SAL 2.0
Secure Access Concentrator Remote Server

Installation and Maintenance Guide

Doc ID: 145332
September 2011
Issue Number: 7

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Open Source Attribution
The Product utilizes open source software. For copyright notifications and license text of third-party open source components, please see the file named Avaya/Gateway/LegalNotices.txt in the directory in which you have installed the software.

Avaya support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Table of Contents

Preface

Purpose

The SAL 2.0 Concentrator Remote Server Installation and Maintenance Guide explains how to install and configure a Concentrator Remote Server.

Audience

This document is for the use of support personnel who:

- Install the gateway
- Configure the gateway for the remote service of managed devices

Conventions used

- Font: **Bold** is used for:
  - Emphasis
  - User interface labels

    Example: Click **Next**.
- Font: Courier New, Bold is used for commands.

  Example: Execute the command **`unzip SAL.zip`**.
- Font: Courier is used for GUI output.

  Example: `The directory already exists!`
- Font: Verdana, with expanded character spacing, is used for inputs.

  Example: You must enter the value `abc`.

Contacting Avaya technical support

If you still have questions after reading this manual, or the online help for the SAL Gateway Installer, you can contact Avaya for technical support.

Avaya Support	
Mail	Avaya Inc. 211 Mt. Airy Road, Basking Ridge, NJ 07920, USA
Internet	http://support.avaya.com
Phone	+1 (866)-GO-AVAYA

Chapter 1: Using this guide

This guide contains the following chapters and appendices:

Chapter 1, ***Using this guide***, describes what information is contained in this manual and how to receive technical support.

Chapter 2, ***SAL system***, describes the SAL (SAL) system architecture, system requirements, and licensing.

Chapter 3, ***Using a Sun ONE LDAP Directory Server with SAL***, explains how to configure a Sun ONE LDAP Directory Server as the authentication service in your SAL system. It explains the groups and users that you must define in LDAP for the SAL system.

Chapter 4, ***Using Microsoft's Active Directory with SAL***, explains how to configure a Microsoft Active Directory as the authentication service in your SAL system. It explains the groups and users that you must define in LDAP for the SAL system.

Chapter 5, ***Installing and configuring JBoss and Concentrator Remote Server***, explains how to install the JBoss Enterprise Application Platform Server and the Secure Access Concentrator Remote Server. It also explains how to configure your JBoss Server for use with the Concentrator Remote Server, applications, Oracle database, and LDAP Directory Server.

Note:

Complete JBoss server documentation is available directly at the Red Hat Web site: http://www.redhat.com/docs/en-US/JBoss_Enterprise_Application_Platform/. Avaya encourages you to search this site for JBoss server documentation explaining available patches, server information, supported Web application plug-ins, and so forth.

Chapter 6, ***Configuring the Oracle database***, explains how to configure the Oracle database for a new installation of the Secure Access Concentrator Remote Server system. This chapter provides the instructions to create the database tablespaces and user. It also explains how to create and initialize database tables.

Chapter 7, ***Installing and configuring the Reporting software***, explains how to install the Cognos 8 Business Intelligence software, which is the engine behind the Report application. The Cognos 8 reporting software is integrated with the SAL system and provided on the installation CD-ROMs. This chapter also explains configuration steps and how to set up the reports provided as part of your SAL.

Chapter 8, ***Configuring the Applications***, explains how to set up your Internet Explorer browser for the applications. In addition, it provides important configuration information for the Software Management application and for the Charting features of the Usage application. It also provides instructions for configuring and customizing the applications, including uploading reports and displays, integrating Access support, configuring Quick Launch, and setting other system properties. Finally, this chapter explains how to schedule tasks.

Chapter 9, ***Testing the installation and setting up your system***, explains how to start the Secure Access Concentrator Remote Server and conduct a test of your SAL system installation. It then explains how to use the Administration application to set up additional security and to check the system configuration. Finally, it explains the next steps to take (configuring devices and data) and refers you to the online help for the applications for instructions.

Chapter 10, ***Maintaining the SAL***, explains maintenance procedures, such as starting up the system, shutting it down, backing up data, and restoring data. It also explains various aspects of the interactions between the Secure Access Concentrator Remote Server and Agents, including dynamic redirection and maintenance mode. This chapter also provides error information and troubleshooting tips, explains how to perform specific tasks and how to contact Avaya.

Appendix A, ***Preinstallation checklist***, is a table of the fields that are a part of the installation data. The information must be kept handy before starting the installation process.

Appendix B, ***Concentrator Remote Server files***, lists the directories and files in a Secure Access Concentrator Remote Server installation.

Appendix C, ***Editing the DRMConfig.properties file***, lists and describes all of the properties in the order in which they appear in the DRMConfig.properties file. This file is the main configuration file for the system. The main chapters in this guide explain any changes you may need to make, based on your choices of components (LDAP Directory Server and Web Application Server). This appendix is provided as a reference for all of the properties.

Appendix D, ***Site Preparation Utility***, provides an overview of the Site Preparation Utility and explains how to log in and run diagnostics.

Chapter 2: Avaya Secure Access Link System

About this chapter

Introducing SAL introduces you to the Avaya Secure Access Link (SAL) system and briefly describes the components of the system and the data sources for the system.

Supported server configurations shows and briefly describes the single server configuration that you can use for your SAL system.

Considerations for setting up the server describes the hardware and software requirements for SAL.

Registering a Concentrator Remote Server with Avaya describes the process of registering a new server with Avaya.

Licensing the SAL system describes the functionality covered by the SAL license, and how to locate and read the license.

Introducing SAL

Key features in the SAL (SAL) system enable service personnel to diagnose, repair, and control devices from remote locations. In addition, service personnel can manage software and monitor device usage remotely. Companies deploying SAL are able to lower the cost of service while improving device uptime and performance, thus increasing customer satisfaction.

