the steps necessary to securely install Oracle Communications Services Gatekeeper (Services Gatekeeper).

Installing Services Gatekeeper Securely

The following sections explain how to install Services Gatekeeper securely.

Recommended Deployment Configurations

See *Oracle Communications Services Gatekeeper Deployment Guide* for a description of the Services Gatekeeper components, and a discussion of how to protect them from software attack. *Oracle Communications Services Gatekeeper Deployment Guide* also explains the deployment templates that Services Gatekeeper includes for deploying the different types of deployments that Services Gatekeeper supports.

The discussion on XML appliances in *Oracle Communications Services Gatekeeper Deployment Guide* explains where your firewalls should be situated to protect your Services Gatekeeper components.

Pre-Installation Tasks

This section explains security-related tasks that you perform before installing Services Gatekeeper.

Implementing Database Security

Before installing Services Gatekeeper, you must install a database to support Services Gatekeeper information. See the discussion on supported databases in *Oracle Communications Services Gatekeeper Installation Guide* for a list of the supported databases.

Oracle strongly recommends that you deploy the Services Gatekeeper database in its own tier, for both security and performance reasons. See *Oracle Communications Services Gatekeeper Deployment Guide* for more details.

Creating and Authorizing Database Users

Your database must have a database user for Services Gatekeeper with an unlimited quota and have privileges to create sessions and tables. Record and protect these credentials as you would any other administrative password. You reference them during domain configuration. See the discussions on defining a database user for the

Oracle Database and configuring domain settings in *Oracle Communications Services Gatekeeper Installation Guide* for details.

Installing Services Gatekeeper Securely

You perform a secure Services Gatekeeper installation by:

- Installing Services Gatekeeper in a clustered deployment (separate application and networking tiers) so that the individual components are easier to defend.
- Obtaining and installing firewalls between the tiers for protection. See "Securing Services Gatekeeper Components with Firewalls" for more information.
- Creating Services Gatekeeper administrative users to administer Services Gatekeeper and any third-party services developers. See "Creating Administrative Users" for more information.
- Obtaining and installing Java Cryptography Extension (optional).
- Obtaining and installing a custom password validator (optional).

See the *Oracle Communications Services Gatekeeper Installation Guide* for instructions on how to perform these tasks. The sections that follow provide more information.

Securing Services Gatekeeper Components with Firewalls

Firewalls are essential for securing production implementations, but may be omitted for test and evaluation implementations. See *Oracle Communications Services Gatekeeper Deployment Guide* for examples of where to place firewalls in your implementation.

Creating Administrative Users

You create two different types of administrative users: *traffic users* are application instances that use application-facing instances to send traffic, and *management users* that administer Services Gatekeeper itself. You collect these types of users into groups to more easily manage them.

Every implementation must have a main administrator user that you create when you first configure a domain, by entering the username and password. Record and protect these credentials because the main administrator user has the power to grant or deny access for all other users. See the discussions on configuring administrator user names and passwords in *Oracle Communications Services Gatekeeper Installation Guide* for details on creating the main administrator user.

Create as few management users as possible, protect their credentials, and have procedures in place that allow you to quickly remove management users as they are relieved of responsibility.

You also need to create traffic users (application instances) that use the application-facing instances to send traffic, and other management users to manage and administer Services Gatekeeper itself. See the discussion on managing management users and management user groups in *Oracle Communications Services Gatekeeper System Administrator's Guide* for details. That discussion also contains the APIs that you use to manage traffic and management users.

Creating a Secure Services Gatekeeper Implementation

This section explains security-related tasks that you perform during and immediately after installing Services Gatekeeper, but before you put it into production.

Securing the Domain

For information on securing Services Gatekeeper domains, see the discussion on RDBMS security store in *Oracle Communications Services Gatekeeper Installation Guide*.

