

Oracle® Communications IP Service Activator Installation Guide



Release 7.5
F59538-01
September 2022

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2011, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

| | |
|-----------------------------|------|
| Audience | viii |
| Documentation Accessibility | viii |
| Diversity and Inclusion | viii |

1 IP Service Activator Installation Overview

| | |
|---|-----|
| IP Service Activator Installation Overview | 1-1 |
| Installation Sequence | 1-1 |
| Pre-installation Checklist | 1-2 |
| Downloading the IP Service Activator Software | 1-2 |

2 Planning an IP Service Activator Installation

| | |
|--|-----|
| About Planning an IP Service Activator Installation | 2-1 |
| Overview of IP Service Activator Architecture | 2-1 |
| IP Service Activator Components and Modules | 2-1 |
| Optional Integration Components | 2-3 |
| Optional Service Modules | 2-3 |
| Additional Software Requirements | 2-4 |
| Oracle Real Application Clusters in IP Service Activator | 2-4 |
| Planning Guidelines and Engineering Considerations | 2-4 |
| System Configuration Overview | 2-4 |
| Assistance in the Sizing Process | 2-4 |
| Customer Responsibilities | 2-4 |
| IP Service Activator Component Architecture | 2-5 |

3 IP Service Activator System Requirements

| | |
|--|-----|
| Support for Linux | 3-1 |
| Support for Windows | 3-1 |
| Solaris Installation and Configuration | 3-1 |
| Check the Solaris OS Version | 3-1 |

| | |
|---|-----|
| Check the Solaris Patches | 3-2 |
| Supported Devices and Operating Systems | 3-2 |
| Cisco IOS XR Cartridge | 3-2 |
| Cisco IOS Cartridge | 3-2 |
| Cisco CatOS Cartridge | 3-3 |
| Huawei Cartridge | 3-3 |
| Juniper JUNOS Cartridge | 3-3 |
| Pre-installation Tasks for Solaris and Linux | 3-4 |
| Enabling Per-process Core Dumps for Solaris | 3-4 |
| Enabling Per-process Core Dumps for Linux | 3-4 |
| Setting File Resources for Device Discovery | 3-5 |
| Synchronizing IP Service Activator Host Machines | 3-6 |
| IP Service Activator Administrator UNIX User ID (ipsaadm) | 3-6 |
| Setting Permissions for the Installation UNIX User ID | 3-6 |
| Java Development Environment | 3-7 |
| Hardware Requirements | 3-7 |

4 Installing and Configuring Oracle Database Software

| | |
|--|-----|
| Preparation | 4-1 |
| Installing Oracle Database Using Oracle Universal Installer | 4-2 |
| Oracle Database Post-Installation Tasks | 4-2 |
| Updating the Net Service Name Setting | 4-2 |
| Setting Up the IP Service Activator Environment in Oracle Database | 4-2 |

5 Installing and Configuring WebLogic Server

| | |
|--|-----|
| Installing WebLogic Server Software | 5-1 |
| Creating the WebLogic Server Domain | 5-1 |
| Configuring the WebLogic Server Domain | 5-1 |
| Increasing the Memory Settings for WebLogic Servers | 5-2 |
| Preventing Connection Timeout when Using a Remote Database | 5-2 |

6 Installing and Configuring Supplemental Software Components

| | |
|--|-----|
| Installing Supplemental Software Components | 6-1 |
| Preparing the Supplemental Software Component Packages | 6-1 |
| CORBA ORB Configuration for IP Service Activator | 6-2 |

7 Installing IP Service Activator

| | |
|--|-----|
| Installing IP Service Activator on an Oracle Solaris or Linux Server | 7-1 |
|--|-----|

| | |
|---|------|
| Preparing to Install IP Service Activator | 7-1 |
| Running the Oracle Universal Installer for IP Service Activator | 7-2 |
| About Silent Installations | 7-5 |
| Running a Silent Installation | 7-6 |
| Installing the IP Service Activator Client on Windows | 7-7 |
| Before Running IP Service Activator Client Installer | 7-7 |
| Configuring the 64-bit Windows Host to Prefer IPv4 Over IPv6 Addresses | 7-8 |
| Installing the Client | 7-8 |
| Running IP Service Activator Client Installer in Silent Mode | 7-10 |
| Oracle Database Connection Considerations for the IP Service Activator Client | 7-11 |
| Oracle Database Client Requirements to View Logs in the IP Service Activator Client | 7-12 |
| Setting Up an FTP or a TFTP Server | 7-12 |
| Setting Up the Syslog Server | 7-12 |
| Pre-Installation of the Configuration Template Module | 7-12 |
| Verifying that Oracle XML Database is Installed | 7-12 |
| Configuring OIM to Keep Inactive Sessions Running | 7-13 |
| Restoring Configuration When the Device Model Contains Configlets | 7-13 |

8 IP Service Activator Post-installation Tasks

| | |
|--|-----|
| IP Service Activator Post-installation Tasks | 8-1 |
| Configuring Web Services | 8-1 |

9 Upgrading and Patching IP Service Activator

| | |
|---|------|
| About Upgrading IP Service Activator | 9-1 |
| Supported Upgrade Paths | 9-1 |
| About the Upgrade Process | 9-2 |
| About Network Processor Upgrade Tool Script - npUpgrade | 9-3 |
| Preparing for the IP Service Activator Upgrade | 9-4 |
| Prerequisites | 9-4 |
| Terminology | 9-4 |
| Preparing to Upgrade | 9-5 |
| Backing Up Custom Configuration Policies and Cartridges | 9-6 |
| Backing Up IP Service Activator | 9-7 |
| Upgrading to the New IP Service Activator Software | 9-8 |
| Updating Customizations | 9-9 |
| Updating Cartridge Registry (MIPSA_registry.xml) | 9-10 |
| Updating Capabilities | 9-11 |
| Cisco Cartridge Configuration Utility | 9-12 |
| Upgrading a CTM Template Schema to Version 4 or later | 9-12 |

| | |
|---|------|
| Upgrade Tools | 9-13 |
| Network Processor on Multiple Servers | 9-13 |
| Running npAdmin to Update Network Processor Internal Data | 9-13 |
| Running npUpgrade: Network Processor Upgrade Script | 9-14 |
| Running Failure Analysis on npUpgrade Results | 9-14 |
| Running dbUpgrade to Upgrade the Database | 9-15 |
| Starting the New IP Service Activator System | 9-16 |
| Network Processor Configuration | 9-16 |
| Starting the New IP Service Activator System | 9-16 |
| Upgrading IP Service Activator to a New Location | 9-18 |
| Performing Post-Upgrade Data Cleanup | 9-19 |
| Cleaning Up Interface Description Mismatches | 9-19 |
| Rolling Back the Upgrade | 9-20 |
| Prerequisites | 9-20 |
| Rolling Back the Upgrade | 9-20 |
| Upgrade Reference Information | 9-20 |
| Network Processor Upgrade Tool default.properties File | 9-20 |
| npUpgrade Script Logging Properties | 9-21 |
| npUpgrade Script Failure Analysis | 9-21 |
| Sub-interface Unit Number on Juniper | 9-22 |
| Interface Per-packet Load-sharing on Cisco | 9-22 |
| Interface Description String on Cisco | 9-22 |
| Network Processor Upgrade Directory Structure | 9-22 |
| Patching IP Service Activator | 9-23 |
| Prerequisites | 9-23 |
| Installing a Patch | 9-24 |
| Updating Configuration Policy Definitions | 9-24 |

10 Uninstalling IP Service Activator

| | |
|--|------|
| Uninstalling IP Service Activator from UNIX Server | 10-1 |
| Uninstalling IP Service Activator Client | 10-2 |

11 Troubleshooting the Installation

| | |
|--|------|
| Oracle Database Installation Fails to Run | 11-1 |
| Oracle Database Installation Fails Before Completion | 11-2 |
| Manually Configuring Oracle Client Connection: Solaris | 11-2 |
| Client Errors | 11-3 |
| omniORB Use of TCP Wrappers | 11-3 |
| Oracle Universal Installer Error | 11-3 |

| | |
|--|------|
| Client Cannot Connect to Policy Server | 11-4 |
| Loading SharedPolicyData.policy to Avoid Incomplete Software Upgrade | 11-4 |
| IPSAPS Does Not Work | 11-4 |
| Problem Running npUpgrade on Linux | 11-4 |

A Installation Checklists and Worksheet

| | |
|--|-----|
| Oracle Database Installation Data | A-1 |
| IP Service Activator Multi-host General Installation Checklist | A-2 |
| Client Installation Checklist | A-3 |
| Site Survey Worksheet | A-3 |

B Directories and Files

| | |
|--------------------------|-----|
| Directory Structure | B-1 |
| Symbolic Links | B-2 |
| Directories and Contents | B-2 |

Preface

This guide provides instructions for installing Oracle Communications IP Service Activator components and modules using the Oracle Universal Installer.

Audience

This document is intended for network administrators and equipment planners. Readers should be familiar with the following topics:

- Solaris or Linux and its commands
- Oracle Database
- Installing and configuring software on Unix and Windows environments
- A text editor such as vi

Example commands are shown in Bourne shell syntax. This is the recommended shell for the Oracle user and is the syntax used in the template files supplied with IP Service Activator. The Bourne shell is included with all UNIX systems.

Before choosing the hardware configuration to host IP Service Activator, see "[Planning an IP Service Activator Installation](#)" for engineering guidelines and information about preparing for an IP Service Activator install.

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of

these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

IP Service Activator Installation Overview

This chapter provides an overview for installing Oracle Communications IP Service Activator.

IP Service Activator Installation Overview

Before beginning the IP Service Activator installation, you need to plan the installation and overall system configuration, gather information, and set up your hosts (servers and workstations). See "[About Planning an IP Service Activator Installation](#)" for engineering guidelines and other planning details.

For later reference, you need to gather and record important installation information, such as settings, account names, and passwords. This document provides checklists in "[Installation Checklists and Worksheet](#)".

Server and workstation preparation can include the installation and configuration of:

- Operating systems, including the creation of user accounts
- Oracle Database software
- Other required third-party software components

After the servers and workstations are correctly configured, you run the Oracle Universal Installer. Depending on system configuration, IP Service Activator server software is installed on at least one, and possibly multiple, hosts. IP Service Activator client software is installed on each Windows host.

After software installation, post-installation activities may be required. These are described in this guide and in *IP Service Activator System Administrator's Guide*.

Installation Sequence

The following list outlines the main tasks to install IP Service Activator:

1. Plan the installation and prepare your hosts for IP Service Activator installation. See "[Planning an IP Service Activator Installation](#)".
2. Perform the pre-installation checks. See "[Pre-installation Checklist](#)".
3. Install the operating system (OS) and apply patches. Complete additional OS configuration tasks. See "[Installing IP Service Activator on an Oracle Solaris or Linux Server](#)".
4. Install and configure Oracle Database software. See "[Installing and Configuring Oracle Database Software](#)".
5. Perform post-installation tasks on Oracle Database software. See "[Oracle Database Post-Installation Tasks](#)".
6. Configure the CORBA ORB settings. See "[CORBA ORB Configuration for IP Service Activator](#)".

7. If you are installing the Configuration Template Module (CTM), perform additional configuration steps to support it. See "[Pre-Installation of the Configuration Template Module](#)".
8. Install supplemental software components. See "[Installing Supplemental Software Components](#)".
9. Install the necessary IP Service Activator components on the server(s). See "[Installing IP Service Activator on an Oracle Solaris or Linux Server](#)".
10. Install the IP Service Activator client and required modules on the Windows hosts. See "[Installing the IP Service Activator Client on Windows](#)".
11. Apply any required IP Service Activator software patches.
12. Perform additional setup tasks that apply to your system prior to starting IP Service Activator. See "[Pre-Installation of the Configuration Template Module](#)" for a brief list. Details on the additional setup tasks are given in the *IP Service Activator System Administrator's Guide*.

Pre-installation Checklist

Before beginning the installation, check that:

- You have read "[Planning an IP Service Activator Installation](#)" and planned how to distribute IP Service Activator components across your hosts. You can record the plan for each host in the Installation Checklists. See "[Installation Checklists and Worksheet](#)".
- If you have a previous installation of IP Service Activator, do the following:
Perform a proper shutdown of the IP Service Activator system, and uninstall it before proceeding with a new installation.

If you are upgrading from a previous IP Service Activator system that used an Oracle-supplied serial number, you must re-use that serial number in the new installation.

Note:

To uninstall IP Service Activator 7.5, you do not have to run the **uninstall.sh** script. The Oracle Universal Installer has the capability to uninstall IP Service Activator. You can also install and uninstall IP Service Activator 7.5 on your local machine.

Downloading the IP Service Activator Software

To download the IP Service Activator software from the Oracle software delivery website (<https://edelivery.oracle.com>):

1. Select the IP Service Activator software package for your platform from the Oracle E-Delivery Web site.
2. Download the software package.
3. Extract the components that you need from the downloaded file.
4. Follow the installation procedure for each component that you want to install.

2

Planning an IP Service Activator Installation

This chapter describes how to plan an Oracle Communications IP Service Activator installation.

About Planning an IP Service Activator Installation

Before beginning the IP Service Activator installation, you need to plan the installation and overall system configuration, gather information, and set up your hosts (servers and workstations).

For later reference, you need to gather and record important installation information, such as settings, account names, and passwords. This document provides checklists and a worksheet in "[Installation Checklists and Worksheet](#)".

Server and workstation preparation can include the installation and configuration of:

- Operating systems, including the creation of user accounts
- Oracle Database software
- Other required third-party software components

After the servers and workstations are correctly configured, you run the Oracle Universal Installer. Depending on system configuration, IP Service Activator server software is installed on at least one, and possibly multiple, hosts. IP Service Activator client software is installed on each Windows host.

After software installation, post-installation activities may be required. These are described in this guide and in *IP Service Activator System Administrator's Guide*.

Overview of IP Service Activator Architecture

This section provides an overview of the IP Service Activator distributed architecture. It includes the following topics:

- IP Service Activator components and modules
- Additional software recommendations and requirements

IP Service Activator Components and Modules

IP Service Activator has a modular software architecture that supports deployment across multiple hosts in a network. This section describes components and modules with a brief overview of how they are deployed in a production installation.

IP Service Activator consists of the core product components described in [Table 2-1](#).

Table 2-1 IP Service Activator Components

| Component | Description |
|------------------------------------|---|
| Policy Server | <p>The Policy Server is the central component of the system and is responsible for the following:</p> <ul style="list-style-type: none"> • Coordinates access to the data repository from the client components • Performs network topology discovery • Validates and transmits policy configurations to the network processor components. <p>Two sub-components, the Naming Service and the System Logger, maintain the naming and location information for the other system components and log system messages.</p> <p>One Policy Server is installed per IP Service Activator installation.</p> |
| Network Processor | <p>The network processor provides XML-based cartridges that support vendor-specific device configurations. Cartridges enable you to support your existing services, and support emerging services and business needs. Cartridges operate in conjunction with IP Service Activator core product.</p> |
| Cartridges | <p>Cartridges enable you to support your existing services, and support emerging services and business needs. Cartridges operate in conjunction with IP Service Activator core product.</p> |
| Windows-based client | <p>The graphical user interface (GUI) provides access to the database and Policy Server. This component is supported on systems running Windows 2000 and above.</p> <p>Multiple instances of the GUI can be used concurrently, by adding additional Windows GUI hosts and installing the IP Service Activator client.</p> |
| Component Manager | <p>The component manager starts all system components, and monitors and reports their status.</p> <p>The component manager is required on each host system on which one or more IP Service Activator components are installed (except the client).</p> |
| Configuration Management Collector | <p>The Configuration Management Collector collects device configuration changes as they occur and archives these changes in the IP Service Activator repository.</p> |
| Database | <p>The Oracle database management system is used for the data repository for IP Service Activator and must be running on your network. The database stores data related to the network topology and all configured services.</p> |

In most production environments, IP Service Activator components are installed on multiple hosts in order to distribute the processing requirements. IP Service Activator resource requirements are CPU core-centric and all hardware resource requirements are expressed in terms of CPU- core requirements.

Most current servers are constructed around CPUs that contain two or more cores, and it is these cores that are referenced. An example of this would be a Sun Enterprise M5000 Server. This server can be configured with the SPARC64 VI processor, which is a dual (or split) core processor. While this server can contain up to 8 processors, those 8 processors represent 16 CPU-cores when configured with the dual-core SPARC64 VI. Configuring the M5000 Server with the quad-core SPARC64

VII processor could represent 32 CPU-cores, when 8 processors are present. This IP Service Activator planning section focuses on the number of the CPU-cores.

This reduces the total cost of ownership because multiple IP Service Activator components are deployed on a single, appropriately-sized server.

Optional Integration Components

[Table 2-2](#) describes the integration components that can be installed as part of the base product.

Table 2-2 IP Service Activator Optional Integration Components

| Component | Description |
|-------------------------------|--|
| OSS Integration Manager (OIM) | Consists of an open API that enables easy integration between the core system and external systems such as flow-through provisioning, fault management, and performance monitoring. |
| Web Services | An optional component of the IP Service Activator installation that allows IP Service Activator to integrate with external systems. To use the Web Services with IP Service Activator, you must complete the following tasks in sequential order: install a WebLogic server and create a WebLogic domain. |

Optional Service Modules

[Table 2-3](#) describes the optional modules that are installed separately from the base product.

Table 2-3 IP Service Activator Optional Service Modules

| Component | Description |
|---------------------------------|--|
| Configuration Management Module | The Configuration Management module enables you to implement automated and consistent configuration management practices, such as: <ul style="list-style-type: none"> • Archiving device configurations • Tracking real-time configuration changes • Tracing configuration changes • Repairing managed services • Restoring device configurations |
| Configuration Template module | The Configuration Template module streamlines the activation of services on network objects. Through the use of pre-defined or customized templates, the module extends the capability of the IP Service Activator to configure devices and interfaces. |
| TACC module | The Threshold Activated Configuration Control (TACC) module, along with device level Thresholding, allows you to accept or reject transactions that exceed the configuration removal threshold. |

The currently supported software versions are found in "[Supported Devices and Operating Systems](#)".