The SAL system is a suite of software products. In this suite of products:

- Applications enable users to gain business insight on device information, by enhancing remote service and support as well as providing new revenue generating activities through preventive maintenance, usage tracking, and software management. The Service application provides tools for monitoring your devices and advanced search capabilities. To do this, the Service application uses algorithms for locating devices based on various criteria, such as data items, patches downloaded to devices (as Packages), accounts, regions, and device conditions.
- The Concentrator Remote Server provides central storage of device data and rules, enabling proactive fault detection and device and access control in a securely managed enterprise environment.
- Agents provide device-level intelligence to connect to valuable data and manage two-way communication within the distributed architecture of the SAL system.
- Transport enables customers, whose devices are not connected to a SAL system during normal operation, to upgrade, perform routine maintenance, and troubleshoot these devices using the Service and Software Management applications of the SAL system.
- Integration and Customization products connect to other enterprise software systems, and enable customization and extension of the SAL system.

Figure 2-1 provides an overview of the SAL system, showing the relationship between the Secure Access Concentrator Remote Server and other components of the system.

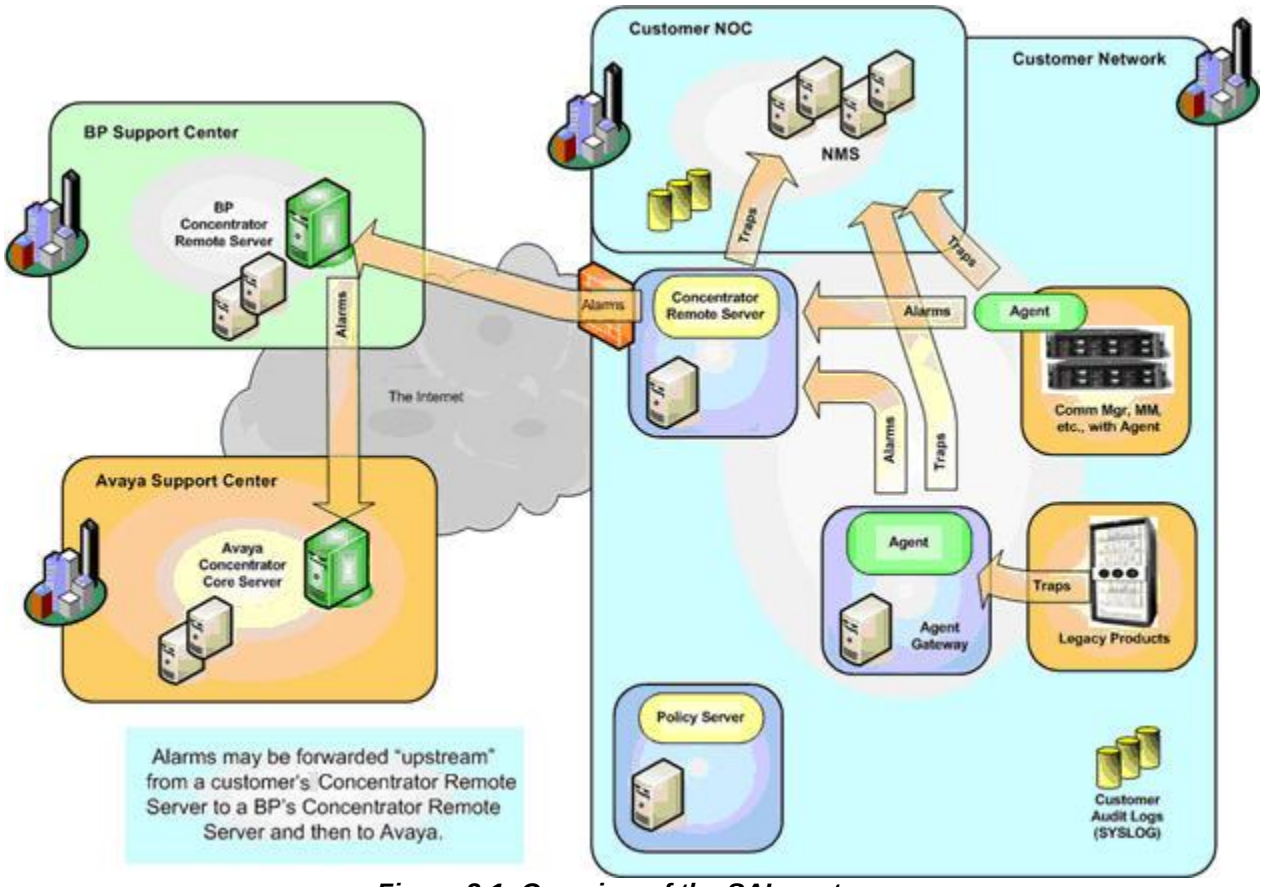


Figure 2-1: Overview of the SAL system

Secure Access Concentrator Remote Server

The Secure Access Concentrator Remote Server is a secure, fault-tolerant application server that enables and manages communication exchange between remote, intelligent devices and your business systems. The Secure Access Concentrator Remote Server collects data from Agents running on intelligent devices through a JBoss application server. It also manages the storage, processing, and retrieval of the data using JDBC connections to an Oracle database.

Applications

Browser-based applications provide user interfaces (UI) to the Secure Access Concentrator Remote Server and its data. You can use these UIs to set up your database of devices and control access to the devices and their data. After the database is set up and devices are sending data to the server, you can log in to the applications and perform a wide variety of tasks. While some applications are part of the base system, other applications require an additional license. The complete set of applications includes:

Access	This base application provides support for remote sessions. The Access application keeps track of current remote sessions, and from its Session Audit page, you can search for sessions and view details about them.
Administration	You can use the Administration application to find and view users currently defined in your directory service system. Through the User tools, you can manage user authentication for, and access to, the SAL system. Through the User Groups tools, you can view, modify, and delete information associated with user groups. Use the User Group tools to assign users, user groups, privileges, device groups, data item groups, accounts, regions, and functional locations to user groups. You can also delete user groups. Administration application provides additional tools to search through auditing records for all of your applications, to view and delete information associated with Remote Access sessions, and to view, add, modify, and delete roles, device groups, and data item groups. In addition, you can set the default properties of newly registered devices and view the current configuration settings for the system.
Avaya Dashboard	You can use the Dashboard application to create, view, and manage dashboards. A dashboard can be created using a variety of Web-based objects, such as hyperlinks and images, as well as Report objects. For more information about this application, see *Report Pack: Dashboards Reference Guide*.
Avaya Report	There are three levels of users for Cognos reports: Consumer, Power User, and Administrator. In addition, there are two levels of features: Reports and Ad Hoc Queries. Consumer users can schedule, run, and view reports. Power Users have all the privileges of Consumer users. In addition, they can edit existing

