Oracle® Communications IP Service Activator

Security Guide

Release 7.2

E35657-01

October 2013

Oracle Communications IP Service Activator Security Guide, Release 7.2

E35657-01

Contents

Preface

This guide provides guidelines and recommendations for setting up Oracle Communications IP Service Activator in a secure configuration.

Following the steps in this guide allows you to enable a variety of security features. The guide also describes how to make sure that new components and cartridges are developed securely.

Audience

This guide is intended for the customer or system integrator that has IP Service Activator as part of a solution deployment. It assumes that the reader has detailed knowledge of IP Service Activator and has taken the necessary training.

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.

1

IP Service Activator Security Overview

This chapter provides an overview of Oracle Communications IP Service Activator security.

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.
- **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:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`
- **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 IP Service Activator Installation" for more information.
- **Learn about and use the IP Service Activator security features.** See "Implementing IP Service Activator 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 "Security Considerations for Developers" for more information.

Understanding the IP Service Activator Environment

When planning an IP Service Activator implementation, consider the following:

- **Which resources need to be protected?**

  For example:

  - You must protect internal data.
  - You must protect system components from being disabled by external attacks or intentional system overloads.

  - You must protect the archived device configurations.
  - You must protect the IP Service Activator object information model (the database).

- **Who are you protecting data from?**

  For example, you must protect customer data from other customers, but someone in your organization might need to access that data in order to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.

- **What will happen if protections on a strategic resource 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 helps you protect it properly.

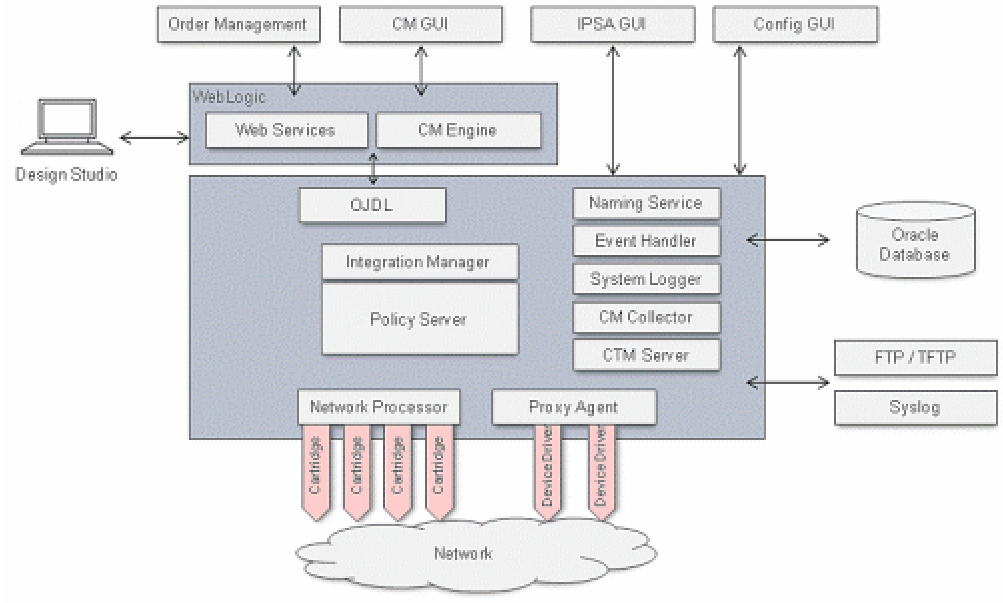
Overview of IP Service Activator Security

IP Service Activator security is designed to protect IP Service Activator users, IP Service Activator modules, the router configuration data, the database, the application logs, and the IP Service Activator Web service.