Additional Software Requirements

The Oracle Instant Client connection (OIC) is required for Policy Server, System Logger, cartridges, and Network Processor. The OIC is installed as part of the IP Service Activator installation.

Although the OIC is required for parts of the IP Service Activator client, such as viewing system logs, it is not automatically installed during client installation. Select the OIC option for installation during the client installation process.

Oracle Real Application Clusters in IP Service Activator

As of IP Service Activator 7.0, connectivity to Oracle Real Application Clusters (Oracle RAC) instances is supported. An Oracle RAC deployment allows for improved IP Service Activator reliability because the Oracle RAC deployment can contain multiple nodes, and continues to support database access as long as at least one node is active and available. When IP Service Activator is connected to an Oracle RAC instance, failover activity, within the database deployment, is invisible to IP Service Activator.

IP Service Activator uses database resources such that multiple nodes within an Oracle RAC deployment do not positively impact performance, but safeguard that IP Service Activator deployment against most database failure issues.

Planning Guidelines and Engineering Considerations

This section describes the hardware and system configuration considerations applicable to establishing a functioning IP Service Activator system in a network. It includes the following topics:

- System configuration overview
- Component configuration recommendations
- Hardware requirements

System Configuration Overview

This section describes key roles and responsibilities in configuring and maintaining an IP Service Activator deployment, and provides an overview of the IP Service Activator components and the concepts to be considered when planning a deployment.

Assistance in the Sizing Process

This section will help you correctly identify the hardware necessary for a successful IP Service Activator implementation. The implementation should be performed with the aid of Oracle Global Customer Support or Sales Engineering representatives.

Customer Responsibilities

After an IP Service Activator system has been deployed, it is the responsibility of the deployment owner to monitor the managed network growth and resource use of the various IP Service Activator components.

Relevant IP Service Activator metrics include the number of devices and the number of network sites. This information is available through the System Statistics view in the client.

Relevant operating system metrics include CPU utilization and real memory consumption. There are many third-party tools, including SunSolve Solutions and command-line processes, that provide this information. Consult Oracle Global Customer Support for further details.

IP Service Activator Component Architecture

A typical IP Service Activator system consists of the following components:

- Policy Server
- Network Processors
- Cartridges
- Graphical User Interfaces (one or more)
- System Logger
- Component manager
- Naming Service
- Databases to persist the Object Model and Configuration Management Archives
- Supplemental software components (See "[Supported Devices and Operating Systems](#)" for details.)

Optionally, IP Service Activator systems may also contain one or more instances of:

- OSS Integration Manager (OIM)
- Web Service

A typical IP Service Activator implementation has specific CPU-core requirements for the following groups of components:

- Policy Server, OIM, System Logger, Naming Service, Component Manager: Four CPU-cores (two cores for Policy Server, one core for System Logger, Naming Service, Component Manager, and so on, and one core for OIM).
- Network Processor: Two or more CPU-cores per instance
- Database Server: Two to four CPU-cores
- Client: May be multiple workstations

[Table 2-4](#) lists the components of IP Service Activator and their CPU-cores. The following optional modules are installed separately from the base product.

Table 2-4 Component CPU-core Requirements

| Component | CPU-cores |
|--|----------------------|
| Policy Server | 2 (minimum) |
| System Logger, Naming Service, and Component Manager | 1 (minimum) |
| OSS Integration Manager | 1 (per OIM instance) |
| Network Processor | 2 |
| Database Server | 2 (minimum) |

A component manager must be present and active on each server to manage all components except the Naming Service, the database, the client, and the application server.

With Oracle Solaris 11 or Oracle Linux 8, OS containers allow for fewer larger servers to host complete IP Service Activator deployments over multiple containers as opposed to deploying many smaller servers to accomplish the task.

Oracle Database, for performance reasons, should be running on a separate server from the Policy Server and Network Processor.

For required operating system and peripheral component system (for example Solaris) versions, refer to "[Supported Devices and Operating Systems](#)". For Oracle Database, make sure you are using the latest version (19c or later).

3

IP Service Activator System Requirements

This chapter describes the software and hardware requirements for installing Oracle Communications IP Service Activator.

Support for Linux

IP Service Activator supports Oracle Linux 8.2 (or later) as a 64-bit application. For new host installations, install Oracle Linux as a 64-bit application. The IP Service Activator client runs on Windows. See "[Support for Windows](#)" for more information.

To install IP Service Activator on Linux, follow the server installation procedure. Differences between an Oracle Solaris and a Linux installation are identified within the procedure steps.

Support for Windows

IP Service Activator supports the following versions of Windows, all running on 64-bit applications:

- Windows Server 2019
- Windows 10
- Windows 11

Solaris Installation and Configuration

For new host installations, install the full Oracle Enterprise Manager (OEM) version of Solaris. This ensures that Solaris functions well with IP Service Activator.

Check the Solaris OS Version

IP Service Activator is supported on the following Solaris operating systems (OS):

- Solaris 11.4 (or later)

For supported versions of third-party software, including Solaris, see "[Supported Devices and Operating Systems](#)".

To check the Solaris OS version, enter:

```
$ uname -r
```

or

```
$ uname -a
```

The SunOS version is returned. For Solaris 11 systems, 5.11 is returned.

For a more detailed indication of your Solaris version, check the **`/etc/release`** text file:

Go to the **/etc** directory of the installed image and enter:

```
# more release
```

The installed version is returned.

For example:

```
Oracle Solaris 11.3 SPARC  
Copyright (c) 1983, 2018, Oracle and/or its affiliates. All rights reserved.  
Assembled 09 May 2018
```

Check the Solaris Patches

Ensure that the latest recommended Solaris patch cluster is installed on each IP Service Activator host machine. This includes those patches recommended for Solaris by Sun.

Patches are available for download on Oracle Technology Network at:

<http://www.oracle.com/technetwork/topics/security/whatsnew/index.html>

To check which patch revision numbers you have installed:

On the Solaris 64-bit platform, enter:

```
$ showrev -p | more
```

Supported Devices and Operating Systems

The following tables list IP Service Activator support for vendor devices and operating systems in this release. For more information about which services are supported on each device and OS combination, refer to the respective cartridge guide or device support guide.

Cisco IOS XR Cartridge

[Table 3-1](#) lists the Cisco IOS XR cartridge support on Cisco devices and IOS XR versions.

Table 3-1 Cisco IOS XR Cartridge Support

| Devices Supported by IP Service Activator | Cisco IOS XR Version |
|---|----------------------|
| Cisco IOS XRv 9000 Series | 6.x, 7.x |

Cisco IOS Cartridge

[Table 3-2](#) lists the Cisco IOS cartridge support on Cisco devices and IOS versions.

Table 3-2 Cisco IOS Cartridge Support

| Devices Supported by IP Service Activator | Cisco IOS Version |
|---|--|
| Cisco 1000, 2000, 3000, 4000, 6000, 7000, 10000, 12000 series devices | IOS 12.2(33)SRE+, IOS 12.4(24)T+, IOS 12.0(33)S+, IOS 15.0(1)M+, IOS 15.1(2)T+, IOS 15.5(2)S+, IOS 15.6(2)T+, IOS 16.6.1+, and IOS 17.3+ |

Cisco CatOS Cartridge

[Table 3-3](#) lists the Cisco CatOS cartridge support on Cisco devices and CatOS versions.

Table 3-3 Cisco CatOS Cartridge Support

| Devices Supported by IP Service Activator | Cisco CatOS Version |
|---|---------------------|
| Cisco 3500, 3750, 4500, 5500, 6500 series devices | CatOS 7.6, 8.5 |

Huawei Cartridge

[Table 3-4](#) lists the Huawei cartridge support on Huawei devices and VRP versions.

Table 3-4 Huawei Cartridge Support

| Devices Supported by IP Service Activator | VRP Version |
|---|---------------|
| Huawei Quidway Series Routers AR18-xx, AR28-xx, AR46-xx | 3.4 |
| Huawei Quidway NetEngine 05/08/16 | 5.3, 5.5, 5.7 |
| Huawei Quidway NetEngine 16E, 40-2, 40-4, 40-8, 80 | 5.3, 5.5, 5.7 |
| Huawei Quidway NetEngine 40E, 80E | 5.3, 5.5, 5.7 |
| Huawei Quidway Eudemon 500, 1000 | 3.1 |
| Huawei CX600 | 5.3, 5.5, 5.7 |
| Huawei AR 1220, 2220, 2240, 3260 | 5.130 |
| Huawei NE40E-X8A | 8.80 |
| Huawei NE40E-X3 | 5.160 |

Juniper JUNOS Cartridge

[Table 3-5](#) lists the Juniper JUNOS cartridge support on Juniper devices and JUNOS versions.

Table 3-5 Juniper JUNOS Cartridge Support

| Devices Supported by IP Service Activator | JUNOS Version |
|---|---|
| Juniper SRX-series Juniper MX-series | JUNOS 15x, 17.x, 18.x, 19.x, 20.x, 21.x, and 22.x |

Pre-installation Tasks for Solaris and Linux

This section describes the tasks that you must complete before you install IP Service Activator on Solaris and Linux operating systems.

Enabling Per-process Core Dumps for Solaris

For Solaris, you must verify that the `COREADM_PROC_ENABLED` is enabled in the system core configuration file: `coreadm.conf`. If `COREADM_PROC_ENABLED` is enabled, the corresponding core file is generated for the IP Service Activator process when a core dump occurs. You can use the `pstack` tool to review and troubleshoot any core dump of a process.



Note:

`COREADM_PROC_ENABLED` is a system default.

To see the values of the core dump parameters in the `coreadm.conf` file, you can use this command:

```
cat /etc/coreadm.conf
```

The parameters of this file are as follows:

```
COREADM_GLOB_PATTERN=  
COREADM_GLOB_CONTENT=default  
COREADM_INIT_PATTERN=core  
COREADM_INIT_CONTENT=default  
COREADM_GLOB_ENABLED=no  
COREADM_PROC_ENABLED=yes  
COREADM_GLOB_SETID_ENABLED=no  
COREADM_PROC_SETID_ENABLED=no  
COREADM_GLOB_LOG_ENABLED=no
```

To set the core dump parameters, you can run the following command:

```
coreadm
```

Enabling Per-process Core Dumps for Linux

With some applications requiring Linux, the `coreadm` tool is missing. Instead, core file management is configured in the kernel configuration file: `/etc/sysctl.conf`.

You need to enable core dumps from `setuid` process, remove file size limits for core dumps, and save them in an appropriate location using meaningful names. To do this, you need to add the following lines into the `/etc/sysctl.conf` file.

- `fs.suid_dumpable = 2`
- `kernel.core_pattern = /var/core/core_%h_%e_%u_%g_%t_%p`

To make sure you are not imposing limits on the core files, you need to add the following to the `/etc/sysconfig/init` file:

- `DAEMON_COREFILE_LIMIT='unlimited'`

After you update the `/etc/sysctl.conf` and `/etc/sysconfig/init` files, you can refresh the settings by running `sysctl`, as follows:

```
[root@altix ~]# /sbin/sysctl -p
< list of kernel tunables >
fs.suid_dumpable = 2
kernel.core_pattern = /var/core/core_%h_%e_%u_%g_%t_%p
< list of kernel tunables >
```

Setting File Resources for Device Discovery

A host supporting IP Service Activator must be configured to support a certain minimum number of available open files (File Descriptors) in order for IP Service Activator to successfully discover large numbers of devices (up to 65535) within one device discovery task. The setting for the number of available file descriptors should be 1024 or greater.

To permanently set the File Descriptors value on the Policy Server host:

1. Open the `/etc/system` file.
2. Add the following two lines:

```
set rlim_fd_cur=1024 (or greater)
set rlim_fd_max=1024 (or greater)
```

3. Save and close the file.

To determine the current Solaris kernel settings, enter:

```
ulimit -a
```

If the value of the `nfiles` (descriptors) is greater than or equal to 1024, enough file descriptors are available.

There is no advantage, from a scalability or performance standpoint, to have more than 1024 file descriptors available. Setting these parameters higher uses additional memory resources with no improvement in IP Service Activator performance.

Note:

Ensure that the Max File descriptors is set to a value of at least 1024, to eliminate platform issues.

Note:

For increasing the number of available open files (file descriptors), you must edit `etc/system` file in Solaris. The corresponding file for Linux is `etc/security/limits.conf`. The limit is 1024 in Linux by default.

Synchronizing IP Service Activator Host Machines

You should synchronize the system time between IP Service Activator host machines using time synchronization software. Where machines are not synchronized, delays are likely to occur when configuring devices.

Ensure you synchronize the NTP times correctly.

IP Service Activator Administrator UNIX User ID (ipsaadm)

The IP Service Activator administrator (user ID **ipsaadm**) is the UNIX user account given permissions (during installation) to start and stop the naming service and component manager manually. You must create this user account prior to IP Service Activator software installation.

When creating the **ipsaadm** user, specify the following details:

- Username: ipsaadm
- Group: ipsagr
- Secondary group: sys
- Login shell: /bin/bash
- Home directory: select any location (known in this document as *Service_Activator_home*)

Throughout this document, **ipsaadm** is used as the UNIX user ID associated with IP Service Activator. If you have defined another UNIX user ID for specific uses with IP Service Activator, use it instead of **ipsaadm** where appropriate.

Setting Permissions for the Installation UNIX User ID

The default permissions set for the installation UNIX account user ID affect the permissions of the directories and files created by the Oracle Universal Installer and configured by the configuration tool. The rest of this section refers to **ipsaadm** as the account used to run the install.

You must set the umask for the **ipsaadm** account appropriately for your needs before running the Installer.

The Installer uses the umask from the **ipsaadm** account during the installation to determine how to adjust the directories and files that it creates.

To set the umask for the ipsaadm account, use the UNIX umask command:

```
umask [file_creation_mask]
```

See the Solaris or Linux UNIX documentation for more information about the user account umask.

For example, if the **ipsaadm** account has a umask of 027, this translates to permissions of "rwxr-x---". The Installer then creates directories with permissions of "rwxr-x---" and configuration files with the permissions "rw-r----".

 **Note:**

It is recommended that you use the umask setting of 077, which translates to directory permissions of "rwx-----" and configuration file permissions of "rw-----" (full access to the user and no access to the group or anyone else).

Java Development Environment

To develop Java code, you need a development environment, such as the Java Standard Edition (64-bit), previously known as the Java Development Kit (JDK).

It is recommended that you use the following version:

- Java SE 1.8.x with the latest Critical Patch Update

For more information about developing application programming interfaces for IP Service Activator, see *IP Service Activator API Developer's Guide*.

Hardware Requirements

The tables in this section list the hardware required for IP Service Activator to manage networks. The tables include the hardware required for third-party software used in support of IP Service Activator.

The hardware sizing recommendations in this section assume that the Optimized Customer Edge (CE) and Provider Edge (PE) management capabilities are applied in large and very large network deployments.

In order to apply these minimum requirements effectively, you must determine whether you require hardware for a CE or PE deployment. For example, if more than 20 percent of the devices in your deployment are PEs, you should use the PE minimum hardware requirements. Accurately completing the site survey worksheet can help you determine your needs. See "[Site Survey Worksheet](#)" for more information.

The network processor can support an equal number of large provider edge routers as customer edge routers. The network processor is limited, however, by the number of transform threads that are available. Transform threads are a subset of worker threads. Each transform thread calculates the difference between the service model and the device model. For provider edges, this calculation requires more memory and time than for customer edges. And while a network processor with a 16gb server allocated with 12gb JVM can support approximately 40,000 devices of any type, you should limit the number of transform threads to approximately 10-20. Limiting the number of transform threads ensures that you don't tax the JVM heap in a scenario where transform threads are calculating deltas for 50 provider edges simultaneously. However, if you have only 10 transform threads calculating 60 devices changes, the network processor can calculate only 10 at a time. You can monitor the JVM heap with the standard java tool and increase the number of transform threads if you have available memory. Oracle recommends that you distribute provider edges to multiple network processors and address gaps with smaller devices.

 **Note:**

When considering your hardware requirements, ensure that you remember to allocate space for running the OS.

Table 3-6 lists the minimum hardware requirements for Policy Server.

Table 3-6 Policy Server Minimum Hardware Requirements

| Network Size (number of managed CE or PE devices) | CPU-threads for CEs | CPU-threads for PEs | RAM for CEs | RAM for PEs |
|---|---------------------|---------------------|-------------|-------------|
| Small (1-1500) | 1 | 2 | 1 GB | 2 GB |
| Medium (1500-4000) | 1 | 2 | 2 GB | 4 GB |
| Large (4000-10000) | 2 | 4 | 2 GB | 4 GB |
| Very Large (10000 +) 64-bit | 2+ | 4+ | 8 GB | 16 GB |

Table 3-7 lists the minimum hardware requirements for Integration Manager.

Table 3-7 Integration Manager Minimum Hardware Requirements

| Network Size (number of managed CE or PE devices) | CPU-threads | RAM for CEs | RAM for PEs |
|---|-------------|-------------|-------------|
| Small (1-1500) | 1 | 500 MB | 2 GB |
| Medium (1500-4000) | 1 | 500 MB | 2 GB |
| Large (4000-10000) | 1 | 1 GB | 4 GB |
| Very Large (10000 +) 64-bit | 1 | 2 GB | 8 GB |

Table 3-8 lists the minimum hardware requirements for Network Processor with Configuration Management Collector.

Table 3-8 Network Processor with Configuration Management Collector Minimum Hardware Requirements

| Network Size (number of managed CE or PE devices) | CPU-threads for CEs | CPU-threads for PEs | RAM for CEs | RAM for PEs |
|---|---------------------|---------------------|-------------|-------------|
| Small (1-1500) | 3 | 6 | 5 GB | 10 GB |
| Medium (1500-4000) | 3 | 6 | 5 GB | 10 GB |
| Large (4000-10000) | 3 | 6 | 5 GB | 10 GB |
| Very Large (10000 +) 64-bit | 4 | 8 | 8 GB | 16 GB |

Table 3-9 lists the minimum hardware requirements for IP Service Activator Client.