	reports, add new reports, and create Dashboards if you purchase these features. Administrators can view and generate existing reports, schedule them, edit schedules, and control access to reports and dashboards. The SAL system ships with a set of standard reports that are available to Consumer users. See *Report Pack: Standard Reports Reference Guide* for details about these reports. For information about the query objects available for creating reports and dashboards, see *Report Pack: Query Objects Reference Guide*.
Device	This base application provides asset management tools for defining business rules that convert device data into actions. You can define business rules for device availability. Business rules comprise the conditions to evaluate, and one or more associated operations to perform on the related device or within the database. These operations are called actions. For example, event rules determine if a specified event occurred on the device, and registration rules determine if a specified device registers with the server. Actions are defined to notify users or other systems to take action. For example, a rule could be configured to evaluate if a device becomes unavailable and, if so, notify service personnel to take corrective action (the action).
Service	Use this base application to search for devices using algorithms to display a list of devices based on criteria, such as actions, data items, patches applied, and more. After you have located a device, you can display its Device dashboard, where you can view and react to data, and events sent from devices. From this dashboard, you can start a remote session with the device to diagnose and troubleshoot problems. You can also upload log files from the device or download software upgrades to the device from this dashboard. The links in this dashboard provide access to the Preventive Maintenance applications (if you have purchased the licenses for these applications).
Software Management	By creating *packages* with this application, you can upload files from devices, download files, including new versions of software, to devices, and run applications and scripts on devices to perform routine maintenance.
Preventive Maintenance	For service organizations providing periodic service to perform preventive maintenance, this separately licensed application provides tools to schedule preventive maintenance based on mean failure rates of components and on the usage of computers at customer sites. The application tracks the operation of computers against preset time intervals and machine cycles. Pages for searching for devices and scheduled maintenance information for devices as well as notification rules can help your service organization track computer operation and more effectively schedule preventive maintenance calls.

Usage	This separately licensed application is designed to help you track the frequency and volume of use that devices are experiencing in the field. The application abstracts raw device data into a set of higher-level, business-oriented data. You can filter and group data by device, account, functional location, and so on. The pages of the application display the frequency or volume for particular usage items for particular devices. From these pages, you can flexibly filter and aggregate usage information, display billing estimate information, graph, export, and print the data.

Partner login sessions

Partner login supports limited and monitored access to the Avaya applications by accounts, groups, customers, and so on, that have an interest in one or more deployed SAL devices, but that are not *true* applications users. A partner may be the support account for your device. Occasionally, this partner would need access to the Avaya Applications to remotely manage, troubleshoot, or repair your devices.

True Avaya applications users are defined in SAL user groups that have been created in the SAL directory service. They have their own applications login accounts and privileges granted through the user group settings. *Partners* are defined in a secondary directory service (outside SAL) and given limited access to Applications. Each partner has an associated user group and that user group is created automatically by the server in the directory service defined for partner login accounts. The partner user group is not exposed to the Applications administrator or user.

For example, through Case Management you can create a case and assign it to a partner. The server sends the case information to the specified partner. Part of the information sent includes a session code that provides the partner's contacts with privileges and access to the Applications. Partner contacts cannot log in to the Applications until they receive the session codes and SAL URLs for the devices to be managed. Each partner contact logs in and then provides the session code created for the session. Partner contacts are restricted by the amount of time they can use the Applications, and the actual tools they are permitted to use.

When assigning the case, only partners associated with user groups defined in the directory service for partners are available for assignment. A contact of that partner can log in to the application to use its tools and information.

See the Applications Help for more information.

Data sources for Secure Access Concentrator Remote Server

Agents, which include Connector and Gateway, are application servers that can be run on or embedded in intelligent devices. Agents provide configurable software modules, designed to enable intelligent devices to communicate over the Internet. Agents and the Secure Access Concentrator Remote Server communicate through the Internet.

The Agents send data up to the Secure Access Concentrator Remote Server, which in turn can write data back down to the agents. The Agents running on the devices initiate all communication between devices and the Secure Access Concentrator Remote Server. When an Agent sends a message to the Secure Access Concentrator Remote Server, the response

message carries information from the Secure Access Concentrator Remote Server to the agent.

Note:

Any source can send data to the Secure Access Concentrator Remote Server using XML protocol. For more information, contact Avaya.

Supported server configurations

The Secure Access Concentrator Remote Server runs on a JBoss application server (JBoss Enterprise Application Platform) with a Web Server component. For the purposes of using SAL, think of the Secure Access Concentrator Remote Server and your JBoss application server as a single application server.

You set up the Secure Access Concentrator Remote Server with your JBoss server to operate as a standalone server that can handle hundreds of devices.

The following diagram in Figure 2-2 illustrates and example of a server configuration for the SAL system. In the diagram, a single computer system runs all the main components. For the best performance, Avaya recommends that you configure the system such that the database is on a different server. The following diagram in Figure 2-2 shows an example of a server configuration.