- **IP Service Activator application security:** Users of the application are authenticated using the Oracle IP Service Activator object model, based on the roles and groups defined in it. This applies both to the IP Service Activator user interface (client) and the command line interface.
- **IP Service Activator module security:** Module security follows the same methods for validation and authentication as the client.
- **Router configuration data security:** The router configurations are stored in the Oracle Database, which requires database credentials or can be accessed by using Configuration Management. Configuration Management is stored securely by IP Service Activator application security.
- **Database security:** Different interfaces are stored differently. The client and command line interface use credentials encrypted in a file. The IP Service Activator Web service and the Configuration Management module credentials are stored securely inside the Java Database Connectivity (JDBC) data source in the Oracle WebLogic server.
- **Application log security:** The application, settings and properties, and logs are protected by the user authorization and authentication procedures of the host system (UNIX or Oracle Linux). Only the installed user has access to the files, based on file permissions.
- **IP Service Activator Web service security:** The Web service is secured by an Oracle WebLogic security policy, along with a WebLogic user and group created using the IP Service Activator Configuration GUI.

IP Service Activator comprises the various components shown in Figure 1–1, including the components to which it connects. Each installed or integrated component requires special steps and configurations to ensure system security.

Figure 1–1 IP Service Activator Components

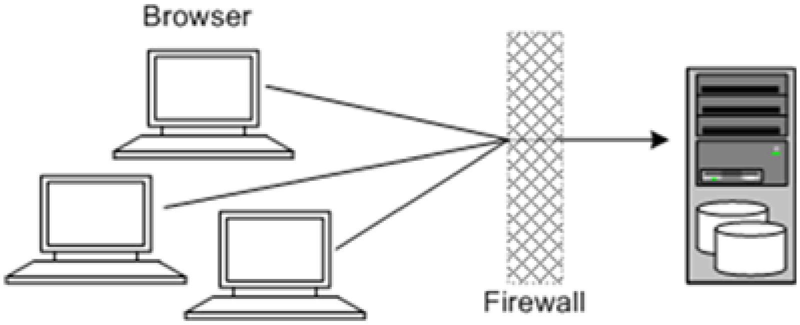


Recommended Deployment Topologies

This section describes recommended deployment topologies for IP Service Activator.

Figure 1–2 shows a single-computer deployment topology: the simplest IP Service Activator deployment architecture.

Figure 1–2 Single-Computer Deployment Topology



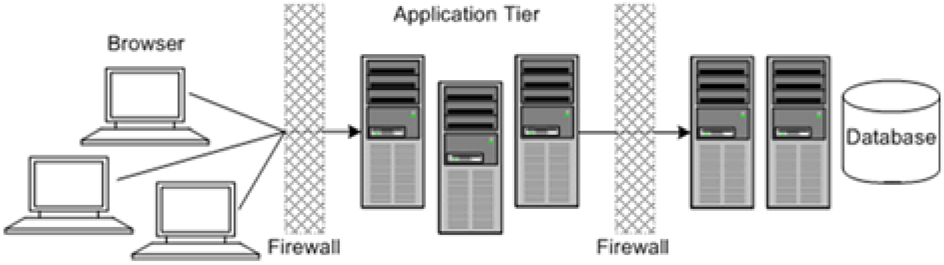
In this topology, all the application components and data are kept on a single system, protected from external attacks by a firewall. The firewall can be configured to block known illegal traffic types. There are fewer resources to secure because all the components are on a single system and all the communication is local. Fewer ports have to be opened through the firewall. Conversely, there are fewer points of attack, and, if security is compromised, an attacker would have access to the entire system and data.

Oracle recommends that you run the whole system inside the customer's intranet and not expose components or computers to the public Internet.

A single-computer installation topology is best suited for test and lab environments or a small network. See *IP Service Activator Installation Guide* for information about the system setup depending on your network size.

Figure 1–3 shows a tiered deployment topology: a scalable IP Service Activator deployment offering greater security.

Figure 1–3 Tiered Deployment Topology



In this topology, firewalls isolate the application tier from the intranet. Oracle recommends that you run the whole system inside your intranet and not expose components or computers to the public Internet. Two layers of firewall protect the database and servers from potential attacks. Both firewalls can be configured to block known illegal traffic types. The two layers of firewall provide intrusion containment. Although there are a greater number of components to secure, and more ports have to be opened to allow secure communication between the tiers, the attack surface is spread out.

The application tier has components like the Policy Server and Web Server. The other tier has components like the Network Processor, database, and routers.

Operating System Security

This section lists IP Service Activator-specific operating system security configurations.