Table 3-9 IP Service Activator Client Minimum Hardware Requirements

| Network Size (number of managed CE or PE devices) | CPU-cores | RAM |
|---|-----------|------|
| Small (1-1500) | 1 | 1 GB |
| Medium (1500-4000) | 1 | 1 GB |
| Large (4000-10000) | 1 | 2 GB |
| Very Large (10000 +) 64-bit | 1 | 4 GB |

[Table 3-10](#) lists the minimum hardware requirements for Oracle Database Server. Ensure that you are using Oracle Database 19c (19.15.0.0.0).

Table 3-10 Oracle Database Server Minimum Hardware Requirements

| Network Size (number of managed CE or PE devices) | CPU-threads for CEs | CPU-threads for PEs | RAM for CEs | RAM for PEs |
|---|---------------------|---------------------|-------------|-------------|
| Small (1-1500) | 2 | 8 | 4 GB | 8 GB |
| Medium (1500-4000) | 2 | 8 | 4 GB | 8 GB |
| Large (4000-10000) | 4 | 16 | 4 GB | 8 GB |
| Very Large (10000 +) 64-bit | 4 | 16 | 8 GB | 16 GB |

[Table 3-11](#) lists the minimum hardware requirements for Oracle WebLogic Server. Ensure that you are using Oracle WebLogic Server 14c (14.1.1.0.0).

Table 3-11 Oracle WebLogic Server Minimum Hardware Requirements

| Network Size (number of managed CE or PE devices) | CPU-cores | RAM |
|---|-----------|------|
| Small (1-1500) | 2 | 2 GB |
| Medium (1500-4000) | 2 | 2 GB |
| Large (4000-10000) | 2 | 2 GB |
| Very Large (10000 +) 64-bit | 2 | 2 GB |

[Table 3-12](#) lists the minimum hardware requirements for Web Services.

Table 3-12 Web Services Minimum Hardware Requirements

| Daily IP Service Activator Order Volume | CPU-cores | RAM |
|---|-----------|------|
| Small (1-500) | 2 | 2 GB |
| Medium (500-1500) | 2 | 4 GB |
| Large (1500+) | 4 | 8 GB |

4

Installing and Configuring Oracle Database Software

This chapter provides Oracle Communications IP Service Activator-specific guidance for installing Oracle Database software.

IP Service Activator supports Oracle Database 19c (19.15.0.0.0). For more information about the currently supported version numbers of additional software components, refer to "[IP Service Activator System Requirements](#)".

Note:

As you perform the installation, record custom values in the Oracle Database Installation Data checklist. See "[Installation Checklists and Worksheet](#)".

Oracle Database software components must be installed before you begin installation of IP Service Activator.

For the latest versions of Oracle Database documentation, with details about the installation and configuration of Oracle Database software, consult the following Oracle documentation repository:

<http://docs.oracle.com/en/database/>

If Oracle Database is already installed, arrange with your on-site Oracle Database administrator to create and configure the IP Service Activator database and to configure Oracle Database components. When this is complete, you can install IP Service Activator system components. Refer to the Oracle Installation Data checklist in "[Installation Checklists and Worksheet](#)" for configuration information.

If you are already running an instance of the Oracle Instant Client, you can configure IP Service Activator to use it by providing connection information during the IP Service Activator installation process.

Preparation

This section provides information about some of the configuration decisions you must make before installing Oracle Database.

For supported versions of software components, including Oracle Database software, see "[IP Service Activator System Requirements](#)".

Some of the IP Service Activator components (for example, Policy Server, System Logger, Configuration Management, and Network Processor) require that an Oracle Instant Client be installed on the machine on which they reside. The Oracle Instant Client is bundled with IP Service Activator and is typically installed automatically.

Installing Oracle Database Using Oracle Universal Installer

Install the Oracle Database software using the Oracle Universal Installer. When prompted, choose a 'General Purpose' database installation.

When installing, the **listener.ora**, **sqlnet.ora**, and **tnsnames.ora** environment files are configured. The naming method for connecting to the database must be set to the default local naming method.

Provide the following information when prompted.

In the Database Identification window, specify:

- Global Database Name: **IPSA.WORLD**

The Global database name consists of the System Identifier (IPSA) and your network domain.

- System Identifier (SID), \$ORACLE_SID: **IPSA**

If the environment variables were set before Oracle Database installation, this is the default value.

In the **Database Character Set** dialog box, click the **Choose one of the common character sets** button, and select a character set.

Oracle recommends using the AL32UTF8 character set for the IP Service Activator database instance. However, if IP Service Activator is the only application that is using the database instance, you can use the default character set for your location.

The national character set can be left to the default value for your location.

Oracle Database Post-Installation Tasks

Additional Oracle Database configuration tasks may be required. For more information, see *Oracle Database Installation Guide*.

Updating the Net Service Name Setting

After installing Oracle Database, you might have to update the Net Service Name setting.

Note:

The Net Service Name value in the **IPSA** section of the **tnsnames.ora** file on the Policy Server machine must match the equivalent Net Service Name value in your global Oracle Database settings.

Setting Up the IP Service Activator Environment in Oracle Database

When you create an Oracle Database tablespace for use with IP Service Activator, Oracle recommends using **IPServiceActivatorDb** for the tablespace name.

 **Note:**

You can choose a different name. Make sure it is an identifiable name for the IP Service Activator system tablespace and that there are no spaces between its characters, and then record the name in the Oracle Database Installation Data checklist located in "[Installation Checklists and Worksheet](#)".

Text that you enter in the dialog box is automatically displayed in capitals.

Use an initial file size of 250 MB. Use the AUTOEXTEND parameter, and set the **Increment** value to **5 MB**. Set the **Maximum size** to **Unlimited**.

When you create an Oracle Database user for IP Service Activator, set the Name to **admin** (or other suitable database user name). This is the name that you are prompted for when IP Service Activator is installed. Set your password and make sure you record it in the Oracle Installation Data checklist, located in "[Installation Checklists and Worksheet](#)".

Set the Default value for Tablespaces to **IPServiceActivatorDb**. This ensures that IP Service Activator tables use the correct tablespace. Leave the Temporary tablespace as the default value: *system-assigned*.

Grant the new Oracle Database user the following privileges:

- UNLIMITED TABLESPACE
- CONNECT
- RESOURCE
- CREATE VIEW
- CREATE DIRECTORY
- CREATE PROCEDURE
- CREATE TRIGGER
- CREATE TABLE
- CREATE TYPE
- CREATE SEQUENCE

The SQL commands to create the tablespace, Oracle Database user, and granting privileges are as follows:

```
> sqlplus system/manager
SQL> connect / as sysdba
SQL> create tablespace <tablespacename> logging datafile '/opt/oracle/oradata/
<databaseinstancename>/<tablespacename>.dbf' size 250M reuse autoextend on next 5M
maxsize unlimited default storage (initial 128K next 128K minextents 1 maxextents
2147483645 pctincrease 0);
SQL> create user ipsaadm profile "DEFAULT" identified by <password for ipsaadm user>
default tablespace <tablespacename> temporary tablespace <temporarytablespacename>
account unlock;
SQL> grant unlimited tablespace to ipsaadm;
SQL> grant connect to ipsaadm;
SQL> grant resource to ipsaadm;
SQL> grant create view to ipsaadm;
SQL> create directory ipsa_plsql_dir as '<ipsadir>';
SQL> grant read,write on directory ipsa_plsql_dir to ipsaadm;
```

```
SQL> grant execute on sys.utl_file to ipsaadm;  
SQL> grant create procedure to ipsaadm;  
SQL> grant create trigger to ipsaadm;  
SQL> grant create table to ipsaadm;  
SQL> grant create type to ipsaadm;  
SQL> grant create sequence to ipsaadm;
```

Suggested minimum values for Oracle Database parameters are as follows:

- shared_pool_size:50 331 648
- large_pool_size:8 388 608
- db_cache_size:25 165 824
- undo_management:auto
- undo_retention:10 800
- processes:1000
- open_cursors:5000

5

Installing and Configuring WebLogic Server

This chapter provides information about installing and configuring Oracle WebLogic Server for Oracle Communications IP Service Activator.

Installing WebLogic Server Software

You install WebLogic Server on all machines that will participate in your domain. The installation directories must be the same on all machines. For complete installation instructions and general information about installing and configuring WebLogic Server, see the WebLogic Server documentation.

For more information about installing WebLogic Server, see *Fusion Middleware Installing and Configuring Oracle WebLogic Server and Coherence* at the Oracle Help Center.

Creating the WebLogic Server Domain

To create the WebLogic Server domain for IP Service Activator, create a domain as described in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*, and make the following selections:

1. On the Templates screen, ensure that the **Basic WebLogic Server Domain** template is selected by default. You cannot deselect it.
2. On the Domain Mode and JDK screen, select or browse to the version of the Java Development Kit (JDK) that is supported by IP Service Activator.
3. On the Advanced Configuration screen, do one of the following:

- To create an administration server without any managed servers, select only **Administration Server**.

This configuration is appropriate for most development and test environments. However, because performance testing and staging environments should use the same server configuration as the production environment, a different configuration may be more appropriate.

- To create an administration server with a single managed server select at least **Administration Server, Managed Servers, and Deployments and Services**.

This configuration is appropriate for production environments that are not highly available. Having the administration traffic on the administration server and the application traffic on the managed server ensures that critical administration operations (such as starting and stopping servers, changing a server's configuration, and deploying applications) do not compete with high-volume application traffic on the same network connection.

Configuring the WebLogic Server Domain

The following tasks can be performed either before or after installing IP Service Activator, but Oracle recommends performing them before installing IP Service Activator.

Increasing the Memory Settings for WebLogic Servers

IP Service Activator requires more memory than the amount configured for the WebLogic server by default. For production environments, you must tune the values to meet your specific performance requirements. See the WebLogic Server documentation for more information about increasing the memory settings for non-clustered WebLogic servers on UNIX and Linux.

Preventing Connection Timeout when Using a Remote Database

To prevent a connection time out when your database and server are in separate locations, do the following:

1. Increase the value of the Stuck Thread Max time parameter as follows:
 - a. Log in to the WebLogic Server Administration Console.
 - b. In the **Domain Structure** tree, expand **Environment** and then click **Servers**.
The Summary of Servers page is displayed.
 - c. Click the name of the WebLogic server where you want to deploy the cartridges.
The configuration parameters for the server are displayed on a tabbed page.
 - d. Click the **Tuning** tab, and modify the value of the **Stuck Thread Max Time** parameter to an appropriate value (for example 1800) in seconds.
 - e. Click **Save**.
2. Increase the value of the Timeout Seconds Java Transaction API parameter as follows:
 - a. In the **Domain Structure** tree of the WebLogic Server Administration Console, click the name the WebLogic server domain.
The configuration parameters for the domain are displayed on a tabbed page.
 - b. Click the **JTA** tab, and modify the value of the **Timeout Seconds** parameter to an appropriate value. In most cases, a value of 2400 seconds is sufficient.

 **Note:**

If the value is less than 600 when you run the Installer, you are prompted to increase it during installation.

- c. Click **Save**.

See the WebLogic Server documentation for more information about these parameters.

6

Installing and Configuring Supplemental Software Components

This chapter provides instructions for installing and configuring the supplemental software components required by Oracle Communications IP Service Activator.

Installing Supplemental Software Components

IP Service Activator requires the supplemental software components listed in [Table 6-1](#).

Table 6-1 Supplemental Software Components

| OS | Type | Filename | Download Link |
|----------------|--------|--|---|
| Linux | 64 bit | omniORB-4.2.4-linux-gcc-x86_64.tar.gz | https://sourceforge.net/projects/omniorbipsa/files/omniORB-omniORBpy-IPSA/4.2.4-IPSA-v35/omniORB-4.2.4-linux-gcc-x86_64.tar.gz/download |
| Linux | 64 bit | saxonb8-8-0-7j.zip | http://sourceforge.net/projects/saxon/files/Saxon-B/8.8.0.7/ |
| Oracle Solaris | 64 bit | omniORB-4.2.4-sol64.tar.gz | https://sourceforge.net/projects/omniorbipsa/files/omniORB-omniORBpy-IPSA/4.2.4-IPSA-v35/omniORB-4.2.4-sol64.tar.gz/download |
| Oracle Solaris | 64 bit | saxonb8-8-0-7j.zip | http://sourceforge.net/projects/saxon/files/Saxon-B/8.8.0.7/ |
| Windows | 64 bit | omniORB_424-omniORBpy_424-ipsa-win64.zip | https://sourceforge.net/projects/omniorbipsa/files/omniORB-omniORBpy-IPSA/4.2.4-IPSA-v35/omniORB_424-omniORBpy_424-ipsa-win64.zip/download |

Download the supplemental software components, unzip and untar them to a folder, and use them during installation. For more information, see "[Preparing the Supplemental Software Component Packages](#)".

Preparing the Supplemental Software Component Packages

This procedure describes how to download and prepare the supplemental software components (omniORB, GCC runtime, and Saxon-B) needed by IP Service Activator.

 **Note:**

Create a directory and download the supplemental software components to this directory, for example, **/opt/web/supplementalSoftware**. When you run the Oracle Universal Installer, you will use this directory path. Do not uncompress the files. The Installer uncompresses the files as part of its process.

Download the omniORB distribution. Use the link in table 6-1 to download the correct distribution for the OS on the server where you are installing IP Service Activator or the IP Service Activator client.

On a Solaris 64-bit or Linux server:

1. Download the Saxon-B distribution using the link in the table above.
Note: Download the supplemental software components to the same directory, for example, **/opt/web/supplementalSoftware**. When you run the Installer, you will use this directory path. Do not uncompress the files. The Installer uncompresses the files as part of its process.
2. Ensure the tar, gzip, gunzip, zip, and unzip utilities are installed and in the path for the **ipsaadm** user.
3. Preserve the contents of the directory for other installations.

 **Note:**

During installation, on the **Supplemental Software Location** window, specify the directory created.

On a Windows host:

1. Create a directory for the supplemental software.
2. Transfer the omniORB zip file into this directory.
3. Preserve the contents of the directory for other installations.

 **Note:**

During installation, on the **Supplemental Software Location** window specify the directory created.

CORBA ORB Configuration for IP Service Activator

IP Service Activator requires omniOrb 4.2.4 on Solaris, Linux, and Windows platforms to provide CORBA ORB services.

By default, IP Service Activator uses TCP wrappers for access control for CORBA connections. IP Service Activator processes must be properly named as being allowed to connect to the ORB.

One approach is to ensure that the default configuration files allow the connection of the various IP Service Activator components. The configuration files are:

```
/etc/hosts.allow  
/etc/hosts.deny
```

Another approach is to provide alternative configuration files to the ORB by adding the following lines to the **omniorb.cfg** file of the IP Service Activator Config folder:

```
GATEKEEPER_ALLOWFILE /opt/OracleCommunications/ServiceActivator/Config/hosts.allow  
GATEKEEPER_DENYFILE /opt/OracleCommunications/ServiceActivator/Config/hosts.deny
```

Alternatively, you can use specific component names as the daemon names (for example, **/opt/OracleCommunications/ServiceActivator/bin/policy_server**). A simpler approach to implement this solution is to use a common string such as IPSA as the daemon name, and provide **-ORBserverName IPSA** as a command line option for each of the components by adding the option to the **cman.cfg** file.

The appropriate **hosts.allow** file should be configured to allow the communication to the service (IPSA in the example above).

The use of TCP wrappers might be disabled on the IP Service Activator installation because it is possible to disable TCP wrappers by specifying non-existent configuration files.

7

Installing IP Service Activator

This chapter describes how to install Oracle Communications IP Service Activator components on one or more host machines.



Note:

You must repeat the steps in this chapter, as well as the "Additional setup tasks after startup" in *IP Service Activator System Administrator's Guide*, on each server where IP Service Activator is to be installed, selecting the components and settings for each server.

Installing IP Service Activator on an Oracle Solaris or Linux Server

This section describes how to install IP Service Activator components on a Solaris or Linux server. This installation does *not* include the IP Service Activator client, which must be installed on a Windows platform. For more information, see "[Installing the IP Service Activator Client on Windows](#)".

Preparing to Install IP Service Activator

Before running the Oracle Universal Installer, ensure that you:

- Log in to the server as the **ipsaadm** user. For information, see "[IP Service Activator Administrator UNIX User ID \(ipsaadm\)](#)".
- Install the required supplemental software components, as described in "[Installing Supplemental Software Components](#)".
- Log in to the Oracle software delivery Web site and download the IP Service Activator software. See "[Downloading the IP Service Activator Software](#)" for more information.
 - Download the Linux Oracle Universal Installer if you are installing onto a Linux 64-bit server.
 - Download the Solaris 64-bit Oracle Universal Installer if you are installing onto a Solaris 64-bit server.
- Un-zip the IP Service Activator software on each server where you want to install IP Service Activator. For example, on a Linux server, run the following command to unzip the file:

```
unzip IPServiceActivator-7.x.x.x-x-linux.zip
```
- Synchronize times across all host machines where IP Service Activator components are installed. For example, by using a Network Time Protocol (NTP) server. If device times are not synchronized, delays and problems are likely to occur.

Running the Oracle Universal Installer for IP Service Activator

1. Log in to the server as the **ipsaadm** user.
2. Go to the directory *software un-zip location/ipsa/Disk1/install*.
3. There are two installation methods:
 - Interactive: For an interactive installation, continue with step 4.
 - Silent: For information about silent installations, including recording an installation session for later re-use in a silent installation, see "[About Silent Installations](#)".
4. Create a directory in which to install IP Service Activator, such as **/opt/OracleCommunications**. Ensure the ipsaadm user has read/write/execute access to this directory.
5. Run the following command:

```
./runInstaller
```

The Welcome window opens.

Note:

Make sure that the display settings are correct. If you cannot use X display, you must run a silent installation.