Securing the WebLogic Server

Services Gatekeeper is based on a WebLogic server, and it share many of the same security concerns. For example:

- The ability to use SSL/TLS security to protect web-based traffic.
- The ability to use a credential store to protect web-based traffic.
- The ability to create single sign-on (SSO) logins for your subscribers (or your customer's subscribers).

For an overview and details, see *Oracle Fusion Middleware Securing Oracle WebLogic Server* here: `http://docs.oracle.com/cd/E24329_01/index.htm`

Configuring JDBC with Database Credentials

You need to configure the JDBC data and Oracle RAC Multi-Data sources by referencing the database users you created in "Creating and Authorizing Database Users" section. For details see the discussion on configuring domain settings in *Oracle Communications Services Gatekeeper Installation Guide*.

Securing Oracle Access Manager MBeans

By default any administrative user can access and change the OAM MBean settings using the Oracle Fusion Middleware Oracle WebLogic Server Administration Console. If your implementation requires a more restrictive control, see the discussions on securing web services and OAM MBeans in *Oracle Communications Services Gatekeeper System Administrator's Guide*.

Securing Web Services

Web services security determines the level of protection that Services Gatekeeper requires for the web messages it sends and receives. The default level of security requires authentication tokens (username and password) for all messages. The choices are:

- Username/Password Authentication (Username Token)
- XML Digital Signatures (X.509 Certificate Token)
- Encryption (SSL or TLS SAML Tokens)

You set authentication level by web service using the Services Gatekeeper Administration Console, and if more security is required, using WebLogic tools.

For details see the discussions on securing web services and Oracle Access Manager MBeans in *Oracle Communications Services Gatekeeper System Administrator's Guide*. Some of those procedures require database administration privileges. For details, see the discussion on configuring administrator user names and passwords in *Oracle Communications Services Gatekeeper Installation Guide*.

For instructions on setting up TLS/SSL see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Securing Oracle Service Bus and the Service Oriented Architecture Facades

For information about installing Oracle Service Bus (OSB), see *Oracle Fusion Middleware Installation Guide for Oracle Service Bus 11g Release 1 (11.1.1.3)* at:
http://download.oracle.com/docs/cd/E14571_01/doc.1111/e15017/toc.htm

For information on securing Services Gatekeeper Service Oriented Architecture (SOA) see the discussion on managing and configuring SOA facades in *Oracle Communications Services Gatekeeper System Administrator's Guide*.

Securing Geographically Redundant Deployments

Separating Services Gatekeeper geographically protects you against data loss and service failure in the event of a natural disaster or other catastrophic event.

For details on geographically redundant deployments, see *Oracle Communications Services Gatekeeper Deployment Guide*.

(Optional) Adding Custom Password Validators

A password validator is not required to run Services Gatekeeper, but it ensures that your partners and their subscribers adhere to a consistent level of password security. See the discussion on post installation in *Oracle Communications Services Gatekeeper Installation Guide* for details on adding custom password valdiators.

(Optional) Install Java Cryptography Extension (JCE)

Java Cryptography Extension (JCE) is not required for Services Gatekeeper to run, but it does relieve web servers from the burden imposed by secure socket layer (SSL) security. See the discussion on post installation in *Oracle Communications Services Gatekeeper Installation Guide* for details on adding JCE.

3

Administering Services Gatekeeper Security

This section explains the tasks required to manage a secure running Oracle Communications Services Gatekeeper (Services Gatekeeper) implementation.

Administering Services Gatekeeper Security

Administering Services Gatekeeper securely includes the following tasks that are covered in the following sections:

- Maintaining Security Standards
- Securing Partner Relationship Manager
- Monitoring Your Services Gatekeeper Implementation
- Backing Up and Restoring Services Gatekeeper Data

Maintaining Security Standards

Your security-related day-to-day administrative tasks include maintaining security standards. For example:

- Only grant access to administrative users as they require it.
- Maintain your firewalls with an appropriate level of security.
- Monitor your Services Gatekeeper servers for unauthorized access attempts. See "Monitoring Your Services Gatekeeper Implementation" for details.