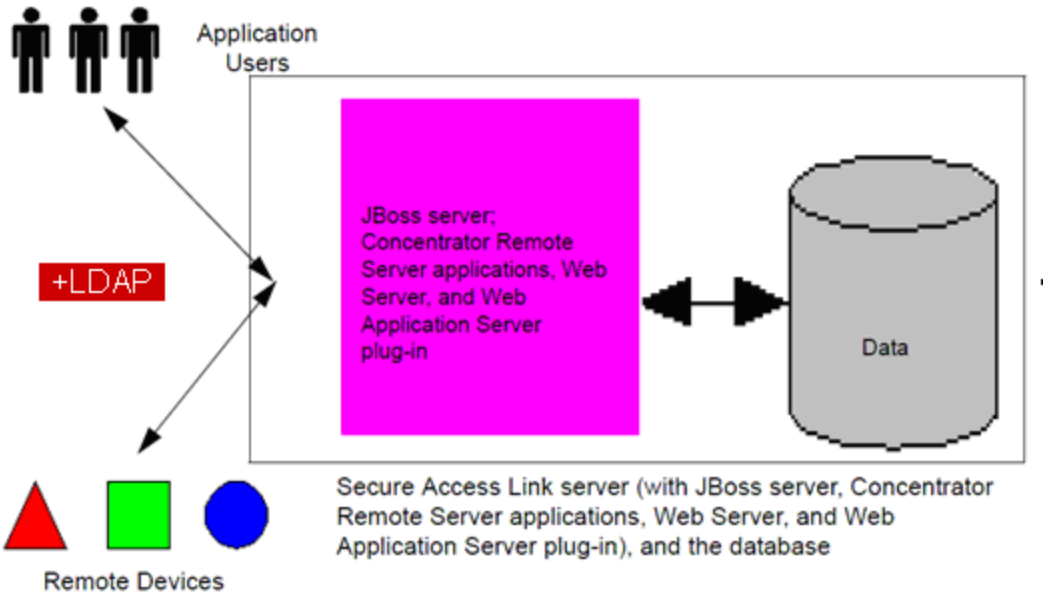


Figure 2-2: Sample SAL Server Configuration

The Web server, JBoss Enterprise Application Platform server, and the Oracle database software must be purchased separately from the SAL system. You will also need the appropriate plug-in to your JBoss server for the Web server.

What is new in Concentrator Remote Serve release 2.0

Secure Access Concentrator Remote Server release 2.0 is built on its previous release and has the following new feature.

CA certificate refresh

Avaya periodically releases Certificate Authority (CA) certificates packages for all SAL components to avoid any service interruption that might occur due to CA certificate expiration. You can download the latest CA certificate package, delivered by Avaya as a zip file, from the repository of the Secure Access Concentrator Core Enterprise Server, and import the new certificates to the Concentrator Remote Server truststore.

SAL release 2.0 provides you a Certificate Refresh patch that you need to install in the computer where the Concentrator Remote Server is installed. This patch creates the CACertificateRefresh directory under the Concentrator Remote Server installation directory and places the importCertificates script in the directory. You have to run this script to import the certificates to the truststore.

Considerations for setting up the server

To determine how to set up the server, you first need to consider how the server will be used. How many users and devices does the server need to support? How much data do you expect to gather and at what regular intervals? How much data do you need to keep in the system and for how long? Based on your answers, how do you want to configure your system?

When selecting a platform for the Secure Access Concentrator Remote Server, keep in mind that you must install the JBoss server on the same computer as the Concentrator Remote Server.

Avaya has tested the JBoss server with the Secure Access Concentrator Remote Server on the Linux platform. The Secure Access Concentrator Remote Server provides a fully functional, J2EE-compliant (Java 2™, Enterprise Edition) platform. An Oracle relational database stores the data and is integrated with the Secure Access Concentrator Remote Server through JDBC connections made using the JBoss server.

Hardware and software requirements

For the requirements of a specific release of the Oracle database software, see the Oracle documentation. In general for better performance, the database software should be installed and maintained on a computer separate from the Secure Access Concentrator Remote Server and the JBoss application server. For details about using the Oracle database with the SAL system, see the documentation for the Oracle Database reference specific to the version you are using. For details about installing the Oracle database software and creating a database, see http://www.oracle.com/technology/documentation/index.html. For information about setting up the database, see Configuring the Oracle database.

The following tables list the hardware and software requirements for running the Secure Access Concentrator Remote Server and the JBoss application server. You should also study

the requirements for your application server and your version of the Oracle database for more details.

Hardware Requirements		
Component	**Minimum**	**Recommended**
Web Server	1 CPU; 1 GHz 1-GB RAM 40-GB drive	
Application Server	2 Xeon processors (separate or dual-core processors) 4-GB RAM 80-GB free disk space	
Database Server	1 CPU; >2 GHz 2-GB RAM 80-GB drive SCSI RAID array OR attached storage using RAID OR a Storage Area Network (SAN)	Dual processor
Service Intelligence Server (Reporting)	1 CPU; >2 GHz minimum 1-GB drive 2-GB RAM	It is recommended that a separate server is used when the Report or the Dashboard applications have been purchased.
Storage	Attached storage for database	
Routers and Firewalls	Additional hardware for network connection and security.	
Network Connection	100-Mbps NIC	

Software Requirements		
Component	**Software and Version-Minimum**	**Hardware**
Operating System	Windows XP SP2 and later	X86 (32-bit)
	Red Hat Enterprise Linux release 5.0-5.4	X86 (32-bit)
Web Server	Apache 2.0.42 and later	X86 (32-bit)
LDAP Directory Server	Microsoft Active Directory	X86 (32-bit)
	Sun ONE (iPlanet) 5	X86 (32-bit)

Application Server	JBoss EAP 4.3	X86 (32-bit)
Database Application	Oracle 10g™ 10.2.0.4**	X86 (32-bit) X86-64*
Web browser	Internet Explorer 6.0 and 7.0, Mozilla Firefox 3 and later.	

Where the asterisk indicates:

- * Contact Oracle for details regarding support and configuration for 64-bit operating systems.
- **Avaya recommends that you must routinely apply Oracle security patches.

Notes:

- Oracle Standard Edition is the minimum software edition required.
- Oracle Enterprise Edition is required for high volume systems with data sets exceeding 250M rows.
- Oracle 10g RAC (Real Application Clusters) Edition is required for high availability configurations.

Network Requirements		
Component	**Minimum**	**Recommended**
Network	100-Mbps LAN connection	Host computer should be DNS registered and should have a valid host name and show the fully qualified domain name (FQDN).
Connections	• Between the Secure Access Concentrator Remote Server and database computers • Between the Secure Access Concentrator Remote Server and Cognos 8 Report server • Between the Secure Access Concentrator Remote Server and Internet • Between the SAL Gateway and Internet	

Bandwidth requirement for SAL

When you use SAL as the remote support interface, ensure that the upload bandwidth for customer to Avaya communications is at least 90 kB/s (720 kb/s) with latency no greater than 150 ms (round trip). The specified upload bandwidth ensures that Avaya Global Services can provide remote support effectively by means of SAL.