If you have not run an Oracle product that installs with Oracle Universal Installer on the target system, the Specify Inventory Directory and Credentials window opens.

6. Enter the path of the inventory directory **/export/home/oracle/orainventory** when Oracle Universal Installer is run for a new installation on the server. Then enter the UNIX group name. The **orainventory** directory contains the following:
 - oraInstaller.properties
 - logs
 - backup
 - install.platform
 - ContentsXML
 - OUI
7. Click **Next**.

The Select Installation Type window opens.

8. Select the components that you want to install.

You can select any of the following installation types:

- **All Components**: includes all IP Service Activator components. This is for a complete installation.
- **Policy Server**: includes all Policy Server components

- **Cartridges:** includes all Cartridges
- **Web Service:** allows you to use the web service to integrate IP Service Activator with Oracle Communications Order and Service Management (OSM)

For information about configuring the web service installation, see the web services chapters in *IP Service Activator API Developer's Guide*.

- **All Except Web Service:** Includes all IP Service Activator components except web service.
- **Custom:** allows you to select the specific components that you want to install

If you are performing a distributed installation, select the correct components for the host on which you are currently installing. Decisions on which hosts various components are installed on vary depending on the needs of your site. Typically, you might install the Policy Server on one host and the Network Processors on another. For information about distributing components across servers, see "[Planning an IP Service Activator Installation](#)".

The Specify Home Details window opens.

9. Enter the directory path of the base installation and accept the default name, **OracleCommunications**.

OracleCommunications identifies the name of the Oracle home on which Oracle services are installed. Click **Next**.

- If you selected the installation options **All Components** or **Policy Server** in the previous step, the Supplemental Software Location window opens.
- If you selected the installation option **Cartridges** in the previous step, the Available Product Components window appears and you must select the specific cartridges that you want to install, and then click **Next**. The Supplemental Software Location window opens.
- If you selected the installation option **Custom** in the previous step, you must select the specific IP Service Activator components you want to install, and then click **Next**. The Supplemental Software Location window opens.

 **Note:**

The Installer checks for the supplemental software files before proceeding with the installation in step 9.

10. Enter the directory path to the location where you placed the supplemental software components. Click **Next**.

The IP Service Activator Startup window opens.

11. Select whether you want IP Service Activator to start at every reboot. Click **Next**.

The Summary window opens.

 **Note:**

The list of installed products might show apparently duplicate entries, however the entries refer to distinct products.

12. Verify the component installation list, and then click **Install**.

The Installation window opens with a progress bar.

The Execute Configuration scripts window opens.

13. Run the configuration scripts by following the steps given in the installation window. The following message appears when you run the scripts:

"Creating symbolic link in *path* so that IP Service Activator is stopped when the machine is shutdown."

After running the scripts, click **OK**. The **root.sh** script is in the *Oracle_home* directory. By running the **root.sh** script, you ensure that IP Service Activator automatically starts when you run the server.

The **orainstRoot.sh** script is in the following directory, under the **oralnventory** home directory:

inventory_home/orainstRoot.sh

The End of Installation window opens.

14. Click **Exit** to continue or click **Installed Products** to see the components that were installed.

When you click **Exit**, the Configuration Assistants and Execute Configuration scripts dialog boxes open.

15. Click **OK**.

The IP Service Activator post-install scripts run.

16. When prompted to start the Configuration GUI to configure IP Service Activator, click **Yes**.

The Configuration GUI starts.

See *IP Service Activator System Administrator's Guide* for information about using the Configuration GUI.

Continue the configuration of IP Service Activator by performing the tasks detailed in Additional setup tasks to be run prior to initial startup topic in *IP Service Activator System Administrator's Guide*.

If you are performing a distributed installation across multiple servers, repeat this procedure for each host.

The following IP Service Activator modules are installed using the Oracle Universal Installer:

- Common
- Configuration Template Module (CTM)
- Threshold Activated Configuration Control (TACC)

The Common module is automatically installed during the installation.

You must import and link the appropriate controller scripts before running the installed modules. For more information, see information about importing and linking controller scripts in *IP Service Activator System Administrator's Guide*.

About Silent Installations

The Oracle Universal Installer supports silent installations using a response file.

A silent installation does not use the Installer GUI and does not display the interactive dialog boxes that you normally see. Instead, installation options are specified in a response file.

 **Note:**

You can record installation details into a response file for use in a future silent installation by running the **runInstaller -record -destinationFile *Path*** command.

Complete details on silent installations, the contents of response files, and customizing and creating new response files are available in Oracle Universal Installer documentation.

To view Oracle Universal Installer documentation on Windows machines on which the IP Service Activator client has been installed:

1. Click **Start** and then select **Programs**.
2. Select **Oracle - Oracle_home**, and then select **Oracle Installation Products**, where *Oracle_home* is the name of the Oracle home on which Oracle services are installed.
3. Select **Universal Installer Concepts Guide**.

Alternatively, you can access Oracle Universal Installer documentation here:

HTML:

http://download.oracle.com/docs/cd/B28359_01/em.111/b31207/toc.htm

PDF:

http://download.oracle.com/docs/cd/B28359_01/em.111/b31207.pdf

 **Note:**

There are some IP Service Activator-specific response parameters that are not mentioned in the Oracle Universal Installer documentation.

IP Service Activator- specific response parameters for Solaris/Linux are as follows:

- **SUPP_SOFTWARE_DIR**: the directory where the supplemental software components are located.
- **AUTOMATIC_STARTUP_REQUIRED**: specifies whether IP Service Activator should be started automatically on reboot.

IP Service Activator- specific response parameter for Windows is as follows:

- **SUPP_SOFTWARE_DIR**: the directory where the supplemental software components are located.

Running a Silent Installation

To run a silent installation:

1. For a **Solaris/Linux** installation, locate the response template file in *software unzip location/ipsa/Disk1/stage/Response* in the IP Service Activator software for the type of installation you require.

The Response folder contains the following response template files for the corresponding installation types:

oracle.communications.ipsa.AllExceptWebService.rsp - All Components except Web Service

oracle.communications.ipsa.AllComponents.rsp - All Components

oracle.communications.ipsa.Cartridges.rsp - Cartridges

oracle.communications.ipsa.Custom.rsp - Custom

oracle.communications.ipsa.PolicyServer.rsp - Policy Server

oracle.communications.ipsa.WebService.rsp - Web Service

For a Custom installation type, open the

oracle.communications.ipsa.Custom.rsp file and remove the components that you do not want to install from the DEPENDENCY_LIST parameters. [Table 7-1](#) maps the internal component names in the DEPENDENCY_LIST parameters with the names in the Oracle Universal Installer.

Table 7-1 DEPENDENCY_LIST Parameter Components For Silent Installation

| Internal component name | Name in the Installer |
|---|-------------------------------|
| oracle.communications.ipsa.policyserver | Policy Server |
| oracle.communications.ipsa.cartridges | Cartridges |
| oracle.communications.ipsa.networkprocessor | Network Processor Framework |
| oracle.communications.ipsa.webservice | Web Service |
| oracle.communications.ipsa.oss | OSS Integration |
| oracle.communications.ipsa.ctm | Configuration Template Module |
| oracle.communications.ipsa.tools | Tools |
| oracle.communications.ipsa.tools.configtool | Configuration GUI |
| oracle.communications.ipsa.tools.dbupgrade | DB Upgrade |
| oracle.communications.ipsa.tools.yangimporter | YANG Importer |
| oracle.communications.ipsa.tools.servicediscovery | Service Discovery |
| oracle.communications.ipsa.cartridges.cisco.catos | Cisco CatOS Cartridge |
| oracle.communications.ipsa.cartridges.cisco.ios | Cisco IOS Cartridge |
| oracle.communications.ipsa.cartridges.cisco.iosxr | Cisco IOS Cartridge XR |
| oracle.communications.ipsa.cartridges.huawei.vrp | Huawei VRP Cartridge |

Table 7-1 (Cont.) DEPENDENCY_LIST Parameter Components For Silent Installation

| Internal component name | Name in the Installer |
|---|---------------------------|
| oracle.communications.ipsa.cartridges.juniper.junos | Juniper JUNOS Cartridge |
| oracle.communications.ipsa.cartridges.generic | Generic Cartridge |
| oracle.communications.ipsa.cartridges.netconf | Netconf Generic Cartridge |
| oracle.communications.ipsa.oss.oim | OSS Integration Manager |

 **Note:**

If you do not remove any of the components from the DEPENDENCY_LIST, the Custom installation type is equivalent to AllComponents installation type.

- (Optional) Open the response template file and modify the following installation parameters:

ORACLE_HOME

ORACLE_HOME_NAME

SUPP_SOFTWARE_DIR

AUTOMATIC_STARTUP_REQUIRED

- Log in to the server as the **admin** user.
- Go to the directory **ipsa/Disk1/install** and run the Oracle Universal Installer as follows:

```
./runInstaller -silent -responseFile full path to response template file,including file name
```

- After the installation is complete, check the log files, and start the Configuration GUI.
See *IP Service Activator System Administrator's Guide* for information about using the Configuration GUI.

Installing the IP Service Activator Client on Windows

This section explains how to install the IP Service Activator client on a 64-bit Windows 10 host, or a 64-bit Windows XP Professional host. You can install the client on multiple hosts distributed throughout the network. You can install the client on terminal services hosts and Oracle VM host machines. The installation process installs the client as well as online Help.

Before Running IP Service Activator Client Installer

- Install the Policy Server on your Solaris or Linux server(s)
- Obtain the required supplemental software components for the client, as described in ["Installing Supplemental Software Components"](#).
- Log in to the Oracle software delivery website and download the IP Service Activator Windows client-only installer software. See ["Downloading the IP Service Activator Software"](#) for more information.

- Un-zip the IP Service Activator Windows software on each Windows host where you want to install the IP Service Activator client to a folder such as **IPSAInstaller_7.x.x.x.x**, which will be referred to as *software un-zip location* in this procedure.
- Configure the Windows host to prefer IPv4 over IPv6 addresses. See "[Configuring the 64-bit Windows Host to Prefer IPv4 Over IPv6 Addresses](#)" for more information.
- Synchronize times across all host machines where IP Service Activator components are installed, for example, by using a Network Time Protocol (NTP) server. If device times are not synchronized, delays and problems are likely to occur. See "[Synchronizing IP Service Activator Host Machines](#)".

Configuring the 64-bit Windows Host to Prefer IPv4 Over IPv6 Addresses

You install the IP Service Activator client on a 64-bit Windows host. The IP Service Activator client communicates with the Policy Server using CORBA through the Naming Service.

This section provides the steps to configure the Windows 64-bit host to prefer and use IPv4 addresses when both IPv4 and IPv6 addresses are available on the host and the IP Service Activator server is configured using IPv4 address.

To configure the Windows host to prefer IPv4 over IPv6 addresses, do one of the following:

- Add two end points with the same port number to the Configuration GUI. Add the first endpoint with the DNS name and the second endpoint with the IPv4 address, but both the endpoints should use the same port number.
- Add the endpoints using the `-ORBEndPoint` command line parameter, as follows:

```
-ORBEndPoint giop:tcp:dns:port -ORBEndPoint giop:tcp:ipv4address:port
```

where *dns* is the DNS name, *port* is the port number, and *ipv4address* is the IPv4 address of the Windows host.

The second endpoint (*ipv4_address:port*) forces the Configuration GUI to listen on the IPv4 port so that the Policy Server can call back.

For example:

```
-ORBEndPoint giop:tcp:ipsahostdnsname@example.com:2909 -ORBEndPoint  
giop:tcp:10.44.32.4:3906
```

Note:

Do not use the IPv4 loopback IP address as the IP Service Activator server address.

Installing the Client

Before you run the Configuration GUI, make sure all file permissions are set correctly. For more information, see "[Setting Permissions for the Installation UNIX User ID](#)".

1. On the Windows host, go to the directory *software un-zip location\client\Disk1\install*.
2. There are two installation methods:
 - Interactive: continue with step 3.
 - Silent: For information about silent installation, see "[To run a silent installation:](#)".
3. Double-click **setup.exe**.

If you are installing on a Windows 10 host and see an error regarding swap space/virtual memory, see "[Oracle Universal Installer Error](#)" for a resolution.

The Welcome window opens.

4. Click **Next**.

The Select Installation Type window opens.

5. Select the components you want to install.

You can select from the following installation types:

- All Client Components: includes the main IP Service Activator client, the client extensions, and the Configuration GUI
- Custom: allows you to select the specific components you want to install

Click **Next**.

The Specify Home Details window opens.

6. Enter the directory path of the base installation and accept the default name, Oracle Communications. Click **Next**.

If you selected the installation option All Client Components in step 5, the Supplemental Software Location window opens.

If you selected the installation option Custom in step 5, the Available Product Components window appears. Select the specific components you wish to install, then click **Next**. The Supplemental Software Components window opens.

7. Enter the directory path to the location where you placed the supplemental software components. Click **Next**.

The Summary window opens.

8. Verify the component installation list, and then click **Install**.

The Installation window opens with a progress bar.

When the Installer is finished running, the End of Installation window opens.

9. Click **Exit** if you want to start the configuration GUI and configure the installation, or click **Installed Products** to see the components that were installed.

10. When prompted to start the Configuration GUI to configure IP Service Activator, click **Yes**.

The Configuration GUI starts.

See *IP Service Activator System Administrator's Guide* for information about using the Configuration GUI.

The following IP Service Activator modules are installed using the Oracle Universal Installer:

- Common
- Configuration Management

- CTM GUI Extension
- TACC

The Common module is automatically installed during the installation.

11. If you installed the IP Service Activator client on a Windows 10 host, navigate to the folder in which the IP Service Activator client is installed, such as **C:\Program Files\OracleCommunications**. Right-click **OracleCommunications**. Click the **Security** tab and give full read and write permissions to users who will use IP Service Activator.

Running IP Service Activator Client Installer in Silent Mode

To run the client installer in silent mode:

1. For a **Windows** installation, locate the response template file in **client\Disk1\stage\Response** in the IP Service Activator Windows software.

The client is supported only on Windows.

The Response folder contains the following response template files for the corresponding installation types:

- **oracle.communications.ipsa.AllClientComponents.rsp**: All Client Components
- **oracle.communications.ipsa.Custom.rsp**: Custom

In a Custom installation type, open the **oracle.communications.ipsa.Custom.rsp** file and remove the entries that you do not want to install from the **DEPENDENCY_LIST** parameters. [Table 7-2](#) maps the internal component names in the **DEPENDENCY_LIST** parameters with the names in the Oracle Universal Installer.

Table 7-2 DEPENDENCY_LIST Parameter Components For Client Installer

| Internal component name | Name in the Installer |
|---|---|
| oracle.communications.ipsa.client | Windows GUI Client |
| oracle.communications.ipsa.servicemodules | Service Module GUI Extensions |
| oracle.communications.ipsa.oss | OSS Integration GUI Extensions |
| oracle.communications.ipsa.ctm | Configuration Template Module GUI Extension |
| oracle.communications.ipsa.configmgmt | Configuration Management Module GUI Extension |
| oracle.communications.ipsa.tools | Tools |
| oracle.communications.ipsa.tools.configtool | Configuration GUI |
| oracle.communications.ipsa.tools.tacc | Threshold Activated Configuration Control GUI Extension |

 **Note:**

If you do not remove any of the components from the `DEPENDENCY_LIST`, the Custom installation type is equivalent to `AllClientComponents` installation type.

- (Optional) Open the response template file and modify the following installation parameters:

- ORACLE_HOME
- ORACLE_HOME_NAME
- SUPP_SOFTWARE_DIR

If you are installing on Windows 10, navigate to the directory `software un-zip location\client\Disk1\install`, right-click on **setup.exe**, and select **Properties**. In the Properties dialog box, click the **Compatibility** tab and select **Run this program in compatibility mode for Windows XP Service Pack 3**. Click **OK**.

- Go to the directory `client\Disk1\install` and run the Oracle Universal Installer as follows:

```
setup.exe -silent -responseFile file name
```

where *filename* is the full path to response template file, including the file name.

- After the installation is complete, check the log files, and start the Configuration GUI.
See "Using the Configuration GUI" in *IP Service Activator System Administrator's Guide* for information about using the Configuration GUI.
- If you installed the IP Service Activator client on a Windows 10 host, navigate to the folder in which the IP Service Activator client is installed, such as **C:\Program Files\Oracle\Communications**. Right-click **OracleCommunications** and, on the **Security** tab, give full read and write permissions to users who will use IP Service Activator.
- If you installed the IP Service Activator client on a Windows 10 host, navigate to the Program folder of IP Service Activator, such as **C:\Program Files\Oracle\Communications\Service Activator\Program**, right-click **ipsa_explorer.exe**, and select **Properties**.
The Properties dialog box opens.
- Click the **Compatibility** tab and select **Run as Administrator**.

Oracle Database Connection Considerations for the IP Service Activator Client

When you run the Solaris/Linux-based Installer for IP Service Activator server software, the Oracle Instant Client is automatically installed and a **tnsnames.ora** file is configured to provide connectivity to the Oracle Database. However, the Windows-based Installer for the IP Service Activator client does not include the Oracle Instant Client.

The IP Service Activator client communicates with the Policy Server using CORBA, through the Naming Service. In general, the Oracle Instant Client is not required for the IP Service Activator client, unless you want to be able to access logs from the client.

Oracle Database Client Requirements to View Logs in the IP Service Activator Client

Logs are stored directly in the Oracle Database. To view audit trail, device configuration, or system message logs in the IP Service Activator client, you must install and configure an Oracle client (such as the Oracle Instant Client) and configure an ODBC Data Source for IP Service Activator on the client host.

For Oracle Client configuration details, see "[Manually Configuring Oracle Client Connection: Solaris](#)".

Setting Up an FTP or a TFTP Server

If you want to use the restore functionality of the Configuration Management module, you must set up a valid FTP or TFTP server to which the Configuration Management module can connect to. See the Solaris or Linux documentation for more information about setting up an FTP or a TFTP server on a Solaris or Linux server.