Securing Partner Relationship Manager

Secure the Services Gatekeeper Partner Relationship Manager (PRM) by securing the administrative users who administer it.

For details, see the discussion on security in *Oracle Communications Services Gatekeeper Partner Relationship Management Guide*.

Monitoring Your Services Gatekeeper Implementation

Services Gatekeeper includes tools to monitor the number of transactions your Services Gatekeeper is processing. These statistics are intended for calculating usage and grouping reports, but can also be valuable tools to alert you to denial of service attacks. See the discussion on managing and configuring statistics and transaction licenses in *Oracle Communications Services Gatekeeper System Administrator's Guide.*

Services Gatekeeper provides a mechanism that alerts you to impending system overload using the WebLogic Overload Alarms feature. For details, see the discussion on overload alarms in *Oracle Communications Services Gatekeeper System Backup and Restore Guide*.

Backing Up and Restoring Services Gatekeeper Data

Even in clustered, redundant systems, regular backups are an essential part of a secure Services Gatekeeper implementation. See these topics in *Oracle Communications Services Gatekeeper System Backup and Restore Guide* for details on the tasks that provide help and advice on backing up and recovering Services Gatekeeper data:

- Redundancy and failover for clustered services
- Automatic restart for managed servers
- Managed server independence mode
- Automatic migration of failed managed servers
- Backing up the domain configuration.
- Restarting a failed administration server
- Restarting failed access and network tier servers
- Moving an access or network tier server to a different system.

4

Securing Partner Accounts and Services

This chapter explains security considerations for administering your partners and also developers who add services to Oracle Communications Services Gatekeeper (Services Gatekeeper).

Administering Partners

Your partners add their services to Services Gatekeeper using the Partner Manager Portal. When your partners create these accounts they also create passwords and security questions. The Partner Manager Portal then uses the passwords and questions to authenticate your partners when they log in.

However, you still need to assign security personnel to monitor the accounts being created to ensure that they are legitimate. Partners are assigned one of the service provider interfaces created for them. These interfaces are administrative user types and must be managed like other administrative users and only granted the access privileges they require. You must grant service providers the necessary privileges to do their jobs, but no more.

See "Setting Up the Partner Portal and Partner Manager Portal" for information on creating these accounts.

See the discussion on service provider login for information on creating service provider accounts, and the discussion on the service provider interfaces for information on granting and removing privileges, both in *Oracle Communications Services Gatekeeper Partner Relationship Management Guide*.

Setting Up the Partner Portal and Partner Manager Portal

Your partners (service providers) use the Partner Portal to administer their partner accounts, including granting and revoking service access. The service providers may be internal or external to your organization. Set up the Partner Portal and Partner Manager Portal with the security appropriate for your implementation.

- Educate partners to:
  - Enable security for communication services.
  - Use the secure interfaces supplied with Services Gatekeeper to communicate with Services Gatekeeper.
  - Use Oracle OAuth to manage access to secured resources (such as pictures or secured URLs).
  - Record their Partner Portal credentials somewhere safe.

  - Change their automatically-generated application IDs as soon as possible because they are predictable.

For details see these documents:

- *Oracle Communications Services Gatekeeper Partner Relationship Management Guide*
- Services Gatekeeper Partner Portal online help

Securing Communication Services

The communication services that your partners provide generally require both authentication and authorization services to remain secure. You have several ways of providing this security:

- The Services Gatekeeper security provider authenticates subscribers by verifying their application's ids and passwords.
- The Services Gatekeeper service-level agreements (SLAs) provide authorization. You secure communication services by authorizing service requests with SLAs, and authenticating the users making the requests with web services security. This is true for services created by you or your partners. SLA can define which API and what TPS the application can use. The following sections discuss these tasks:
  - Authorizing Access to Services with SLAs
  - Authenticating Service User Requests
- Using OAuth to provide both authorization and SSO authentication for third-party resources.