Tip:

Avaya recommends you to install the Secure Access Concentrator Remote Server and components in the following order: Web server, directory server, Oracle database, JBoss server, SAL (Concentrator Remote Server and Applications), and Cognos 8.

Requirements for large file transfers

If you plan to take advantage of the ability of SAL to handle large file transfers, keep in mind that the operating systems and file systems on the computers running the Concentrator Remote Servers, client computers, and devices must support 64-bit-based file operations.

Multiple directory services

Many companies already use one or more directory services. The Concentrator Remote Server can operate with multiple LDAP authenticators. SAL users can be defined in more than one directory service, and the Concentrator Remote Server will authenticate against each defined LDAP service. Currently, the multiple authenticator feature applies only to a JBoss server implementation with a Sun ONE directory service.

If you do not have an LDAP directory server already in use, you need to purchase the software separately from the purchase of the SAL system and install it.

All access to the SAL system is controlled through an LDAP directory server, so you need to set this up prior to installing the JBoss server and the Concentrator Remote Server. For information on setting up a directory server to run with the SAL system, see Chapter 3, Using a Sun ONE LDAP Directory Server with SAL.

Installation media details

The following components of the SAL system are shipped on the installation CD-ROMs:

- Disk 1:
  - Secure Access Concentrator Remote Server files
  - Application files
  - Deployment Utility
  - Documentation for all of these products
- Disk 2:
  - Report pack files (if purchased and licensed)
  - Cognos 8 Business Intelligence server and report applications (based on license)
- Other disks (if purchased and licensed):
  - Secure Access Policy Server
  - Secure Access Global Access Server
  - Agent Embedded
  - SAL Service Pack (if applicable)
- Connector, Gateway, or alternative data collection software installed on intelligent devices

Registering a Concentrator Remote Server with Avaya

Registering a product with Avaya is a process that uniquely identifies the device so that Avaya can service it. To register the device, the user who configures the device for SAL must notify Avaya Global Support Services, along with the appropriate information. After registration, Avaya assigns a Solution Element ID and Product ID to the device. To support and access your devices correctly, you must use the identifiers provided by Avaya.

A new Concentrator Remote Server that is deployed in your environment must be registered with Avaya using the process described below. The Concentrator Core and Concentrator Remote Servers deployed at Avaya do not accept unregistered devices.

To register a Concentrator Remote Server:

- Send an e-mail message to salreg@avaya.com with the subject line as SALCRS Solution Element Creation. Provide the following information in the body of the message:
    a. Customer name
    b. Avaya Sold-to Number (customer number)
    c. Your contact information, so that Avaya can contact you if there are questions

Avaya uses this information to register your server. When the registration is complete, Avaya sends you an e-mail message with the Solution Element ID and Product ID numbers.

Licensing the SAL system

The SAL system is a licensed product that is protected by contract with the end user. The system includes a licensing facility that limits access to features for each installation. The system will not start up and operate without the presence of a license file, called axeda-license.xml, in the config directory of the Secure Access Concentrator Remote Server installation location. You must place the axeda-license.xml file in the /<Secure Access Link application>/config directory, for example, `../avaya/SAL/CRS/config/axeda-license.xml`.

Note:

Avaya generates licenses for each customer. A license file is required for the system to operate. See Contacting Avaya Technical Support if you need assistance.

The license file contains a list of the features provided by the license and the encoded license data. Certain features may be entirely present or absent, and portions of certain features may be locked or unlocked. If a main feature is enabled, some of its components may be disabled.

Table 2-1 shows the main features and their components that are licensed individually.

Table 2-1 Feature Licensing

Feature	Components
Access	By default, the Access component provides support for the application remote session. The ability to view and use Access sessions from the Device

Feature	Components
	dashboard (Remote Sessions module). Remote Sessions functionality in Administration.
Report Web Admin (1)	Maximum number of named users permitted as Report administrators. SAL permits only one named user for report administration.
Service	Support for the Service application.
Software Management	Support for the Software Management application; also includes support for Software Package-related actions in the Device application and Software Management package deployments in the Device dashboard.
Remote Application	The ability to create and support remote application sessions.
Report	All Report application functionalities, including the Report tab, the ability to create new reports (either ad-hoc or standard), the ability to schedule reports, or modify or delete reports.
Dashboard	All Dashboard application functionalities, including the Dashboard tab, and the ability to create, modify, or delete dashboards.
Report Studio (2)	Maximum number of named users permitted to use Report Studio. SAL defaults to two (2) named users for Report Studio. Can be defined only if the Dashboard component is selected.

The following features of the SAL system are always provided. These features are *not* limited or controlled by the license.

- Asset management, which includes the Device application and its core features for managing product families and devices.
- System administration, which includes the Administration application and all of its features for managing system users, user groups, device groups, and so on.
- Device connectivity, which includes basic device connectivity functionality. Note that the license does affect the number of devices that can register with the system.
- Reliable one-to-one file transfer functionality.

To view license information, you can use the Administration application. The license data may include optional expiration dates, IDs, and count values, as follows:

- Warning Date: When the warning date is reached, the system sends an e-mail message to the system administrator defined in the DRMConfig.properties file. In addition, a warning is printed to the console at startup.
- Cutoff Date: When the cutoff date is reached, the system sends an e-mail message to the system administrator defined in the DRMConfig.properties file. In addition, if the server is running, it exits immediately. If the server is not running, it will not start up after the cutoff date.
- Data Center ID: Identifies this data center, if applicable.
- Number of CPUs: Identifies the CPU restrictions for this Concentrator Remote Server, if applicable.

License checking

At startup, the Secure Access Concentrator Remote Server checks the expiration date in the license file. If the expiration date has passed, the system prints the following message to the console, sends an e-mail message to the system administrator, and exits:

```
The license for Concentrator Remote Server for licensee
expired on date. Please contact Avaya for a new license. The
system will now exit.
```

If the warning date has passed, the system prints the following message to the console and sends an e-mail message to the system administrator:

```
The license for Concentrator Remote Server for licensee
will expire on date. At that time, the system will no
longer function. Please contact Avaya for a new license.
```

If the warning and expiration dates have not passed, the system prints the following message to the console:

```
Concentrator Remote Server version licensed to licensee
expires on <date>.
```

Device licensing

The SAL system license includes an optional limit on the number of *devices under management*. A *device under management* is defined as a device in the database that has not been deleted. The license can specify a warning limit and a cutoff limit, as follows:

- Warning limit: When the warning number of devices is reached, the system sends an e-mail message to the system administrator defined in the *DRMConfig.properties* file. In addition, a warning is printed to the console at startup.
- Cutoff limit: When the cutoff number of devices is reached, the system sends an e-mail message to the system administrator defined in the *DRMConfig.properties* file. In addition, a warning is printed to the console at startup. Users cannot create any more devices.
- If a new device attempts to register, the registration will fail.
- If a user attempts to create a new device from the Device application, the device creation will fail with an error to the user.