Setting Up the Syslog Server

If you want to use the functionality of the Configuration Management module, you must set up the syslog server, which is used for tracking changes. See the Solaris and Linux documentation for information about setting up the syslog server on a Solaris or Linux server.

Pre-Installation of the Configuration Template Module

Perform the following tasks before you install the Configuration Template Module (CTM):

- Ensure the Oracle XML Database is installed before installing CTM. For more information, see "[Verifying that Oracle XML Database is Installed](#)".
- Install the CTM Request Server on the same server as the Naming Service, to avoid any reconfiguration.
- Configure the OSS Integration Manager (OIM) timeout parameter, so that OIM does not close inactive sessions. For more information, see "[Configuring OIM to Keep Inactive Sessions Running](#)".

For more information about how to use CTM, see the discussion about Configuration Template Module in IP Service Activator online Help.

Verifying that Oracle XML Database is Installed

CTM uses Oracle Database features for XML document handling, and PL/SQL stored procedures for optimizations.

You must ensure the Oracle XML Database is installed prior to installing the Configuration Template module.

Oracle XML Database is usually installed by default with Oracle Database software. For more information about installing Oracle Database, see "[Installing and Configuring Oracle Database Software](#)".

If Oracle XML Database is not installed, see the Oracle Database product documentation for more information.

To verify if the Oracle XML Database is installed, run the following command as user **SYSDBA**:

```
select username from dba_users where username like 'X%';
```

If the XML Database is installed, the response is **XDB**. If no value is returned, it means that the XML Database is not installed.

Configuring OIM to Keep Inactive Sessions Running

CTM connects to OIM for flow-through provisioning.

By default, OIM has a timeout parameter that is configured to close your session after a period of inactivity. Set the OIM timeout value to 0 to keep inactive sessions from timing out.

To configure OIM to keep inactive sessions running:

1. Open the **cman.cfg** configuration file from the directory **/opt/OracleCommunications/ServiceActivator/Config**.

2. Add the following parameter to the OIM line:

```
-timeout 0
```

3. Close the **cman.cfg** configuration file.

Restoring Configuration When the Device Model Contains Configlets

When performing a device restoration operation, if the device model contains one or more configlets that were created and persisted through IP Service Activator, the commands are re-sent to the device even though the restored configuration has the configlets as part of the device model.

To restore a device configuration:

1. Log in to IP Service Activator and display the domain containing the discovered device.
2. Create an archive for the device.
3. Under **Archive List**, select the row of the newly created archive, and from the **Actions** list, select **View**.

The Archive View page appears.

4. Click **View Current Config**.

The Configuration Editor page appears.

5. Create a configlet and activate it.
6. Click **Archive** to create an archive.
7. Navigate to the **Configuration Archives** page.

8. Select the check box for the archive you just created.
9. Click **Restore**, and select **Complete Restore**.
The device is restored and restarted, and it is left in Offline Test mode.
10. Right-click a device, select **Command Delivery**, and then select **Online Mode**.
The configlet is pushed to the device.

Typically, when you restore the configuration to the device, no configuration commands are sent to the device. This is the only exception.

For complete details, see IP Service Activator online Help.

8

IP Service Activator Post-installation Tasks

This chapter describes the post-installation tasks for Oracle Communications IP Service Activator.

IP Service Activator Post-installation Tasks

There are a number of tasks to do after IP Service Activator is installed, but before you create domains, and discover and manage your network devices.

These tasks include:

- running the Configuration GUI to configure various system parameters
- starting the system
- configuring Super User accounts
- checking router configurations
- loading configuration policies
- importing and linking controller scripts
- setting up logging
- enabling Layer 2 Martini support on the Cisco IOS cartridge if you intend to configure Layer 2 Martini VPNs

Note:

The next tasks you should perform are described in the topic about additional setup tasks after startup in *IP Service Activator System Administrator's Guide*. These tasks are required in order to be able to use IP Service Activator.

Tasks include changing the default user group, and default super user when you first log in. After the default user is changed, all users must enter a name and password each time they start the IP Service Activator client. This is described in the topic about changing the default user in *IP Service Activator System Administrator's Guide*.

Configuring Web Services

If you want to use the optional web services component with IP Service Activator, see the chapter about web services in *IP Service Activator API Developer's Guide*.

9

Upgrading and Patching IP Service Activator

This chapter describes how to upgrade an existing system to the latest Oracle Communications IP Service Activator release. This chapter also includes procedures for performing IP Server Activator patch updates.

About Upgrading IP Service Activator

The upgrade procedure should be performed by qualified IP Service Activator administrators. You should be familiar with Oracle Database; IP Service Activator components; IP Service Activator client; IP Service Activator system configuration, including Network Processors, capabilities files, and options files; and details of any customizations to the IP Service Activator configuration.

 **Note:**

Carefully review the procedures and topics in this chapter before performing the upgrade procedures. Ensure that the prerequisites are met and that during the procedure you perform all backup steps.

In this chapter, the release you are upgrading from is called the *old* release and the release you are upgrading to is called the *new* release.

Supported Upgrade Paths

This release of IP Service Activator supports the upgrade path from release 7.4.0 (or later) to release 7.5.0.

 **Note:**

To upgrade IP Service Activator from 7.4.0 (or later) to 7.5.0, follow these steps:

1. Stop the IP Service Activator 7.4.0 components.
2. Uninstall IP Service Activator 7.4.0 (or later).
3. Install IP Service Activator 7.5.0 in the same directory where 7.4.0 was installed.
4. Update the Network Processor version in the database to 7.5.0 using npAdmin.sh tool.
5. Restart your system.

About the Upgrade Process

The flow charts in [Figure 9-1](#) and [Figure 9-2](#) illustrate the upgrade process.

Figure 9-1 IP Service Activator Upgrade Process: Stage 1

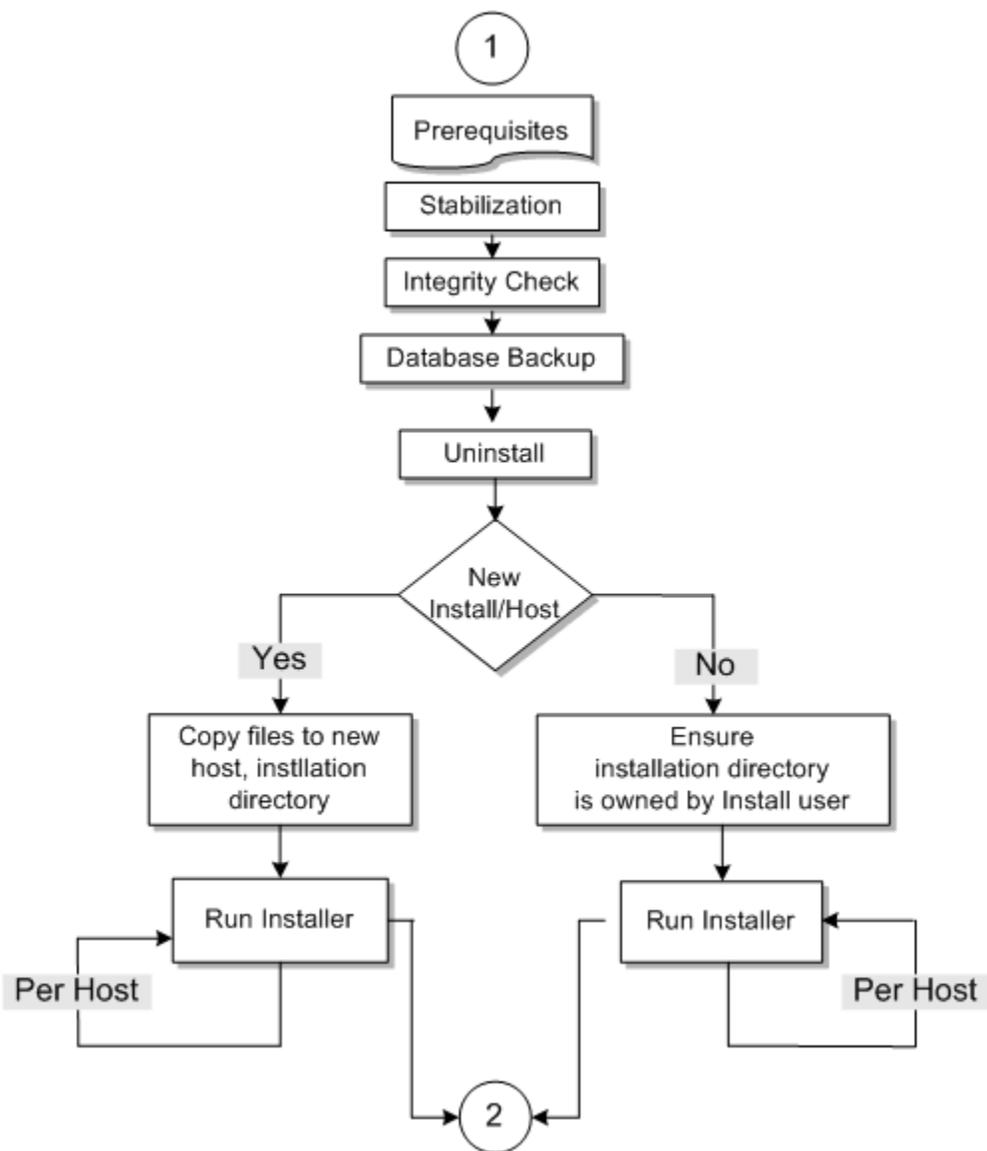
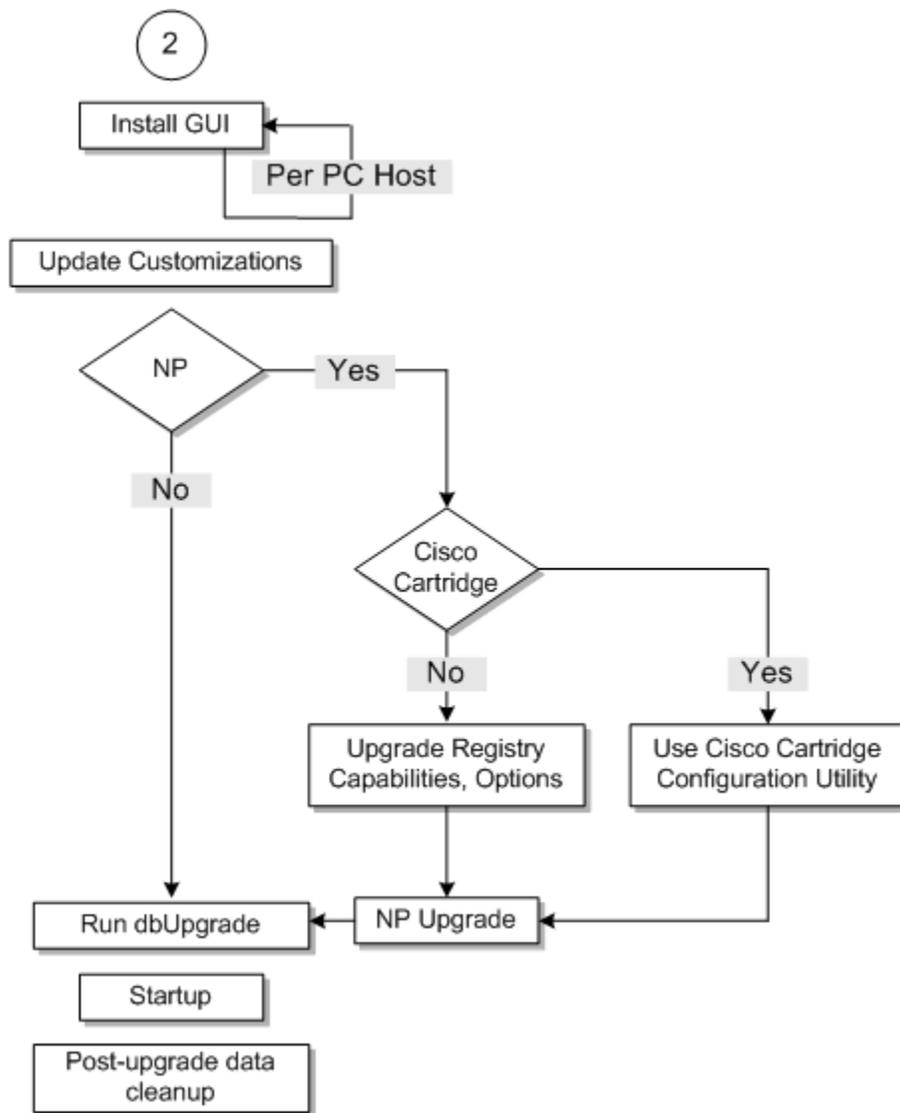


Figure 9-2 IP Service Activator Upgrade Process: Stage 2



About Network Processor Upgrade Tool Script - npUpgrade

npUpgrade performs the following tasks after the new version of IP Service Activator is installed:

- Sets up the database schema or modifies it if one exists
- Transitions all the network processor device data to the new database schema
- Computes the commands generated by the new network processor for each device

The following files are created by the Network Processor Upgrade tool:

- *Service_Activator_home/logs/upgradetool*.log*
- *upgrade_home/upgrade/reports/upgradeReport.txt*
- *upgrade_home/upgrade/success/DeviceAudit_componentId.xml*

- `upgrade_home/upgrade/failure/DeviceAudit_componentId.xml`

where:

- `Service_Activator_home` is the IP Service Activator home directory (typically: `/opt/OracleCommunications/ServiceActivator`)
- `upgrade_home` is a configurable location anywhere on the server (the default value is `Service_Activator_home/upgrade_home`)

Preparing for the IP Service Activator Upgrade

This section provides information about preparing to upgrade IP Service Activator from release 7.4.0 (or later) to release 7.5.0.

Prerequisites

Before upgrading IP Service Activator:

- Ensure that you have the Installer for your old IP Service Activator release, in case you need to roll back the upgrade and revert to your original system.
- Ensure that you have the supplemental software components for your old IP Service Activator release.
- Ensure that the hardware meets the requirements for the new release. See "[Planning an IP Service Activator Installation](#)" for details.
- Go to My Oracle Support to check for the latest patch set for your new release. Otherwise, go to the Oracle software delivery website and download the IP Service Activator software for the platforms that you require. See "[Downloading the IP Service Activator Software](#)" for more information.
- Download the supplemental software components for your new release.
- If you are upgrading on a Linux server, make sure you have installed the Linux **libaio** package files for your Linux version.
- Unzip the IP Service Activator software on each server where you plan to install IP Service Activator.

It is recommended that your IP Service Activator installation be operating as normally as possible before you upgrade. Issues that you do not resolve prior to the upgrade will still exist in the upgraded system. It is recommended that you take the following actions:

- Correct cartridge-managed devices that have any failed configuration (that is, they are in the **Intervention Required** state).
- Correct cartridge-managed devices that have outstanding or pending configuration.
- Minimize critical faults.

Terminology

[Table 9-1](#) maps the terms used in this section with their corresponding default values for different versions of IP Service Activator.

Table 9-1 Term Default Values

| Terminology | Default values for new versions 5.2.4 and later | Default values for new versions 7.0.0 and later |
|--------------------------------|---|---|
| IPSA_admin_unix_account | ipsaadm | ipsaadm |
| default_installation_directory | /opt/OracleCommunications/ServiceActivator | /opt/OracleCommunications/ServiceActivator |
| database_SID | IPSA | IPSA.WORLD |
| database_user_id | - | admin |
| database_password | - | admin |
| process_status_script | ipsaps | ipsaps |
| naming_service_script | ipsans | ipsans |
| component_manager_script | ipsacm | ipsacm |
| DSN_Name | IPServiceActivatorDb | IPServiceActivatorDb |

Preparing to Upgrade

Perform the general steps in this section on the old release prior to upgrading. For more specific information about some of these steps, see the relevant sections in this chapter as described in the following procedure.

To prepare to upgrade to the latest release:

1. Ensure that your old version of IP Service Activator is running.
2. Log in to IP Service Activator client using a Super User ID.
3. Ensure outstanding and scheduled transactions are completed.
4. Attempt to resolve all faults prior to upgrade.
5. Decide whether to delete or save committed IP Service Activator transactions.

Deleting committed transactions prior to upgrading speeds up IP Service Activator startup time. Saving truncated versions of committed transactions increases IP Service Activator startup time but maintains database records for business purposes. Truncation removes the operations associated with the committed transactions. To delete all committed transactions:

- a. Set the transaction archive limit to zero. See the section about setting the archive limit for transactions in *IP Service Activator System Administrator's Guide*.
- b. Export all transactions. See the section about exporting transactions in *IP Service Activator User's Guide*.
- c. Commit the transaction. See the section about committing transactions in *IP Service Activator User's Guide*.

To save committed transactions:

- a. You can save truncated versions of committed transactions during the upgrade process when you upgrade the database. See "[Running dbUpgrade to Upgrade the Database](#)" for more information.
6. Shut down the IP Service Activator processes. See *IP Service Activator System Administrator's Guide* for more information.

7. Run the Integrity Checker from the old IP Service Activator system.
For the Integrity Checker procedure and parameter details, see the Database Integrity Checker topic in *IP Service Activator System Administrator's Guide*.
8. Review Integrity Checker output files and correct errors.
If you correct errors, you might have to restart the system to implement the corrections. If you restart the system, return to the first step in this section.
9. Back up your IP Service Activator database instance.
10. Save the database back-up in a directory so that it is available for later restoration if a roll-back of the upgrade is required.
11. Back up custom cartridges, if installed. For more information, see "[Backing Up Custom Configuration Policies and Cartridges](#)".
12. Back up IP Service Activator. For more information, see "[Backing Up IP Service Activator](#)".
13. Uninstall the old IP Service Activator release using the documentation that corresponds to that release.

Backing Up Custom Configuration Policies and Cartridges

To back up custom configuration policies and cartridges:

1. Copy custom service cartridges from the following path:
`Service_Activator_home/lib/java-lib/cartridges/type/ServiceCartridges/`
to a backup location. Where *type* is the cartridge type, for example, Cisco. See *IP Service Activator SDK Service Cartridge Developer Guide* for more information.