For more information, see the following documents:

- Guide to the Secure Configuration of Red Hat Enterprise Linux 5
- Hardening Tips for the Red Hat Enterprise Linux 5

IP Service Activator Application Ports

IP Service Activator uses the default ports shown in Table 1–1. If you are not using the defaults, ensure that the correct values are entered by using the IP Service Activator Configuration GUI.

Table 1–1 IP Service Activator Default Ports

Port	Value
HTTP	80
CORBA	2809, 2810
FTP (Configuration Management)	20, 21 - (not configurable)
TFTP (Configuration Management)	69 - (not configurable)
Syslog (Configuration Management)	514 (UDP) -(not configurable)
WebLogic Port(s) - Admin Server Port, and the Managed Server Port(s)	7001, 7003 (defined at domain creation)
Oracle Database port	1521

Table 1–1 (Cont.) IP Service Activator Default Ports

Port	Value
SSH	22 (not configurable)
Configuration GUI ORB Server Ports (ports configured in the Configuration GUI)	2810-2828
Telnet	23 (not configurable)
Logreader Socket Port	4446
TACACS (device communication)	49 (not configurable)

If IP Service Activator computers do not use the secure tunnels (see "Secure Integration of IP Service Activator") to communicate between computers, Oracle recommends that you lock the client to a particular port, unless the firewall allows any port to establish a reverse connection from the Policy Server to the client.

If you are using the Network Processor audit and the client is on the other side of the firewall, the port that needs to be forwarded is port 2814 (the default value from the Configuration GUI). For more information, see the knowledge article available on the Oracle Support Web site: `https://support.oracle.com` [ID 1335658.1].

If you are using Configuration Management, the WebLogic port needs to be open between:

- The computer with IP Service Activator Engine (WebLogic Server) and the browser client.
- The computer with IP Service Activator Engine and the computer with the Configuration Management Collector installed.

Oracle recommends that the port on which the WebLogic Administration console runs not be open to the public Internet and be restricted to inside the firewall so that only administration operations can be contained within the customer's network.

Secure Integration of IP Service Activator

This section describes how to secure the configuration between the IP Service Activator computers if the deployment is a multi-computer installation.

Oracle recommends that, if your installation is on multiple computers, the communication between the computers be secured by enabling an encrypted SSH tunnel. This tunnel has all IP Service Activator traffic on it. Configuring this tunnel is well documented in Windows, Linux, and UNIX documentation. At a minimum, the client and the server components will be on different computers, so a tunnel should be set up between the client computer and the Policy Server.

For example, on the Windows computer where the client is installed, the user must redirect all IP Service Activator traffic on the Windows client through the tunnel. To do this, you need administrator rights.

To forward IP Service Activator traffic:

1. Pin down all the floating IP Service Activator ports using the **BOAiiop_name_port** command line option. Take note of all the fixed IP Service Activator ports (for example, naming service).
2. Configure the tunnel to do port forwarding from each of the pinned down or fixed ports into the tunnel (bi-directionally).

To set up the client, modify the IP Service Activator User Interface shortcut found in the **Start** menu. Go to the properties of the shortcut, and modify the target command line to include the following text at the end of the line:

```
BOAiiop_name_port 127.0.0.1:1970
```

This forwards the client to run on port 1970.

Three other ports must be configured so that the client can communicate with the Policy Server. Do the following:

- Configure the SSH port forwarding tunnel from the client to the IP Service Activator naming service. The default is to use **127.0.0.1:2809** as the **Destination**.
- Configure the SSH port forwarding tunnel from the client to the IP Service Activator policy server. The default is to use **127.0.0.1:2810** as the **Destination**.
- Configure the remote SSH port forwarding tunnel from the Policy Server to IP Service Activator. The default is to use **127.0.0.1:1970** as the **Destination**.