Whenever the system tries to add a new device to the database, it checks the number of devices allowed. If the number of devices under management is greater than the limit allows, the system prints the following error message to the console, sends an e-mail message to the system administrator, and does not create the device:

```
The license for Concentrator Remote Server permits only units devices
under management. An attempt to add a new device has failed. Please
contact Avaya for a new license.
```

If the number of devices under management is greater than the warning limit, the system prints an error message similar to the following to the console, sends an e-mail message to the system administrator, and creates the device:

```
The SAL System currently has number devices under management; the
license only allows units devices. Please contact Avaya for a new
license.
```

License for managed devices vs. Gateway devices

The server licensing provides for two types of remote device support: Gateway devices and managed devices. Gateway devices are devices that are operating as gateways and running Gateway. Managed Devices are remote devices that are managed by gateways. Typically, multiple managed devices communicate through a single gateway device.

The licensing for both types of devices can specify *unlimited* or a specific value, which identifies the maximum number of that device that can be defined in the database.

If there is a specified limitation, the license can specify warning and cutoff values as well. When either a warning or cutoff date is reached, the server generates messages to the Web server console and sends e-mail messages to the system administrator.

Applying a new license

The license generator tool provides the ability to save customer information and the selected applications in an XML file. The name of the XML license file provided from Avaya is in the following format: "<Customer field>-<Server Type field>-<Version field>-avayalicense.xml". For example a license of: "**ACME-Production-SecureAccessLink1_5-avayalicense.xml**" would identify a SAL version 1.5 production server license created for the ACME company.

Before the license can be applied to the server (and the server started), it must be renamed to **axeda-license.xml**.

Updating the license

From the System Configuration: License page of the Administration application, you can view the currently loaded license for the server. In addition, you can reload the license after you install a new or updated license for the server. The operations of the server and Applications are not affected, and the new license and its components appear in the Administration application.

Chapter 3: Using a Sun ONE LDAP Directory Server with SAL

About this chapter

This chapter explains the configuration steps required so that the SAL system can use your Sun ONE LDAP server for user authentication. After you configure your Sun ONE LDAP server, SAL system administrators can make changes to users and user groups in the Sun ONE database through the Administration application. This chapter assumes that you have purchased your Sun ONE LDAP Directory Server software separately and can use the documentation provided for installation instructions.

Note:

The SAL system supports other directory servers for user authentication. Contact Avaya for details.

This chapter contains the following sections:

Support for Sun ONE LDAP provides a brief introduction to the support for Sun ONE LDAP in the SAL system.

Overview of authentication explains the two levels of authentication in the SAL system. It also explains the secondary directory server that SAL supports for Partner Login.

Important steps for successfully using an LDAP Directory Server lists the steps you must take to ensure that your LDAP Directory Server works with your Secure Access Concentrator Remote Server.

Using the LDAP tool to set up SAL users explains what you need to do using an LDAP administrative tool to set up users and user groups for the SAL system.

Help for users new to Sun ONE Directory Servers provides more information for users new to using LDAP. This section explains how to locate information needed for configuring security and for editing SAL system properties so that LDAP authentication works properly.

Preparing the system to use LDAP explains the steps that you need to take as you install the remaining components of the SAL system to enable the use of the LDAP directory server for authentication of users logging in to the system.

Changing the port value for the LDAP Directory Server explains the procedure you need to follow should you need to change the port value for the LDAP directory server.

Enabling SSL encryption for Sun ONE/iPlanet Servers explains how to install and configure SSL support for Sun ONE or iPlanet servers.

Support for Sun ONE LDAP

Directory services provide a central repository for storing and managing identity profiles. The SAL system uses the information stored in the repository for authentication and authorization and to ensure secure access to its components, including Applications. The SAL system currently supports the Sun ONE implementation of LDAP (Lightweight Directory Access Protocol) and of SLDAP (Secure Lightweight Directory Access Protocol). LDAP Directory Servers provide a standard means for scalable, flexible authentication within the SAL system. SLDAP provides additional security through the use of SSL encryption for communications with the Secure Access Concentrator Remote Server and the JBoss Server. Use of multiple Sun ONE Directory Servers is also supported.

This chapter provides instructions for using the Sun ONE directory server with the SAL system. Purchase of the SAL system does not include an LDAP directory server. You must purchase an LDAP directory server separately. You may also want to see the documentation for the administration application of your application server for details on configuring it to use the Sun ONE Directory Server.

Overview of authentication

Two levels of authentication are performed within a SAL system:

- Authentication at the Web Application Server level. The JBoss Server provides this level of authentication to verify the user name and password of an identity profile. This level provides local authentication for the JBoss Server itself.
- Authentication at the Directory query level. The Secure Access Concentrator Remote Server performs this level of authentication when retrieving user and group information from the directory server. This level provides authentication for Applications.

Figure 3-1 illustrates the levels of authentication for SAL.