 **Note:**

Only back up custom service cartridges.

2. Copy custom base cartridges from the following path:
`Service_Activator_home/lib/java-lib/cartridges/type`
to a backup location. Where *type* is the cartridge type, for example, Cisco. See *IP Service Activator SDK Service Cartridge Developer Guide* for more information.

 **Note:**

Only back up custom base cartridges.

3. Copy custom cartridge configuration policies from the following path:
`Service_Activator_home/lib/java-lib/configurationPolicies`
to a backup location.

 **Note:**

Only back up custom configuration policies.

Backing Up IP Service Activator

Back up the *Service_Activator_home* directory and all its contents.

 **Note:**

The system must be shut down before you back up, in case of an upgrade failure.

Files from these backups are needed to complete some of the upgrade steps and to reverse the upgrade in case of an upgrade failure.

[Table 9-2](#) identifies some of the important backed up files from Network Processor hosts.

Table 9-2 Important Backed Up Files From Network Processor Hosts

| Files from Network Processor hosts | Location on the Network Processor host |
|--|---|
| networkprocessor | <i>Service_Activator_home/bin/</i> |
| MIPSA_registry.xml | <i>Service_Activator_home/Config/networkProcessor/</i> |
| Capabilities files (for example: cisco12K_10K.xml) | <i>Service_Activator_home/Config/networkProcessor/com/ metasolv/serviceactivator/cartridges/vendor/capabilities/XMLfile</i> |
| Options files | <i>Service_Activator_home/Config/networkProcessor/com/ metasolv/serviceactivator/cartridges/vendor/option_file</i> |
| Pre-check files | <i>Service_Activator_home/Config/networkProcessor/com/ metasolv/serviceactivator/cartridges/vendor/pre_check/pre-check_file</i> |
| AutoDiscovery.cfg | <i>Service_Activator_home/Config/</i> |
| cman.cfg | <i>Service_Activator_home/Config/</i> |
| logging.properties default.properties ErrorMessages.xml SuccessMessages.xml | <i>Service_Activator_home/Config/networkProcessor/com/ metasolv/serviceactivator/networkprocessor</i> |

[Table 9-3](#) identifies some of the important backed up files from Policy Server hosts.

Table 9-3 Important Backed Up Files From Policy Server Hosts

| Files from Policy Server hosts | Location on the host |
|--------------------------------|--------------------------------------|
| policy_server.cfg | <i>Service_Activator_home/Config</i> |

Table 9-3 (Cont.) Important Backed Up Files From Policy Server Hosts

| Files from Policy Server hosts | Location on the host |
|--------------------------------|---------------------------------------|
| system_limits.cfg | <i>Service_Activator_home/Config</i> |
| AutoDiscovery.cfg | <i>Service_Activator_home/Config</i> |
| cman.cfg | <i>Service_Activator_home/Config</i> |
| config directory | <i>Service_Activator_home/modules</i> |

Upgrading to the New IP Service Activator Software

If you are installing in the same location as the previous installation, follow these general steps. For more specific information, see the relevant sections.



Note:

Your system is still shut down when you proceed with upgrading steps.



Note:

This section is to upgrade IP Service Activator when the old and new releases are in the same location. If you want to upgrade IP Service Activator where the new release is in a different location, see "[Upgrading IP Service Activator to a New Location](#)".

To upgrade IP Service Activator to the latest release:

1. Run the Integrity Checker from the old IP Service Activator system.
For the Integrity Checker procedure and parameter details, see the Database Integrity Checker topic in IP Service Activator System Administrator's Guide.
2. Review Integrity Checker output files and correct errors.
If you correct errors, you might have to restart the system to implement the corrections. If you restart the system, return to the first step in this section.
3. Patch the new release of IP Service Activator (and all necessary components) using the Oracle Universal Installer. The patching is documented in "[Patching IP Service Activator](#)".



Note:

Because you are installing in the same location, the *Service_Activator_home/config* directory; *Service_Activator_home/modules/config* directories; and *Service_Activator_home/upgrade_home* directory are preserved from the previous installation.

4. At the end of the patching procedure, you will be asked if you want to run the Configuration GUI. The Configuration GUI is used during the upgrade procedure to configure many system options. However, you should be aware that additional customizations may be needed for some of the files that the tool manages, and also for files that the Configuration GUI does not affect.

Run the Configuration GUI, setting parameters as described in "[Updating Customizations](#)".

For more information about the Configuration GUI, see *IP Service Activator System Administrator's Guide*.

5. Stop the following Configuration Management tools, which are running as UNIX processes:
 - syslog daemon
 - TFTP server
 - FTP server
6. Update the Network Processor version in the database using the npAdmin.sh tool. See "[Running npAdmin to Update Network Processor Internal Data](#)".
7. Restart your system.

Updating Customizations

Manually run the Configuration GUI and configure your system:

`Service_Activator_home/bin/configGUI.sh`.

Ensure that the npUpgrade tool parameters are set:

- Set the **processes** value to the number of processor cores on the server.
- Set the **memory** amount (which is expressed in MB) to **2048MB** (that is, 2GB).
- Set the **Network Processor Model Source** to indicate where the network processor data was stored in the old IP Service Activator software.
- Ensure that the **database login parameters** are set.

To update customizations:

1. Using the backed up `Service_Activator_home/Config` and `Service_Activator_home/modules/Config` directories, merge your old configuration files, such as `cman.cfg`, and so on, into the new files.

This ensures that you preserve any customized old configuration within the new configuration or settings.

2. After running the Configuration GUI as part of the upgrade process, you must propagate any system configuration file customizations that are not managed by the Configuration GUI (if any) by manually editing the new versions of the files.

See "[Network Processor Upgrade Directory Structure](#)" for more information.

 **Note:**

Capabilities files, options files, and the cartridge registry are covered in a later step.

As well, you need to produce a new, merged version of the `Service_Activator_home/Config/AutoDiscovery.cfg` file. In the new file:

- New entries that were added to the new file must remain in the new, merged file
 - Added and changed entries that were in the old file must be propagated to the new, merged file.
 - Entries commented out from the old file must also be commented out in the new, merged file.
3. Produce new, merged versions of other system configuration files. Compare the backed up version of the following files against the new installed versions. For each file, identify any custom changes that you need to carry forward (that you need to merge into the 7.4.0 version of the file). You can refer to the backed up versions of the files you created in "[Backing Up IP Service Activator](#)".

Files included in this process for network processor installations only:

- Capabilities files. Once updated, copy these files to the following directory:
`Service_Activator_home/Config/networkProcessor/com/metasolv/serviceactivator/cartridges/vendor/capabilities/XMLfile`
See "[Updating Capabilities](#)" for more information on upgrading capabilities files.
- Any other files configuration files including those that were extracted from the cartridge .jar files and customized including:
 - **logging.properties**
 - **default.properties**
 - **ErrorMessages.xml**
 - **SuccessMessages.xml**

 **Note:**

If your IP Service Activator old installation does not use the network processor, run the dbUpgrade script. For information, see "[Running dbUpgrade to Upgrade the Database](#)".

Updating Cartridge Registry (MIPSA_registry.xml)

To update the MIPSAs registry:

1. Inspect the backed up version of the custom **MIPSA_registry.xml** file (from the `Service_Activator_home/Config/NetworkProcessor` directory) for custom entries.

2. If you have the Cisco IOS Cartridge, use the Cisco Cartridge Configuration Utility to generate an initial **MIPSA_registry.xml** file. For more information, see *IP Service Activator Cisco IOS Cartridge Guide*.
3. Create a copy of this file and edit the copy to create the new version of the **MIPSA_registry.xml** file that is compatible with the new IP Service Activator version. (See *IP Service Activator System Administrator's Guide* for details on creating or editing a cartridge registry file.) Following is an example for regex used in **MIPSA_registry.xml**:

```
<osVersion useRegex="true">(12.2.*\)T.*|12.2.*\)ZH.*|12.2.*\)B</osVersion>
```

4. Update the retained custom entries so that each entry properly points to the intended Cartridge Unit directory. You can see the new version of the cartridge unit structure in the sample **MIPSA_registry.xml** file in:

Service_Activator_home/samples/vendorSampleRegistry.

Updating Capabilities

After the **MIPSA_registry.xml** file is updated, copy the capabilities files to the locations as specified in the **MIPSA_registry.xml** file. The default location for capabilities files is *Service_Activator_home/Config/networkProcessor*.

Note:

If you are using IPv6 functionality, see *IP Service Activator Installation Guide* for release 5.2.4 for more information about consolidating capabilities.

You need to produce a new, merged version of the capabilities files. In the new files:

- New entries that were added to the new files must remain in the new, merged files.
- Added and changed entries that were in the old files must be propagated to the new, merged files.
- Entries commented out from the old files must also be commented out in the new, merged files.

Some capabilities are now unused and will cause a validation failure of the *capabilities.xsd* file (at the device level). In order to avoid this, compare the capabilities in your old files with the capabilities in the *capabilities.vsd* file and remove any capabilities that are not in the *capabilities.xsd* file.

The following are examples of now unused capabilities:

```
- <caps:supports_gre_vpns>
- <caps:ike_support>
  - <caps:ike_algorithms_supported>
  - <caps:dh_groups_supported>
  - <caps:supports_shared_keys>
- <caps:ipsec_support>
  - <caps:esp_algorithms_supported>
  - <caps:ah_algorithms_supported>
  - <caps:compression_algorithms_supported>
  - <caps:ipsec_modes_supported>
- <caps:ca_support>
  - <caps:supports_ca>
  - <caps:supports_ca_trusted_roots>
```

The error raised if capabilities files contain the above lines is similar to the example below:

```
20081119-165638|255|WARN|[main] (RegistryResourceLoader.java:42) - Resource
failed validation should be valid: /opt2/OracleCommunications/ServiceActivator/
Config/networkProcessor/cisco_12K_10K.xml:0: error: cvc-complex-type.2.4a:
Expected elements 'saa_support@http://www.metasolv.com/serviceactivator/
capabilities lasserre_support@http://www.metasolv.com/serviceactivator/
capabilities vlan_support@http://www.metasolv.com/serviceactivator/capabilities'
instead of 'supports_gre_vpns@http://www.metasolv.com/serviceactivator/
capabilities' here in element device@http://www.metasolv.com/serviceactivator/
capabilities
. . .
20081119-165638|257|WARN|[main] (CartridgeLoader.java:1395) - Registration
failure, registration entry: (resource=file:/opt2/OracleCommunications/
ServiceActivator/Config/networkProcessor/MIPSA_registry.xml
resourceName=com.metasolv.serviceactivator.cartridges.cisco.units.cu1.10008.12.0
line:-1). Unable to load file "cisco_12K_10K.xml"
```

Cisco Cartridge Configuration Utility

If you are deploying the Cisco IOS Cartridge, you must generate the required options files. For more information, see the Cisco Cartridge Configuration Utility procedures in *IP Service Activator Cisco IOS Cartridge Guide*.

1. Edit the options entries in your custom file to point to the applicable customized options file for each device.
2. Save the changes.

An example options entry (in bold text) follows:

```
<cartridgeUnit>
<name>[your_company_name].cisco.units.cu3.7505.12.2(25)S</name>
<driverType>cisco</driverType>
<deviceType>Cisco 7505</deviceType>
<osVersion>12.2(25)S</osVersion>
:
<capabilities>com/metasolv/serviceactivator/cartridges/cisco/capabilities/
cisco_default.xml</capabilities>
<options>custom_options/cisco/7500-12.2_25_S_QoSoptions.xml</options>
:
</cartridgeUnit>
```

Remove the **cartridge.cisco.saa.actionType.Nmvt.isDefault** entry from the existing cisco options files before upgrading IP Service Activator.

Any previous changes made to the *Service_Activator_home/Config/cisco_options.csv* need to be reflected in the new **cisco_options.csv** files before regenerating the options using the Cisco Cartridge Configuration Utility. You must merge any changes to the version of the file that you backed up using the procedure in "[Backing Up IP Service Activator](#)".

Upgrading a CTM Template Schema to Version 4 or later

You can upgrade a template created in schema versions 1, 2, or 3. Do this by exporting the file and then re-importing the file back into a new CTM template.

See *Design Studio Modeling Activation* online Help for information about how to import and export a template file.

Upgrade Tools

The Network Processor upgrade and database upgrade tools are installed with the IP Service Activator Installer. Perform the activities in this section to configure upgrade properties, and to run the upgrade.

If you are not running the Network Processor, you can run the dbUpgrade script. For more information, see "[Running dbUpgrade to Upgrade the Database](#)".

Network Processor on Multiple Servers

The npUpgrade script runs against the database. If you have the IP Service Activator Network Processor installed on multiple servers:

- If they all use the same database connection parameters (as specified in the Configuration GUI), you need to run npUpgrade only once.
- If they use different database connection parameters, you need to repeat the Network Processor Upgrade once for each Network Processor database.

Running npAdmin to Update Network Processor Internal Data

This section provides information about how to update the Network Processor version in the database after upgrading to a new version of the IP Service Activator.



Note:

To complete this operation, you need the database connection details used by the IP Service Activator.

To update the Network Processor version in the database:

1. Run the **npAdmin** script.
2. Enter the following command to retrieve the current version number of the processor:

```
bash-3.2$ ./npAdmin.sh get_version
```

3. Enter the following command to update the version number of the network processor:

```
bash-3.2$ ./npAdmin.sh set_version 7.5.0
```

4. The following warning appears:

```
Warning! This will modify the Network Processor internal data.  
Do you want to continue? (yes/no):
```

5. Enter yes.
6. Enter your username and password.
7. To confirm the update, enter:

```
bash-3.2$ ./npAdmin.sh get_version
```

The version is updated.

Running npUpgrade: Network Processor Upgrade Script

This section provides information about running the Network Processor upgrade script.

Note:

In order to improve the performance of this process, set the log level for npUpgrade to **info** in the following file:

Config/networkProcessor/upgradeTool/logging.properties

To run the npUpgrade script:

1. Run the **npUpgrade** script.
2. As the *IPSA_admin_unix_account* user, enter:

```
cd Service_Activator_home/bin
npUpgrade.sh -all
```

Note:

Do not run the npUpgrade script unless all required cartridges and service cartridges are installed.

3. Review the *Service_Activator_home/upgradeHome/upgrade/reports/upgradeReport.txt* file for errors.
4. Check the **upgradetool.log** for errors.
5. Refer to the reference sections at the end of this chapter for information about how to handle errors you encounter in the upgrade report or log files:
 - [Network Processor Upgrade Tool default.properties File](#)
 - [npUpgrade Script Failure Analysis](#)
 - [Network Processor Upgrade Directory Structure](#)

Note:

If you receive an error when running the npUpgrade tool on a Linux server, you must make sure that the Linux setup library is installed. See "[Problem Running npUpgrade on Linux](#)" for more information.

Running Failure Analysis on npUpgrade Results

To analyze the Device Audit files for those devices identified as upgrade failures:

1. Copy the contents of the *upgrade_home/upgrade/failures* directory to a separate workstation with a browser.

- For each device identified as an upgrade failure, open its **DeviceAudit.xml** file, check for red text, and analyze it against the failure cases listed in "[Performing Post-Upgrade Data Cleanup](#)". (Certain red text entries are acceptable.)

 **Note:**

If the upgrade of some devices fails, the devices must be unmanaged in IP Service Activator before the next Network Processor restart. To unmanage the failed devices, start all the IP Service Activator components except the Network Processor(s), unmanage the devices that have failed upgrades, then start the Network Processor(s). You can then deal individually with the devices with failed upgrades without affecting other devices. To obtain help dealing with these failures, Oracle recommends that you contact Oracle GCS for assistance using the service request process. Attach a .zip file containing the contents of the `upgrade_home/upgrade/failures` directory to the service request.

- When problem devices have been fixed, you can use the `npUpgrade` script with appropriate options to upgrade individual devices, or a specified list of devices. For example:

```
Usage: npUpgrade.sh [-all] | [-device ipAddress1,ipAddress2,*] | [-file filename]
| [-help]
```

```
Example 1: npUpgrade.sh -device 10.13.3.158,10.13.4.120
where the -device value can be one device IP address, or a comma-separated list of
device IP addresses
```

```
Example 2: npUpgrade.sh -file <filename>
where <filename> contains a list of device IP addresses, with one IP address per
line. <filename> must include the relative path from <upgradeHome>.
```

Running dbUpgrade to Upgrade the Database

This section provides information about running the database upgrade script.

To upgrade the database, you run the **dbUpgrade** script.

Run the `dbUpgrade` database schema upgrade tool as described below to make the required changes to the database for upgrade to the new IP Service Activator release.

 **Caution:**

Do not run the `dbUpgrade` script unless you backed up your old IP Service Activator data. For information, see "[Backing Up IP Service Activator](#)".

Truncating Transactions: If you decided to save committed transaction records, use the `-truncate true` option when you run the `dbUpgrade` script. This option keeps a database record of the archived transactions but removes the active operations associated with them, to reduce the database storage required. If you have already deleted the committed transaction records, then you do not need to use this option.

To run the database upgrade tool:

1. Run the following command:

```
cd Service_Activator_home/bin
dbUpgrade.sh
```

For more information about required and optional parameters, see [Table 9-4](#).

Table 9-4 Database Upgrade Tool Parameters

| dbUpgrade Parameter | Value | Information | Example |
|---------------------|----------------------|--|--|
| -dbHost | DatabaseHostname | required | localhost |
| -dbUser | DatabaseUsername | required | admin |
| -dbPass | DatabasePassword | required | admin |
| [-dbPort] | DatabasePort | optional | 1521 |
| [-dbSid] | DatabaseSID | optional | IPSA.WORLD |
| [-tmpDir] | TempStorageDirectory | optional | default = WorkingData/ dbUpgrade |
| [-truncate] | true false | optional "true" truncates transactions; default = false | false |

2. Ensure that dbUpgrade connects and runs. This may take a while. Check the console window for any errors and updates. Look for the result **Completed** in the messages, which indicates the database upgrade is done.