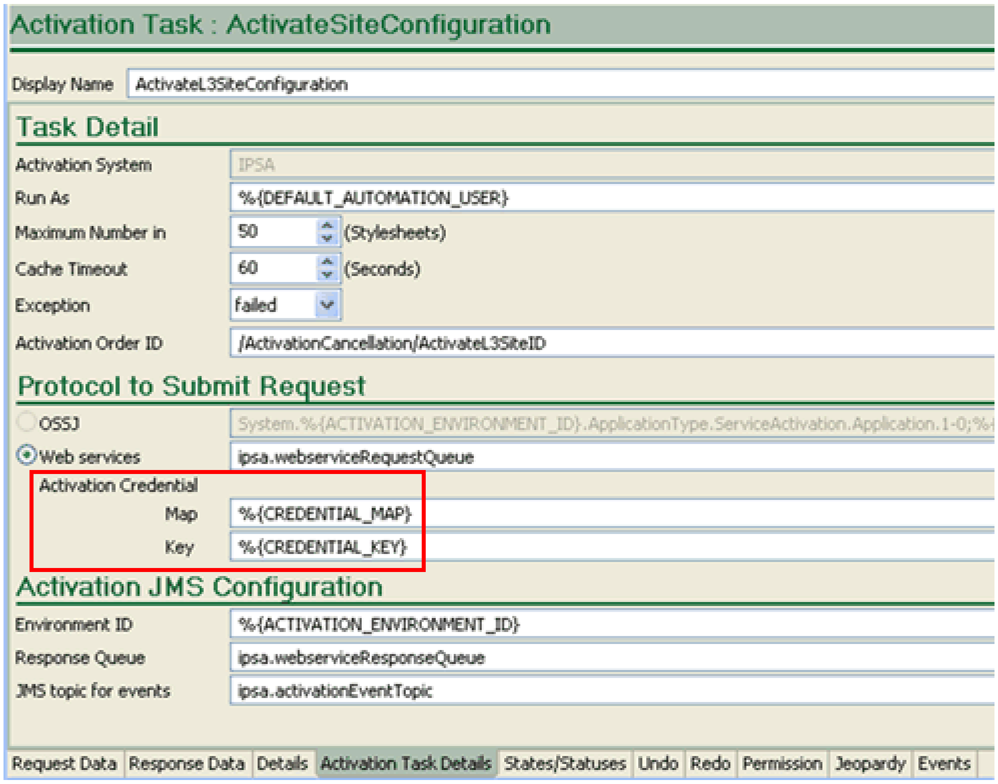
If you are using Citrix as a terminal server, using the client locked to a BOaiiop_port might be a problem because all client instances are connecting from the same IP.

Secure Integration of IP Service Activator with OSM

If you are integrating IP Service Activator and Oracle Communications Order and Service Management (OSM), you must secure the configuration between them. For information about OSM and IP Service Activator integration, see *IP Service Activator Concepts*.

OSM secures Oracle Communications ASAP and IP Service Activator Web service interactions using a Web services user name and password located in the WebLogic server of the activation system (either ASAP or IP Service Activator). Communication is through Java Message Service (for Activation) and HTTP (for view framework). You must store this user name and password within the Fusion Middleware Credential Store Framework (CSF) using the **credStoreAdmin.bat** script located in the *OSM_Home***/SDK/XMLImportExport** folder (where *OSM_Home* is). The **credStoreAdmin.bat** script creates a map and a key that correspond to the activation system Web Service user name and password. For more information about this script, see the *OSM System Administrator's Guide*.

Figure 1–4 Design Studio Activation Task Tab



Activation Task : ActivateSiteConfiguration

Display Name: ActivateL3SiteConfiguration

Task Detail

Activation System: IPSA

Run As: %{DEFAULT_AUTOMATION_USER}

Maximum Number in: 50 (Stylesheets)

Cache Timeout: 60 (Seconds)

Exception: failed

Activation Order ID: /ActivationCancellation/ActivateL3SiteID

Protocol to Submit Request

○ OSSJ: System.%{ACTIVATION_ENVIRONMENT_ID}.ApplicationType.ServiceActivation.Application.1-0;%

● Web services: ipsa.webserviceRequestQueue

Activation Credential

Map: %{CREDENTIAL_MAP}

Key: %{CREDENTIAL_KEY}

Activation JMS Configuration

Environment ID: %{ACTIVATION_ENVIRONMENT_ID}

Response Queue: ipsa.webserviceResponseQueue

JMS topic for events: ipsa.activationEventTopic

In Oracle Communications Design Studio, when you configure an activation task for the IP Service Activator activation system (on the **Activation Task Details** tab), you can choose which protocol to use to submit the request.