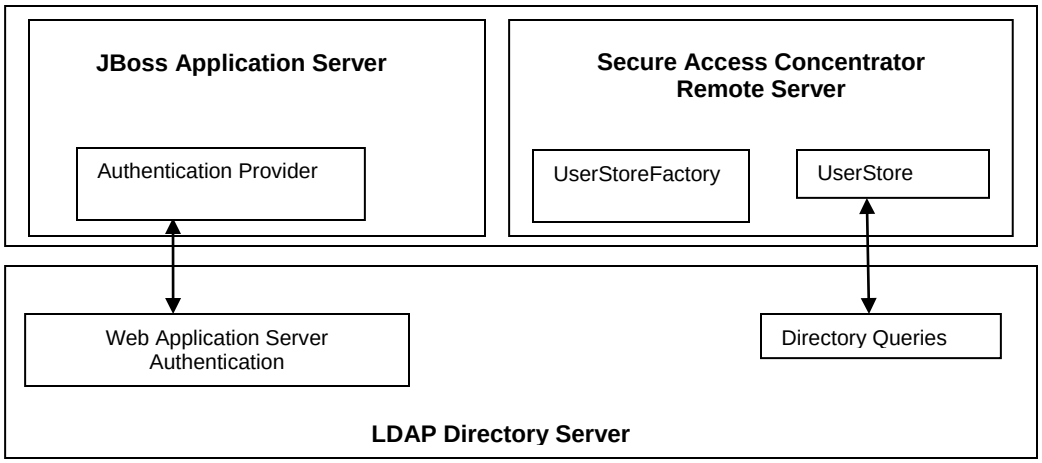


Figure 3-1: SAL System Authentication

Authentication at the Web Application Server level

Web Application Server-level authentication is the first layer of security. The JBoss Server is the application server with a Web server component for the SAL system. Authentication by JBoss Server verifies an entity's identity before completing a connection and protects the JBoss Server environment from unauthorized access. See the documentation for your JBoss Server for details concerning its authentication scheme.

Authentication at the Directory query level

After authentication is achieved at the Web Application Server level, the user name is saved as a session attribute available to Web applications. The Secure Access Concentrator Remote Server uses the user name to query the Directory Server and retrieve the user and group information. To be able to support different Directory Server products, the Secure Access Concentrator Remote Server adopts the *Factory* design pattern. This design pattern defines two authentication adapter interfaces:

- UserStoreFactory interface to instantiate the object that implements the UserStore interface.
- UserStore interface for performing all directory queries.

The full class name for the factory is specified in DRMConfig.properties, which is the configuration file for the Concentrator Remote Server. By default, the class property for the factory is set as follows:

```
com.axeda.drm.userStoreFactoryClass=
      com.axeda.drm.user.LdapUserStoreFactory
```

The default authentication adapter, **LdapUserStoreFactory/LdapUserStore**, is the one you select when installing the SAL software. If you need to change the directory server information after installation, you will need to edit your DRMConfig.properties file using a text editor. For details about this file, see Appendix C: Editing the DRMConfig.properties File.

Configuring LDAP security

Configuring LDAP security entails creating SAL-specific groups, adding users to the various groups, and then assigning to those groups access privileges for the SAL system. The rest of this chapter explains how to configure the groups and user accounts in your LDAP directory server for use with the SAL system. When you install the SAL software (the Concentrator Remote Server and the Applications), you need to know the name of the computer where your LDAP server is running and the number of the port on the computer to use for LDAP authentication. You will also need the configuration information that is available in the section Help for Users New to Sun ONE Directory Servers.

Partner Login directory service

The Partner Login component of SAL supports the use of a secondary directory service. The secondary directory service is not intended to manage a company's global directory, but rather to manage accounts for third-party organizations that need to access the system.

This dedicated, secondary server hosts user groups and user accounts of the partners separately from the main SAL users.

To support the secondary directory server, certain changes in the SAL schema are required in the database. The SAL administrator needs to configure the additional authenticator using the administrative application of your Web Application Server. The authenticator name will be marked as third-party access storage in the SAL configuration file by its name or type.

Important steps for successful use of an LDAP Directory Server

If you are installing the SAL system on an existing network that uses one or more instances of the Sun ONE directory service with a JBoss Server, you can start with Step 2. If you are installing a new directory service, begin with Step 1.

The information presented here applies to any LDAP Directory Server implementation.

1. It is important and essential that the computer that will run the LDAP Directory Server have a fully qualified domain name (FQDN), in the form servername.domain.tld (for example, ldapServer.avaya.com). Therefore, check with your IT department to make sure that they have done this for the new server that will run the LDAP Directory Server.

   If not already done, set this property using the appropriate tool on your Linux machine.

   If the computer does not have a FQDN, the LDAP Directory Server installation program will display this message at the beginning:

   ```
   Warning:
   Installation cannot determine the domain name for this host.
   ```

   If you see this warning, your network settings may not be correct or your host may be on a DHCP network. Also, it helps to ensure that the IP address for the host is static when on a DHCP network.

   If you are using TCP/IP, your domain name must be filled in.

   This warning is correct. Do *not* proceed with the LDAP Directory Server installation until you fix this problem.

2. Complete the installation of the LDAP Directory Server. If you are using the Sun ONE LDAP Directory Server installation program, Avaya recommends the following installation choices:

   - Choose a custom installation, with all of the components selected.
   - Store all entries in the new instance of the directory server.
   - Set the Directory Server Port to 389 or, to use SSL, set the port to 636. While installing the SAL software, specify this port number. The installation program then writes this information to the configuration file for your JBoss server.
   - When prompted by the installation program, do *not* populate with any data.

3. After the LDAP Directory Server has been installed, under the domain to be used by SAL, in the Groups organization, create an 'Administrators' group. In the People organization, create an administrative user name and password for your JBoss

Server in this group. Make sure the passwords you specify are supported by any password length constraints defined in the server configuration. See the DRMConfig.properties file to determine the minimum supported length for passwords. All configuration settings are explained in Appendix C: Editing the DRMConfig.properties File.

4. To the Groups organization, add the groups required for the SAL system, and then add users to the groups. The next section explains this step in more detail.
5. If you want to use SSL for communications with your LDAP Directory Server, follow the instructions in Enabling SSL Encryption for Sun ONE/iPlanet Servers to configure the SAL system to use SSL for communications among the LDAP server, the JBoss Server, and the Concentrator Remote Server.

Using the LDAP tool to set up SAL users

After installing your LDAP Directory Server, you can use its administrative tool to set up the Directory Server database for SAL users and groups. The tasks you need to perform include:

1. Log in to the server as an administrator, capable of creating groups and users.
2. Search for and set up users, groups, attributes, and so forth, to use with the SAL system.
3. Add new entries to the directory (such as a new user or group) and set up to use with the SAL system.