 **Note:**

The dbUpgrade tool upgrades the database and any installed Configuration Policies.

Starting the New IP Service Activator System

This section describes the configurations and explains the steps you need to take to start the new IP Service Activator system after an upgrade.

Network Processor Configuration

Configure network processors for Offline Test mode.

Network processors should be configured initially to start in Offline Test mode. For more information, see "Command Delivery Modes" in *IP Service Activator System Administrator's Guide*.

Starting the New IP Service Activator System

1. As the IP_SA_admin_unix_account user, start the new IP Service Activator server software:

```
naming_service_script start  
component_manager_script start
```

To start the naming service, run the following command:

```
ipsans start
```

To start the component manager, run the following command:

```
ipsacm start
```

To view the processes running for IP Service Activator, run the following command:

```
ipsaps
```

The scripts **ipsans** and **ipsacm** are located at *Service_Activator_home/bin*.

2. Launch the new IP Service Activator client.
3. If you set the transaction archive limit to zero, reset the transaction archive limit:

In the IP Service Activator client, click **Tools**, and then select **Options**.

On the **Options** dialog box, **Transactions** page, set the **Transactions archive limit** to a number appropriate to your installation and click **OK**.

Commit the transaction.

4. Analyze the audit trails for network processors.

Copy the contents of the **/opt/OracleCommunications/ServiceActivator/AuditTrails** directory to a separate workstation with a browser.

For each device identified as an upgrade failure, open its **DeviceAudit.xml** file, check for red text, and analyze it against the failure cases listed in the following section "[Performing Post-Upgrade Data Cleanup](#)". (Certain red text entries are acceptable.)

See "[Running Failure Analysis on npUpgrade Results](#)".

5. Perform a network audit of all network processor devices.

On Solaris or Linux, run the **auditdevice** script with the **-all** parameter.

On a Windows machine, run **auditdevice.bat** with the **-all** parameter.

Refer to *IP Service Activator System Administrator's Guide* for details about auditing.

6. Review all discrepancies for acceptability for your network as in step 4.
7. Re-enable the IP Service Activator users that were disabled before starting the upgrade.
8. Manage devices which are in Offline Maintenance mode.

This causes the Network Processor to make any final adjustments to the device model for each device.

It may also raise faults that identify Interface Description mismatches.

 **Note:**

At this point, the following error message may appear:

```
"Internal Failure, could not find any failed associations to be isolated".
```

You can safely ignore this error message, but you must examine any other error messages that appear and fix the indicated problems.

9. If Interface Description mismatches are identified, perform the activity described in ["Cleaning Up Interface Description Mismatches"](#).
10. Examine the contents of the audit trail file for each vendor cartridge to ensure that the upgrade is complete. The startup should complete but you should not see any activity in the audit trails. These files are stored in the `Service_Activator_home/AuditTrails` directory.
11. Do ["Performing Post-Upgrade Data Cleanup"](#).

The IP Service Activator upgrade procedure is now completed.

Upgrading IP Service Activator to a New Location

This section describes how to upgrade an IP Service Activator installation from one server to another. The old and new servers can be on the same or different platforms. Note that Solaris 32-bit is not supported.

To upgrade IP Service Activator to a new location:

1. Install the new version of IP Service Activator (and all necessary components) on a Solaris or Linux server using the Oracle Universal Installer (Solaris or Linux version). For more information about installing IP Service Activator, see ["Installing IP Service Activator on an Oracle Solaris or Linux Server"](#). For general installation information, see ["Installing IP Service Activator"](#).

 **Note:**

Do not run the Configuration GUI when prompted by the Installer. You must restore your **Config** directory to the new installation directory before running the tool.

2. Copy the `Service_Activator_home/Config` directory and `Service_Activator_home/modules/config` directories from the old server to the new `Service_Activator_home` directory on the new server.
3. Copy the `Service_Activator_home/WorkingData` directory from the old server into the new `Service_Activator_home/WorkingData` directory on the new server.
4. Remove **omninares*** from `Service_Activator_home/WorkingData` on the new server.
5. Manually run the Configuration GUI to configure your system and commit changes to the host.
6. (Optional) Update the CORBA parameters if the new server IP address has changed. Update the database parameters if the database was imported to a new

database user. Update the upgrade home path to the new installation location.
`Service_Activator_home/bin/configGUI.sh`

 **Note:**

If you are upgrading your IP Service Activator installation and migrating to another platform at the same time, follow the upgrade instructions, and ensure that you restore your `Service_Activator_home/upgradeHome` directory from your backup to the new `Service_Activator_home` directory on the new server.

To configure the connection to the new server:

1. From Windows, click **Start**, and then **All Programs**.
2. From the **Oracle - OracleCommunications** menu, select **Service Activator**, and then **Configuration GUI (Local Host)**.
3. Click **OK**.
An information message indicates that the configuration is successfully loaded for the specified host.
4. Double-click the **localhost** folder.
5. Click **CORBA**.
6. Enter values for naming service IP address, and naming service port for connection to the new server.

Performing Post-Upgrade Data Cleanup

This section includes recommended data cleanup activities to be performed after upgrade, if they apply to your system.

Cleaning Up Interface Description Mismatches

The Interface Description attribute can be set in either or both of two places:

- in an **Interface Creation Configuration Policy**.
- in the **Site properties - Addressing page**.

If set in both places, the interface descriptions must match or a fault is raised.

To solve this issue:

1. Check if the interface description set on the **Interface Creation Configuration Policy** matches the interface description for the same interface set on the **Site properties - Addressing page**.
2. Remove the contents of the **Interface Description** field on the **Interface Creation Configuration Policy**, -OR- on the **Site properties - Addressing page**, and submit the change.
3. Repeat for each mismatch identified.

Rolling Back the Upgrade

If required, you can roll back the upgrade to the new IP Service Activator release and return the system to its previous state in the old IP Service Activator release.

Prerequisites

Before rolling back the upgrade, you must have the Installer for the old IP Service Activator release to which you want to revert.

Rolling Back the Upgrade

To roll back the upgrade:

1. Back up the new IP Service Activator database and the IP Service Activator installation directory (by default **opt/OracleCommunications/ServiceActivator/***) for diagnostic use.
2. Uninstall the new IP Service Activator software.
3. Delete the new install directories using `rm -r` (by default **opt/OracleCommunications/ServiceActivator**).
4. Install the old IP Service Activator software. Include all required components.
5. Delete the directories that were created by the old IP Service Activator installation in *Service_Activator_home*. The reason for this is that you will be restoring these directories from your backup.
6. Restore **/opt/Orchestream** and **/var/Orchestream** from your old IP Service Activator backup.
7. Drop the old IP Service Activator database user.
8. Restore the old IP Service Activator Oracle Database information. See Oracle Database documentation for information about methods for restoring the data.
9. Start the system using the same precautions and steps outlined in "[Starting the New IP Service Activator System](#)".

Upgrade Reference Information

This section contains helpful reference information for the upgrade process.

Network Processor Upgrade Tool default.properties File

The **default.properties** file contains the IP Service Activator database login information and the directory location *upgrade_home* for the Network Processor Upgrade tool output. Device models are stored in an Oracle Database table. See sample content for various versions of the file.

Example 9-1 Example IP Service Activator default.properties File Content

```
###  
#Copyright (c) 2008, 2022 Oracle. All rights reserved. Oracle is a trademark
```

```
# of Oracle Corporation and/or its affiliates. Other names may be trademarks
# of their respective owners.
#
# Auto-Generated by the IPSA Configuration Tool [ 2022-05-11 08:36:59 ]

####

# Full path name of the home directory that will hold the "upgrade" sub-directories.
upgradeHome = /opt/OracleCommunications/ServiceActivator/upgradeHome

# deviceList retrieval method = 'database' or explicit list (use one or the other).
Explicit list: oid,name,ipa:oid,name,ipa:oid,name,ipa:oid,name,ipa:oid,name,ipa
deviceList = database

# Location of last device models to be upgraded: 'files' (if stored in cacheDD
directory), 'database' (if stored in np_lds table) or 'np_ldm' (if stored in np_ldm
table).
npModelSource = database

# Checks that saxon is the correct version as is hardcoded in the network processor.
disableEnvCheck = false

# Number of concurrent processes (should be less than the number of processors)
processes = 2

# The total amount of memory (in MB) to be used by all children processes (it will be
divided among them)
totalMemory = 2048
```

**Note:**

The database details are read from the **db.properties** file. The **db.properties** file is created when you run the Configuration GUI.

npUpgrade Script Logging Properties

The **logging.properties** file contains the log file location (which defaults to *Service_Activator_home/logs/upgradetool*.log*) and the desired log level. The following log levels are commonly used:

- error = any exceptions or null variable errors
- info = tool progress and results
- debug = more details

npUpgrade Script Failure Analysis

There may be some errors flagged in the audit reports by **npUpgrade.sh** which do not reflect problems which need resolution.

Audit failures listed below can be ignored.

Sub-interface Unit Number on Juniper

You can ignore the configurations similar to the following displayed in red:

```
###ACTUAL VALUE ON DEVICE: t1-7/0/0:12 ###  
next-hop t1-7/0/0:12.0;
```

The next-hop command changed from having 0:12 at the end to having 0:12.0. Juniper interfaces should be labelled with the subinterface of 0, so no changes are needed.

Interface Per-packet Load-sharing on Cisco

You can ignore the configurations similar to the following displayed in red:

```
ip load-sharing per-packet
```

Interface Description String on Cisco

If you had spaces in your old descriptions, they will be removed in the new descriptions. You can ignore the configurations similar to the following displayed in red:

```
description ... SD:123456789; UD:...
```

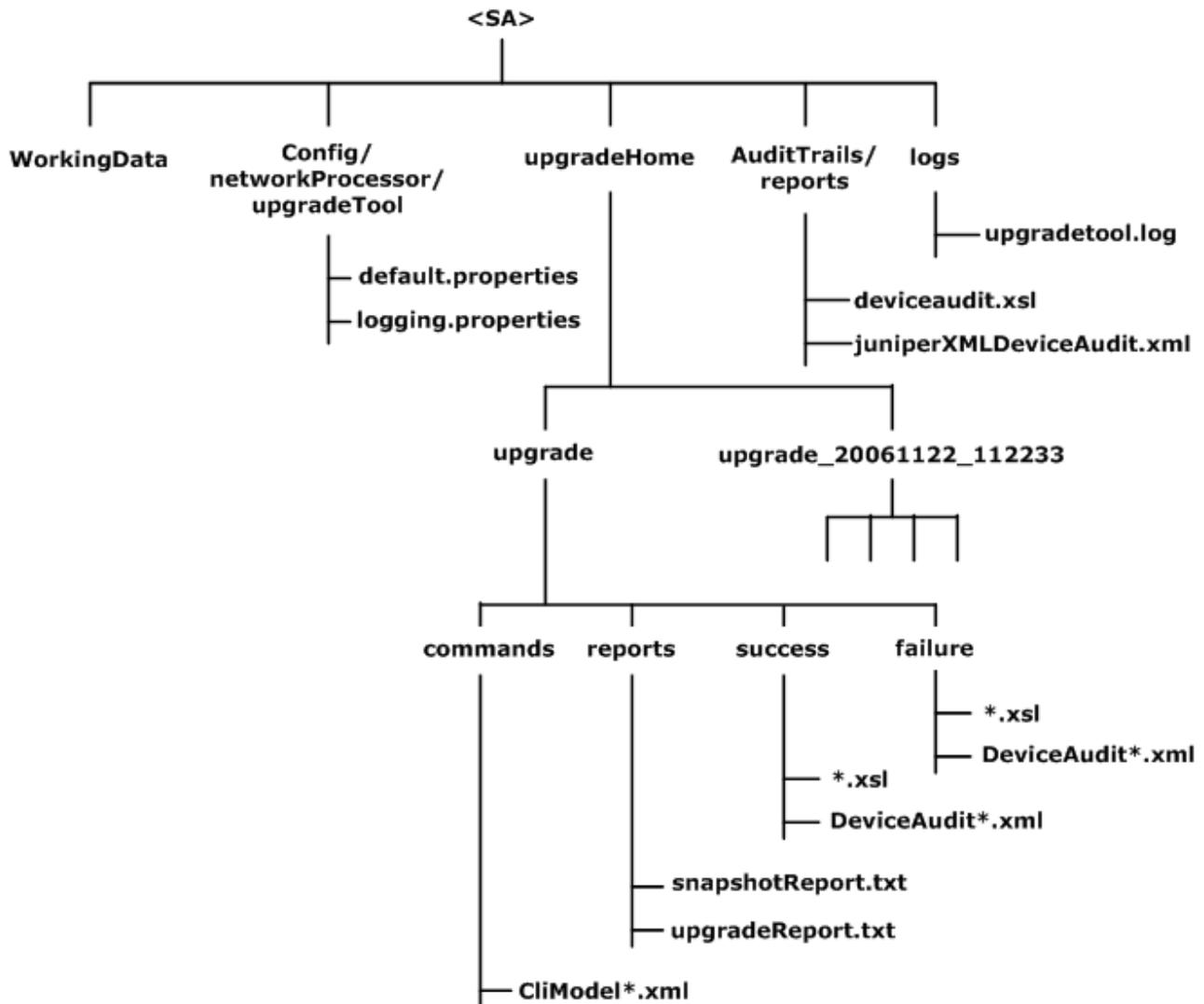
and the configurations similar to the following displayed in blue:

```
description ... SD:123456789;UD:...
```

Network Processor Upgrade Directory Structure

[Figure 9-3](#) shows the directory structure of the files involved in the upgrade (assuming default file locations).

Figure 9-3 Network Processor Upgrade Directory Structure



Patching IP Service Activator

Installing an IP Service Activator patch follows the same process as the original installation. You can customize the patch installation by selecting the **Custom** installation type. Components that are already installed are listed on a summary page and are not re-installed.

Prerequisites

Before installing a patch:

- Back up the Oracle Database. See "[Backing Up IP Service Activator](#)".
- Decide whether to delete or save a truncated version of all committed transaction to avoid generating core files when IP Service Activator restarts. See step 5 in "[Preparing to Upgrade](#)".

Installing a Patch

To install a patch:

1. Log in to Oracle Support at:
<https://support.oracle.com/portal/>
2. Select the **Patches & Updates** tab.
3. Search for the patch number and download the latest patch to the Solaris or Linux server (which has the IP Service Activator server installed) or Windows host (which has IP Service Activator client).
4. Stop IP Service Activator components.
5. Unzip the patch.
6. In the Solaris or Linux console, run the following command:

```
unzip IPServiceActivator-7.x.x.x.xBuild-xxx-.zip
```

In Windows, unzip the **IPServiceActivator-7.x.x.x.xBuild-xxx-win64.zip** file.

The IP Service Activator directory is created.

7. In Windows, run **setup.exe** in the install directory to launch the Oracle Universal Installer and do the client upgrade and installation.

In Solaris and Linux, run the **runInstaller** in **Disk1/install** and complete the server upgrade and installation.

8. Select the installation type you want. To upgrade or reinstall components, select the **Custom** installation type and click the **Required Components** check box.



Note:

You can use silent installation to upgrade IP Service Activator. Previously recorded response files can be used to do the upgrade, or the response template can be used to install the patch. For information about using silent installation, see "[About Silent Installations](#)".

Updating Configuration Policy Definitions

After you install an IP Service Activator patch, you must ensure that the system is using the latest configuration policy definitions.

To update a configuration policy definition:

1. In the Global Setup window, select a domain in the **Hierarchy** pane.
2. Right-click **Domain** and select **Properties**.
3. In the **Domain** dialog box, select the **Setup** property page.
4. Click **Browse**.
5. Select the policy file that is related to the enhanced configuration policy and click **Open**.

6. Click **Load**.
The configuration policy loads and a confirmation dialog box opens.
7. Click **OK**.
The confirmation dialog box closes.
8. Click **OK**.
The Domain dialog box closes.
9. Commit the transaction.
10. Click the domain to open it.
11. Select the **Policy** tab and expand the **Policy Types** folder.
12. Find the sub-folder where your policy type is located.
13. Right-click the Policy Type and select **Properties**.
The Policy Types dialog box opens.
14. Click **Import HTML**.
15. Select the HTML file for the configuration policy that you want to import, and then click **Open**.
16. Click **OK**.
17. Commit the transaction.

10

Uninstalling IP Service Activator

This chapter describes how to safely uninstall the main Oracle Communications IP Service Activator application completely using the uninstaller, or by component package using Admintool. It also describes how to uninstall the IP Service Activator client.

Uninstalling IP Service Activator from UNIX Server



Note:

All UNIX installations, such as Oracle Solaris 64 and Linux, use the following procedure.

To uninstall IP Service Activator components:

1. Go to your IP Service Activator installation directory.
The default is **/opt/OracleCommunications**.
2. Set the **ORACLE_HOME** environment variable to the directory where IP Service Activator is installed. For more information, see "[Preparing to Install IP Service Activator](#)".
3. Go to **ORACLE_HOME/oui/bin** and run the Oracle Universal Installer:

```
./runInstaller
```

The Installer launches and the Welcome window opens.

4. Click **Installed Products**.
The Inventory window opens.
5. Select the items that you want to uninstall and click the **Remove** button.
The Confirmation window opens.
6. Click **Yes**.
The Remove window appears with a progress bar and uninstalls the selected components.
The Inventory window opens without the components that have been uninstalled.
7. Click **Close**.
8. Click **Cancel**.
The **Exit** window opens.
9. Click **Yes** to confirm the uninstallation.

Uninstalling IP Service Activator Client



Note:

All Windows installations, such as Windows 64, use the following procedure.

To uninstall the IP Service Activator client from a Windows host:

1. On your Windows machine, go to the *software un-zip location*\client\Disk1\install directory and double-click **setup.exe**.
The **Welcome** window opens.
2. Click **Deinstall Products**.
The **Inventory** window opens.
3. Select the that items you want to uninstall.
4. Click the **Remove** button.
The **Confirmation** window opens.
5. Click **Yes**.
The **Remove** window opens with a progress bar and uninstalls the selected components.
The **Inventory** window opens without the components that have been uninstalled.
6. Click **Close**.
7. Click **Cancel**.
The **Exit** window appears.
8. Click **Yes** to confirm the uninstallation.