For enhanced security, Oracle recommends using Web services because you must also then specify a map name and a key name (shown in Figure 1–4). During installation and configuration, the OSM SDK **credStoreAdmin.bat** script runs and creates a credential store in WebLogic. The map name and key name are used to access IP Service Activator Web Services credentials at run time. At run time, WebLogic also requires user authorization of the OSM user, which allows the OSM user to use the map name and key name to securely extract the IP Service Activator Web service credentials.

Oracle Security Documentation

IP Service Activator uses other Oracle products, such as Oracle Database and Oracle WebLogic Server. See the following documents, as they apply to IP Service Activator:

- *Oracle Database Security Guide*.
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

2

Performing a Secure IP Service Activator Installation

This chapter presents planning information for the Oracle Communications IP Service Activator secure installation.

For information about installing and configuring IP Service Activator, see *IP Service Activator Installation Guide* and *IP Service Activator System Administrator's Guide*.

For more information about installing Oracle Communications Configuration Management, see *Configuration Management Installation and System Administration Guide*.

Pre-Installation Configuration

You must have at least one dedicated UNIX group and one dedicated user account within that group for IP Service Activator. You must run the Installer as a non-root user. Oracle recommends that the **umask** for this user be set to **077**. An Oracle Database user must be created with no permissions granted to the public user. See *IP Service Activator Installation Guide* for the set of permissions.

> **Note:** If you are using the Configuration Template Module, set the additional permissions listed in *IP Service Activator Installation Guide*.

If you are using the IP Service Activator Web service or Configuration Management, you must create a WebLogic domain. Oracle recommends that you always run in production mode with Oracle WebLogic server. If you are running multiple applications, Oracle recommends that you deploy each application to its own managed server.

When the IP Service Activator Web service is deployed in a managed server that is separate from Oracle Communications Order and Service Management (OSM), a Java Messaging Service message-forwarding mechanism is required to enable JMS message delivery between applications. The Store and Forward (SAF) and IP Service Activator Web Service JMS modules are made secure by using a security policy. For more information, see *Solution Uptake Guide for MPLS VPN with Ethernet Access*.

Installing IP Service Activator Securely

You can install IP Service Activator using a custom installation or a typical installation. Oracle recommends that you do a custom installation to avoid installing components and options that you do not need. To limit your exposure in a production environment, Oracle recommends that you do not install unused options, components, or sample files.

Secure File System Access

Access to files that are created during installation is limited to the owner. IP Service Activator does not allow installation, and issues a warning, if the installation is attempted by a user that has root access.

File Permissions

The following are the default permissions set for the installed files:

- rw-,r--,--- 640 (for all library files)
- rwx,r-x,--- 750 (for all executable files)
- dwx,rwx,--- 770 (for all directories files)

Default permissions are set to the lowest possible level. Oracle recommends keeping the permissions as restrictive as possible, as per your business needs.

Oracle recommends that the WebLogic Server installation user and the IP Service Activator application installation user share the same group and the same user ID.

IP Service Activator uses the **umask** of **039** for auto-generated files (for example, log files), which is explicitly set in all scripts.

Protect the WebLogic configuration (JMS, JDBC, and so on) file, **config.xml**, with the proper permissions. This file is located in the configuration directory of the domain.

The WebLogic Datasource passwords are encrypted using the Oracle-recommended 3AES algorithm and are stored in the WebLogic server configuration files.

Strong Passwords

Oracle recommends having strong password policies for IP Service Activator users and WebLogic Server and Oracle Database schema users. Oracle recommends the following:

- A password length between 6 and 24 characters
- A password containing at least one alpha, numeric, and special character. For example: WebLogic@123.
- That the user name not be part of the password
- Additional IP Service Activator policies that must be configured using the client:
  - The IP Service Activator user's password should expire every 28 days.
  - The IP Service Activator user's password cannot be the same as any of the previous six passwords.
  - The IP Service Activator user's account is disabled after six login failures.

Oracle WebLogic Server Configurations

After you create the WebLogic Server domain for IP Service Activator, start the Admin Server by running the following command:

```
startManagedServer.sh ManagedServer_1 t3s://Hostname:Port
```

where *ManagedServer_1* is the name of the first managed server, and *Hostname* is the hostname of the admin server. For more information about configuring WebLogic, see the WebLogic documentation.