  See "Authenticating and Authorizing Resources with OAuth" for details.

Authenticating and Authorizing Resources with OAuth

See the *Oracle Communications Services Gatekeeper OAuth Guide* and the discussion on Services Gatekeeper OAuth 2.0 authorization resource servers in *Oracle Communications Services Gatekeeper System Administrator's Guide* and for details on using the OAuth precool to grant access to resources (such as photos, video, and so on) without compromising the resource owner's security. OAuth can provide both authorization and authentication services, replacing more traditional SSO mechanisms.

Authorizing Access to Services with SLAs

Your partners create Service Level Agreements (SLAs) to define who is authorized to use their services. Every communication service must have an SLA that specifies access privileges to Services Gatekeeper and the network nodes it communicates with.

For details, see *Oracle Communications Services Gatekeeper Accounts and SLAs Guide*.

Authenticating Service User Requests

Communication services do not have security enabled by default because Services Gatekeeper has no way of knowing what kind of security they allow. You must make sure to add or take advantage of their security measures before allowing subscribers to use them. This section lists the security strategies supported by the communication services and explains where to find details.

Services Gatekeeper supports these types of communication services:

- SOAP-based
- RESTful
- Native

Information about securing these communication services is explained in the sections that follow. See the references provided and the discussions on securing web services and Services Gatekeeper MBeans in *Oracle Communications Services Gatekeeper System Administrator's Guide*, and the discussion on web services security in *Oracle Communications Services Gatekeeper Accounts and SLAs Guide* for details.

Securing SOAP-Based Communication Services

The first step in protecting your SOAP communication services is to ensure that all communication with Services Gatekeeper happen within a session. You set this in the Services Gatekeeper Session Manager Web Service, and it automatically requires applications to provide authorization.

Applications communicating with Services Gatekeeper using a SOAP interface have these options for authentication:

- Username/Password Authentication (Username Token)
- Digital Signatures (X.509 Certificate Token).
- Encryption (SAML Token)
- Session IDs

For details on creating and securing a SOAP-based communication service see the discussion on:

- Interacting with Oracle Communications Services Gatekeeper
- Session management
- Session Manager Web Service

in *Oracle Communications Services Gatekeeper Application Developer's Guide*.

Securing RESTful Communication Services

The RESTful service interfaces uses HTTP basic authentication and session IDs for security. For details on implementing HTTP security see the discussion on securing web services and Oracle Access Manager MBeans in *Oracle Communications Services Gatekeeper Administrator's Guide*.

For details on creating and securing REST communication services see the discussion on interacting with the REST facade in *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*.

For details on requiring sessions for all RESTful communication, see the discussions on session management and the Session Manager Web Service in *Oracle Communications Services Gatekeeper Application Developer's Guide*.

Securing Native Communication Services

Services Gatekeeper supports communication services using the MM7, SMPP, and UCP protocols. The following sections outline their security considerations and provide links to implementation details.

Securing Native MM7 Communication Services Services Gatekeeper uses HTTP basic authentication to secure native MM7 communication services. For details see the

discussion on managing native MM7 in *Oracle Communications Services Gatekeeper Communication Service Guide*.

Securing Native SMPP Communication Services Services Gatekeeper uses authentication credentials to secure native SMPP communication services. For details on creating a native SMPP communications service, see the discussion on native SMPP in *Oracle Communications Services Gatekeeper Communication Service Guide*.

Securing Native UCP Communication Services Services Gatekeeper uses a credential store to secure native UCP communication services. For details on configuring connection information and the credential map, see the discussion on managing and configuring connection information in *Oracle Communications Services Gatekeeper System Administrator's Guide*.

Securing Communication with Service Interceptors

Configuring tunneling for a communication service serves as a "white list" of parameters that you can create. It limits communication service messages to only the parameters that you specify (nothing is limited by default). This strategy is quite restrictive and impractical for most communication, but may fit into your security needs. For details on implementing tunneling, see the discussion on service interceptors in *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*.