11

Troubleshooting the Installation

This chapter outlines some of the problems that can occur during the installation of Oracle Communications IP Service Activator, and explains how to fix them.

See *IP Service Activator System Administrator's Guide* for general troubleshooting information.

Note:

See *IP Service Activator Release Notes* for release-specific workarounds for known issues.

There is no mechanism for repairing IP Service Activator components. If faults are reported by the operating system when starting up a system component, we recommend that you remove and reinstall the software.

If you cannot resolve your installation problem, contact My Oracle Support:

<https://support.oracle.com/portal/>

This chapter provides information about the following:

- [Oracle Database Installation Fails to Run](#)
- [Oracle Database Installation Fails Before Completion](#)
- [Manually Configuring Oracle Client Connection: Solaris](#)
- [Client Errors](#)
- [omniORB Use of TCP Wrappers](#)
- [Oracle Universal Installer Error](#)
- [Client Cannot Connect to Policy Server](#)
- [Loading SharedPolicyData.policy to Avoid Incomplete Software Upgrade](#)
- [IPSAPS Does Not Work](#)
- [Problem Running npUpgrade on Linux](#)

Oracle Database Installation Fails to Run

You might get the following error when trying to run the IP Service Activator 7.3.0 installer:

```
Exception java.lang.UnsatisfiedLinkError:  
/tmp/OraInstall12016-04-01_12-45-51AM/jre/1.6.0/lib/i386/xawt/libmawt.so:  
libXext.so.6: cannot open shared object file: No such file or directory occurred..  
java.lang.UnsatisfiedLinkError:  
/tmp/OraInstall12016-04-01_12-45-51AM/jre/1.6.0/lib/i386/xawt/libmawt.so:  
libXext.so.6: cannot open shared object file: No such file or directory
```

If you receive this error, run the following script:

```
yum install glibc.i686 libXext.i686 libXrender.i686 libXtst.i686 lib.gcc.i686
```

You should then be able to run the installer.

Oracle Database Installation Fails Before Completion

Check the following:

- The parameters in the **/etc/system** file are correct and match those supplied in the template file
- The **oracle** user exists and you are installing Oracle Database software as that user
- The dba group exists and the **oracle** user is assigned to that group
- You have applied all recommended Oracle Solaris patches. For more information, "[Planning an IP Service Activator Installation](#)".
- You have applied all recommended Linux patches.

Note:

For more information about how this works in a Solaris environment, log into a Solaris 11 box and type `man ulimit`.

Manually Configuring Oracle Client Connection: Solaris

The Oracle client connection is typically automatically configured by the IP Service Activator server software installation program on Solaris, which has a pre-selected option to install the Oracle client. However, if you did not install the supplied Oracle client, you must manually configure the database connection to your own Oracle client by editing the **tnsnames.ora** file. It is located at:

ORACLE_HOME/network/admin/tnsnames.ora.

You might also have to create the **ORACLE_HOME** environment variable on the server.

To configure the Oracle client connection manually on Solaris:

1. Change to the **root** user:

```
$ su - root
```

2. Change to the Oracle administration directory. For example, for Oracle8i:

```
# cd /usr/local/oracle/u01/app/oracle/product/8.1.7/network/admin
```

3. Edit the **tnsnames.ora** file as follows:

```
net_service_name =  
(DESCRIPTION = (ADDRESS_LIST =  
(ADDRESS = (PROTOCOL = TCP) (Host = host_name) (Port = port_no))  
)  
(CONNECT_DATA = (SERVICE_NAME = service_name)))
```

where:

- *host_name* is the host name of the machine on which the database resides
- *port_number* is the port number to be used for communication
- *net_service_name* is the name of the Net8 (NetCA) service
- *service_name* matches the value in the equivalent section of the Oracle server's **tnsnames.ora** file

Consult your local Database administrator if you need additional help.

 **Note:**

The procedure for manually configuring the Linux client connection is the same as Solaris.

Client Errors

If an error occurs in the IP Service Activator client, a critical message is written to the current faults pane. These messages are displayed on a red background. See *IP Service Activator System Administrator's Guide* for more information.

omniORB Use of TCP Wrappers

Installers should be aware that omniORB uses TCP wrappers.

Incorrect configuration of TCP wrappers can trigger various CORBA-related issues including:

- Inability of the Policy Server to communicate with the Naming Service
- Inability of the client to connect
- Inability of OSS Integration Manager (OIM) processes to connect
- Other anomalies around the use of the Naming Service

To correct these issues, correct the omniOrb configuration so that IP Service Activator processes are properly named as being allowed to connect to the ORB.

If this condition has already affected your installation, correct the ***/etc/hosts.**** files (***/etc/hosts.deny*** and ***/etc/hosts.allow***) or force omniORB to different configuration files with environment variables. For information about environment variables, see:

<http://omniorb.sourceforge.net/docs.html>

For more information, see "[CORBA ORB Configuration for IP Service Activator](#)".

Oracle Universal Installer Error

You might get an error when Installing the IP Service Activator client on Windows 10.

After double-clicking on **setup.exe**, if you see the following error, either enter **y** to ignore or adjust the virtual memory setting and enter **n**.

```
Starting Oracle Universal Installer...
Checking swap space: 0 MB available, 500 MB required.      Failed <<<<
Checking monitor: must be configured to display at least 256 colors Higher than
256 .      Actual 4294967296      Passed
Some requirement checks failed. You must fulfill these requirements before
continuing with the installation,
Continue? (y/n) [n]
```

If you encounter errors or issues when using the Oracle Universal Installer to install IP Service Activator or the IP Service Activator client, see *Appendix B* in the Universal Installer documentation for more information:

http://docs.oracle.com/cd/B28359_01/em.111/b31207/toc.htm

Client Cannot Connect to Policy Server

- Verify that the policy server is running by running **.Jipsaps** on the server machine. See *IP Service Activator System Administrator's Guide* for more information.
- Verify that you can ping the IP address to which the client is attempting to connect.
- Check that you are attempting to connect a Win64 client to a 64-bit policy server.
- Check whether the Windows firewall is blocking access. On Windows 10, if the firewall is turned on and set to notify when Windows firewall blocks a new program, allow access to the IP Service Activator applications when prompted and they (IP Service Activator, Explorer, omninames) will be added to the list of programs to be allowed through the Windows firewall.

Loading SharedPolicyData.policy to Avoid Incomplete Software Upgrade

Errors received while loading policy files such as **default.policy** or **advanced.policy** into IP Service Activator might be triggered by an incomplete software upgrade.

Load **SharedPolicyData.policy** to create new rows for IPv6 in the database. See *IP Service Activator System Administrator's Guide* for more information about loading configuration policies.

IPSAPS Does Not Work

IPSAPS does not work if the policy server output is too long.

If you see the following error:

```
awk: record ` 12138 ?      S 0...' too long
```

You must set up AWK_PATH, as shown in the following example:

```
AWK_PATH=/usr/xpg4/bin
```

Problem Running npUpgrade on Linux

You might receive the following error when running npUpgrade on Linux:

```
Exception in thread "main" java.lang.UnsatisfiedLinkError: /opt/OracleCommunications/ServiceActivator/odbc/lib/libocijdbc11.so: libaio.so.1: cannot open shared object file: No such file or directory
    at java.lang.ClassLoader$NativeLibrary.load(Native Method)
    at java.lang.ClassLoader.loadLibrary1(Unknown Source)
    at java.lang.ClassLoader.loadLibrary0(Unknown Source)
    at java.lang.ClassLoader.loadLibrary(Unknown Source)
    at java.lang.Runtime.loadLibrary0(Unknown Source)
```

To resolve this error and run npUpgrade successfully, you must make sure the Linux **libaio** package is installed. This package is part of the Linux setup library.

A

Installation Checklists and Worksheet

We strongly recommend that you use the following installation checklists when installing both Oracle Database software and Oracle Communications IP Service Activator components.

These checklists are designed to:

- Provide a quick reference to the recommended installation settings for each installation task
- Enable you to record any user-specific settings you may decide to enter during an installation task
- Help you to provide important configuration information to Oracle GCS when troubleshooting installation problems

Checklists include:

- [Oracle Database Installation Data](#)
- [IP Service Activator Multi-host General Installation Checklist](#)
- [Client Installation Checklist](#)
- [Site Survey Worksheet](#)

Oracle Database Installation Data

[Table A-1](#) is designed to help determine the size of a new network.

Table A-1 Oracle Database Installation Data Worksheet

| Setting | Attribute | Recommended | Recorded value |
|---|--|---|----------------|
| Oracle Database home settings | Location | <code>/usr/local/oracle/u01/app/oracle/product/<i>version</i></code> | |
| NetCA service connection settings | Global Database Name | IPSA.WORLD | |
| Not applicable | Net Service Name | IPSA | * |
| Not applicable | Host Name (IP Service Activator database) | None supplied | |
| Not applicable | Database SID | IPSA | * |
| IP Service Activator database settings | Tablespace name | IPServiceActivatorDb | |
| Not applicable | Datafile Name | <code>/usr/local/oracle/u01/app/oracle/oradata/IPSA/IPSERVICEACTIVATORDB.dbf</code> | |
| Not applicable | File Size | 250 MB | |

Table A-1 (Cont.) Oracle Database Installation Data Worksheet

| Setting | Attribute | Recommended | Recorded value |
|---|-----------------|-------------|----------------|
| Not applicable | Increment | 5 MB | |
| Oracle Database Listener settings | Global name | IPSA.WORLD | |
| IP Service Activator database login settings | Database userID | admin | * |
| Not applicable | Password | admin | * |

*These items are entered when installing the IP Service Activator Policy Server, client, and they must be identical to those defined here.

IP Service Activator Multi-host General Installation Checklist

Complete one copy of [Table A-2](#) for each host.

Table A-2 Multi-Host General Installation Checklist

| Setting | Attribute | Recommended | Recorded value |
|-------------------------------------|------------------------------------|--|----------------|
| Server hostname | | | |
| Serial Number | | If you were provided with a serial number by Oracle Communications for a previous deployment, you must re-enter that value for the new deployment. | |
| Installed Files Location | Destination Folder | Use default supplied | |
| Naming service settings | Hostname | None supplied Record local hostname for reference when installing other components. | |
| Not applicable | TCP/IP Port | 2809 | |
| Database connection settings | Data Source Name (DSN) | IPServiceActivatorDb Check Oracle Database installation | |
| Not applicable | Database Server IP Address | None supplied | |
| Not applicable | Database Server Port | Use default 1521 | |
| Not applicable | Database Service Name (SID.DOMAIN) | IPSA.WORLD Check Oracle Database installation | |
| Not applicable | Database Userid | admin Check Oracle Database installation | |
| Not applicable | Database User Password | admin Check Oracle Database installation | |

Table A-2 (Cont.) Multi-Host General Installation Checklist

| Setting | Attribute | Recommended | Recorded value |
|--|-----------------|----------------------|----------------|
| IP Service Activator Program Folder | Program Folders | Use default supplied | |

Client Installation Checklist

The task in [Table A-3](#) is described in the additional setup tasks to be run prior to initial startup topic in *IP Service Activator System Administrator's Guide*.

Table A-3 Client Installation Checklist

| Setting | Attribute | Recommended | Recorded value |
|-------------------------------------|--------------------|----------------------------|----------------|
| Install Files Location | Destination Folder | Use default supplied | |
| Naming service settings | Hostname | Use Policy Server hostname | |
| Not applicable | TCP/IP Port | 2809 | |
| IP Service Activator Program Folder | Program Folders | Use default supplied | |

Site Survey Worksheet

[Table A-4](#) can help to determine the size of a new network. Use the survey data to determine the appropriate hardware for an IP Service Activator deployment. Being able to answer the questions in this list prior to contacting Oracle Global Customer Support for assistance, can also speed the resolution of sizing and support issues.

Table A-4 Site Survey Worksheet

| Deployment Characteristics | Recorded Values |
|---|-----------------|
| Devices: | |
| Number of managed PEs and vendor type(s) | |
| Average number of interfaces/sub-interfaces/VC-endpoints per PE device | |
| If Configuration Management module is deployed, average number of device configuration archives per PE to be retained | |
| Number of managed CEs and vendor type(s) | |
| Average number of interfaces/sub-interfaces/VC-endpoints per CE device | |
| If Configuration Management module is deployed, average number of device configuration archives per CE to be retained | |
| VPNs: | |

Table A-4 (Cont.) Site Survey Worksheet

| Deployment Characteristics | Recorded Values |
|--|-----------------|
| Number of user VPN connections (Sites) | |
| QoS: | |
| Number of concrete policy elements | |
| Breakdown on a per policy element basis if possible | |
| Miscellaneous IP Service Activator activity: | |
| Number of GUI logins per day | |
| Number of device discoveries and capability fetches per day (the size and nature of CEs and PEs that are likely to be discovered affect discovery times) | |
| PEs (average number of interfaces per device) | |
| CEs (average number of interfaces per device) | |
| System component usage: | |
| OSS Integration Manager (OIM) (deployment generates additional CPU demand on the Policy Server host machine) | |
| Maximum number of concurrent GUI users | |
| System configuration: | |
| Is Citrix usage in use? | |
| List of all other implementation-specific restrictions: | |
| Bandwidth limitations (if any) | |
| Cost considerations | |
| Other deployment issues | |

B

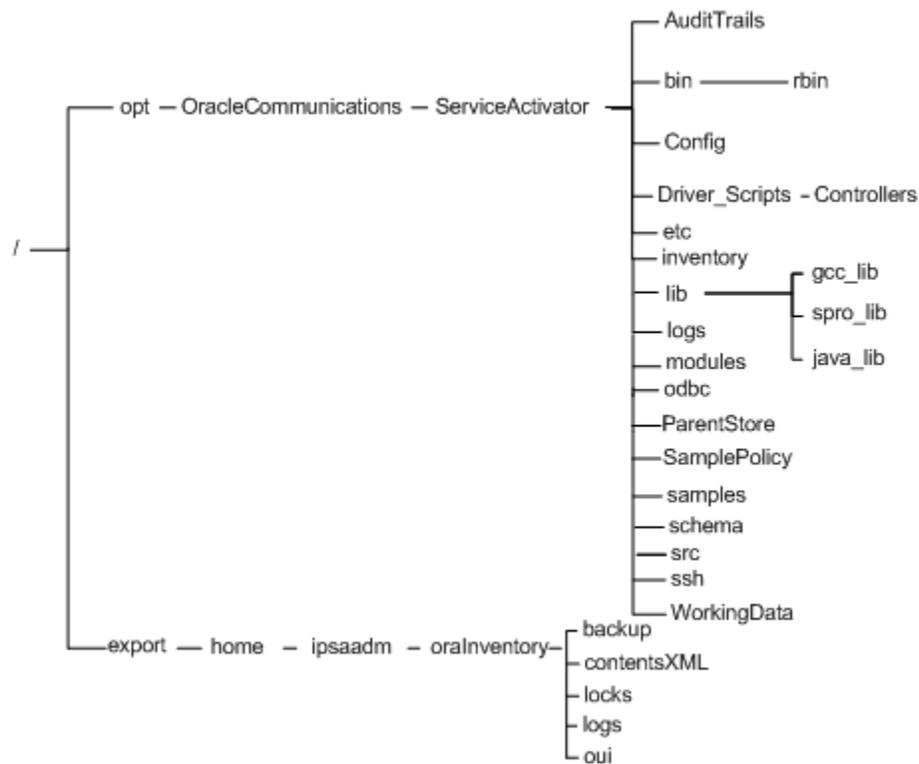
Directories and Files

This appendix describes directories and files created by the Oracle Universal Installer for Oracle Communications IP Service Activator.

Directory Structure

The Installer creates the directory structure shown in [Figure B-1](#).

Figure B-1 IP Service Activator Directory Structure



Note:

The path `/opt/OracleCommunications/ServiceActivator` is usually indicated as `Service_Activator_home` in this document.

Symbolic Links

If you choose to run the naming service and component manager automatically, the following symbolic links are created in **/opt/OracleCommunications/ServiceActivator**:

- In the **/etc/rc0.d** directory, **K09ipsamgr** links to *Service_Activator_home/etc/init.d/ipsamgr* to shut down the naming service and component manager
- In the **/etc/rc3.d** directory, **S99ipsamgr** links to *Service_Activator_home/etc/init.d/ipsamgr* to start up the naming service and component manager

Both links point to the file *Service_Activator_home/etc/init.d/ipsamgr*

The contents of the IP Service Activator directory structure are listed and described in the following sections.

Directories and Contents

[Table B-1](#) lists some of the important directories created by the IP Service Activator installation process and the types of files and programs they contain.

Table B-1 Important Directories Created by Installation Process

| Directory Name | Contents |
|-----------------|---|
| bin bin/rbin | IP Service Activator executable and initialization files |
| Config | Configuration files |
| Driver_Scripts | Driver scripts for import to IP Service Activator |
| inventory | Contains permanent and product specific files. |
| lib | GCC, SunPro, and Tom Sawyer library files. |
| SamplePolicy | Example policy files for loading into IP Service Activator. |
| src | Contains the icons directory, and the integration_manager.idl file required for CORBA. |
| AuditTrails | The audit log files associated with the cartridges are stored in: /opt/OracleCommunications/ServiceActivator/AuditTrails |
| logs | Component manager, naming service, Policy Server, system startup log files, and core files are in /opt/OracleCommunications/ServiceActivator/logs . |
| ParentStore | Files that record the relationships between components are stored in /opt/OracleCommunications/ServiceActivator/ParentStore . Files are created at runtime by components as they register with their parent component. |
| WorkingData | Component log files are stored in /opt/OracleCommunications/ServiceActivator/WorkingData . |
| ipsaadm | The IP Service Activator administrator's home directory is /export/home/ipsaadm . |