Configuring WebLogic Session Timeout

It is a security risk to leave the WebLogic server session running for long periods of time.

The default session timeout in Configuration Management is 60 minutes. The WebLogic Server administrator can change this value.

To change the WebLogic default session timeout:

1. Log in to WebLogic Administration Console.
2. In the Domain Structure section, click **Deployments**.
3. Click the application **Configuration Management** deployed as Enterprise Application.

   The Configuration Management deployment settings appear.
4. Click the **Configuration** tab.
5. Set **Session Timeout (in seconds)** to the new timeout value.
6. Click **Save**.

   If you have not already created a deployment plan, WebLogic creates one with the above changes and prompts you to save the deployment plan. Enter a name and path for the deployment plan and click **OK**.
7. In the Domain Structure section, click **Deployments**.
8. Click the application **Configuration Management** deployed as Enterprise Application.
9. Click **Update**.
10. Select **Update this Application in Place with New Deployment Plan Changes**.
11. Set **Deployment Plan** to the deployment plan created in step 6.
12. Browse to the file by clicking **Change Path**.
13. Click **Next**
14. Click **Finish**.
15. Restart the WebLogic server.

For more information, see "Configuring Applications for Production Deployment" on the Oracle Technology Network Web site.

Configuring Configuration Management Session Timeout

It is a security risk to leave the Configuration Management session running for long periods of time.

The default session timeout in Configuration Management to maintain a connection to IP Service Activator is 30 minutes. You can change this value.

To change the Configuration Management session timeout value:

1. Log in to the Configuration Management client.

2. Click the **Configuration Management Server** Tab.
3. Set **User Interface Session Timeout (mins)** to the new timeout value.
4. Click **Commit**.

Post-Installation Tasks

IP Service Activator communicates over CORBA. To control access for CORBA connections, see "CORBA ORB Configuration for IP Service Activator" in *IP Service Activator Installation Guide*.

IP Service Activator comes with a predefined user account: **admin**. Oracle recommends that, immediately after you install IP Service Activator, you start the client and change the default password for the admin user. Oracle recommends that you create a new **SuperUser** and delete the **admin** user.

3

Implementing IP Service Activator Security

This chapter explains the security features of Oracle Communications IP Service Activator.

Configuring and Using Access Control

This section explains the authorization system used to control access to data, resources, and processes. Authorization is used to control access by:

- Permitting only certain users access or actions
- Applying varying limitations on user access or actions

IP Service Activator uses groups and roles to control access to network topology objects. To change these settings, start the IP Service Activator client and follow the steps in "About Users and Security" in *IP Service Activator System Administrator's Guide*. The IP Service Activator user password policies are also defined in the IP Service Activator client. For more information, see "Passwords" in *IP Service Activator System Administrator's Guide*.

Configuration Management Access Levels

A Configuration Management user with Read/Write access can be restricted to do any or all of the following:

- Restore an archive
- Activate a configlet
- Unlock an archive

By default, the user with this access level is allowed to:

- Change permissions
- Start the Configuration GUI and click the **Configuration Management Server** tab
- Select the operations that you want to restrict, or unselect the operations that you want to allow, and click **Commit** to implement the changes

Users with SuperUser permissions can do all of the above, and users with Read permissions can only view; Read permissions operate like read-only mode.

IP Service Activator User Accounts

Oracle recommends that you use a separate router user account to log in and provision the devices. This is the user account that is defined and used under the IP Service

Activator Device Security panel. If there is a security threat, this user can be locked out by the Administrator.

Configuration Management Security

Oracle recommends that you create a custom IP Service Activator user for the Configuration Management server so that you can monitor and audit Configuration Management activities. You must also ensure that each user has a separate account/user to log in to Configuration Management so that you can monitor and audit operations described in "Configuring and Using Security Audit".

If you are using the restore functionality, Oracle recommends that you clean the router configuration out of the directory after the restore. If the router configuration is left in the directory, it could be downloaded by other users.

Configuring and Using Security Audit

Each application (IP Service Activator, Oracle Database, and WebLogic) has separate logs and audit logs that you can use to monitor activities. You can view WebLogic audit logs and IP Service Activator Web service logs using the Enterprise Manager (if enabled) or in a text editor.

The IP Service Activator application audit and systems logs are stored in the application installed directory. You can open these files in a text editor.

For information about the WebLogic logs, see the WebLogic Server documentation.

For information about the Oracle logs, see the Oracle Database documentation.

IP Service Activator Logs

IP Service Activator creates logs of all the commands and configuration sent to the routers. The logs are located in the IP Service Activator installation directory called Audit Trails, and you can view the logs in a text editor. For example:

/opt/OracleCommunications/ServiceActivator/AuditTrails

IP Service Activator stores and records all transactions, their operations, and their statuses, which you can view using the client. For more information about logs, see *IP Service Activator System Administrator's Guide*.

You can open these logs in a text editor.

The following examples show sample IP Service Activator Device configuration logs.

```
2012-05-17 21:10:55|10.156.68.43|#Applying Configuration
2012-05-17 21:10:56|10.156.68.43|terminal length 0
2012-05-17 21:10:56|10.156.68.43|conf t
2012-05-17 21:10:56|10.156.68.43|interface Tunnel899
2012-05-17 21:10:56|10.156.68.43|description test
2012-05-17 21:10:57|10.156.68.43|alias exec IpsaConfigVersion
2012-05-17T21:10:55.653Z
2012-05-17 21:10:57|10.156.68.43|end
2012-05-17 21:10:57|10.156.68.43|copy running-config startup-config
2012-05-17 21:10:57|10.156.68.43|startup-config
2012-05-17 21:10:59|10.156.68.43|logout
2012-05-17 21:11:00|10.156.68.43|#End Configuration
```

Configuration Management Audit Logs

Configuration Management has audit logs that show the user and the operation performed. The logs are located in the WebLogic domain logs. For example:

```
/opt/Oracle/Middleware/user_projects/domains/DomainName/cmuser.audit.log
```

You can open these logs in a text editor.

Table 3–1 shows sample Configuration Management audit logs.

Table 3–1 Sample Audit Logs

Operation	Sample Audit Log Text
Logging in to Configuration Management	2012-05-17 11:55:55 The user admin has successfully logged in.
Logging out of Configuration Management	2012-05-17 11:57:56 The user admin has logged out.
Unsuccessful login to Configuration Management	2012-05-17 11:57:56 The user admin was not successful logging in.
A schedule is being created in Configuration Management	2012-05-17 17:07:59 Schedule Order operation invoked by user admin.
An archive is being created in Configuration Management	2012-05-17 17:08:33 Archive Order operation invoked by user admin.
An archive is being deleted from Configuration Management	2012-05-17 17:09:33 Delete Archive operation invoked by user admin.
A configlet is being activated in Configuration Management	2012-05-17 17:10:16 Configlet Order operation invoked by user admin.
A configlet is being deleted from Configuration Management	2012-05-17 17:10:18 Delete Configlet operation invoked by user admin.
A restore is being sent to Configuration Management	2012-05-17 17:10:26 Restore Order operation invoked by user admin.
A change tracking policy is being sent to Configuration Management	2012-05-17 17:10:36 Change Tracking Order operation invoked by user admin.

Security Considerations for Developers

To create new components for IP Service Activator without compromising security, when you are passing credentials, do not under any circumstance log the credentials or store them in clear text. If the component or program resides on a different computer than the integration manager, Oracle recommends setting up an SSH tunnel to ensure that the traffic is encrypted.

A

Secure Deployment Checklist

The following security checklist lists guidelines to help you secure Oracle Communications IP Service Activator and its components.

Secure Deployment Checklist

- Install only the components you require.
- Lock and expire default user accounts.
- Enforce strong password management.
- Restrict and control user privileges.
- 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 who accesses your systems.
  - Encrypt network traffic.
  - Harden the operating system by installing it in a secure location where it is difficult for a hacker to access.
- Apply all security patches and workarounds.
- Encrypt sensitive information.
- Contact Oracle Security Products if you discover a vulnerability in any Oracle product.