For each user you want to add to the *ServiceLink* groups, do so in the People organization first. You can then add them to the ServiceLink groups.

Keep in mind the following:

- Users in the ServiceLinkAdmins group must also be members of the ServiceLinkUsers group.
- Nonadministrative users who need to modify the LDAP user or user group configuration will need access to an account defined in the ServiceLinkLdapAdmins group.

  Note:

  It is recommended that you configure only one account in this group and then provide that account information to all non-admin users who need to be able to modify LDAP user or user group settings from within Administration. Those non-admin users will need privileges to the Administration application. See Application Privileges for a description of Applications privileges. Users who are members of the ServiceLinkAdmins group but do not have access to the ServiceLinkLdapAdmins user account will not be able to modify LDAP users and groups.
- Users who are defined only in ServiceLinkLdapAdmins and not in ServiceLinkUsers group will not be able to log in to the Applications.

Specifically, you need to:

1. Set up the following groups of users in the Groups organization (ou) in the Directory Server database:

- Administrators group (for the JBoss Server)
- ServiceLinkAdmins group
- ServiceLinkUsers group
- ServiceLinkLdapAdmins group (applies to Sun ONE implementations only).

2. Create two types of users (People ou) in the Directory Server database:
    - AdminUser who is a member of the ServiceLinkAdmins and ServiceLinkUsers groups.
    - A non-Admin user who is a member of the ServiceLinkUsers group or of a subgroup of the ServiceLinkUsers group. (These non-Admin users should not be members of ServiceLinkLdapAdmins group, but rather have access to an account defined in the ServiceLinkLdapAdmins group.)
3. Make the ServiceLinkAdmins group a member of the ServiceLinkLdapAdmins group.
4. In the Administrators group, create the administrative user that is used by the JBoss Server.

Note:

A group must have at least one member (user) for it to appear in the list of Directory Server groups of the Administration application. It is not sufficient that the group contain only a subgroup.

When configuring each user in the Directory Server, specify the following:

- First Name and Last Name of the user.
- Common Name (cn) for the user. The Directory Server uses this name to address the user on logging in.
- UID (User ID). This ID uniquely identifies the person or object defined by the entry.
- Password to associate with the user. Confirm by typing the password again. Make sure that the length of the password you specify is supported by the server's configuration. The password and other configuration properties are explained in Appendix C: Editing the DRMConfig.properties File.
- E-mail address of the user (optional).
- Phone and fax numbers of the user (optional).

For example, a user in the ldap.siroe.com domain might have the following DN:

```
cn=Barbara Jones,ou=Engineering, dc=siroe, dc=com
```

Note:

The SAL system uses the common name (cn), mail, and telephone number properties from the LDAP server.

Help for users new to Sun ONE Directory Servers

As the title indicates, this section is for anyone who is not familiar with Sun ONE Directory Servers (LDAP). The installation program for SAL automatically sets the appropriate properties for the Sun ONE LDAP Directory Server, as long as you can provide this information while running the installation program. In addition, when you need to configure

the security realm for your JBoss Server, you will need the following information about the Directory Server:

Field	Description
Host Name	The name of the computer where your LDAP server is running.
Listening Port	The number of the port you are using for LDAP authentication.
Directory Server Principal DN	The SAL specific information from your LDAP directory server for the uid (the user name that you use to log into the LDAP server as the administrator), ou's, and o.
Directory Server Principal Password	The system password for accessing the LDAP server. This is the password for the LDAP administrator specified in the Principal uid parameter.

User Base DN	The information appropriate to your directory server setup, as follows:
	• If using an OU:
	`OU=people, DC=company, DC=com`
	Except for `people`, the values shown here are placeholders. You need the actual OU and domain information for your setup.
	• If using the default Users group:
	`CN=Users, DC=machineName, DC=company, DC=com`
	Except for `Users`, the values shown here are placeholders. You need the actual domain information for your setup.

Group Base DN	The information appropriate to your directory server setup, as follows:
	• If using an OU:
	`OU=groups, DC=company, DC=com`
	Except for `groups`, the values shown here are placeholders. You need the actual OU and domain information for your setup.
	• If using the default Users group:
	`CN=Users, DC=machineName, DC=company, DC=com`
	Except for `Users`, the values shown here are placeholders. You need the actual domain information for your setup.

Username Attribute	The attribute of an LDAP user object that specifies the name of the user. For example, for Sun ONE LDAP, you may use the default value, `uid`. For Microsoft Active Directory, you may use the `sAMAccountName`.

Field	Description
Static Group Name Attribute	The attribute of a static LDAP group object that specifies the name of the group. For example, for Sun ONE LDAP, you may use the default value, `cn`. For Active Directory, you may use the `sAMAccountName`.
User From Name Filter	If the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. When running the SAL installation program, you can use the default value for this parameter: `&(uid=%u)(objectclass=person))`
Group From Name Filter	An LDAP search filter for finding a group given the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. When running the SAL installation program, you can use the default value for this parameter: `(|(&(cn=%g)(objectclass=groupofUniqueNames))(&(cn=%g)(objectclass=groupOfURLs)))`

The section below first explains where to locate the required information so that you can set up authentication for the SAL environment more easily. The next section then explains how to get started when adding the users and groups for the SAL system using the Sun Java System Server Console application. It is assumed that a Sun ONE LDAP Directory Server is already installed and that you have access to the Sun Java System Server Console application.

To find information for configuring security

1. Start the Sun Java System Server Console application (`startconsole.sh`).
2. On the **Servers and Applications** tab, expand the node that shows the name of your directory server computer. Using the computer name, ldapServer.avaya.com, expand the node as follows:

   ```
   ldapServer.avaya.com > Server Group > Directory Server
   ```

3. When the information about your Directory Server appears in the right pane, click **Open**.
4. Click the **Directory** tab to display it.
5. In the left pane of the **Directory** tab of the Sun ONE Directory Server application, select **o=NetscapeRoot > TopologyManagement > Administrators**. You are going to locate the information for the Directory Server Principal (DN and Password).
6. In the right pane, right-click the username, **admin**, and select **Edit with Generic Editor**. The Generic Editor dialog box appears, showing the full name assigned to the administrator at the top.

Figure 3-2 shows an example of this dialog box.

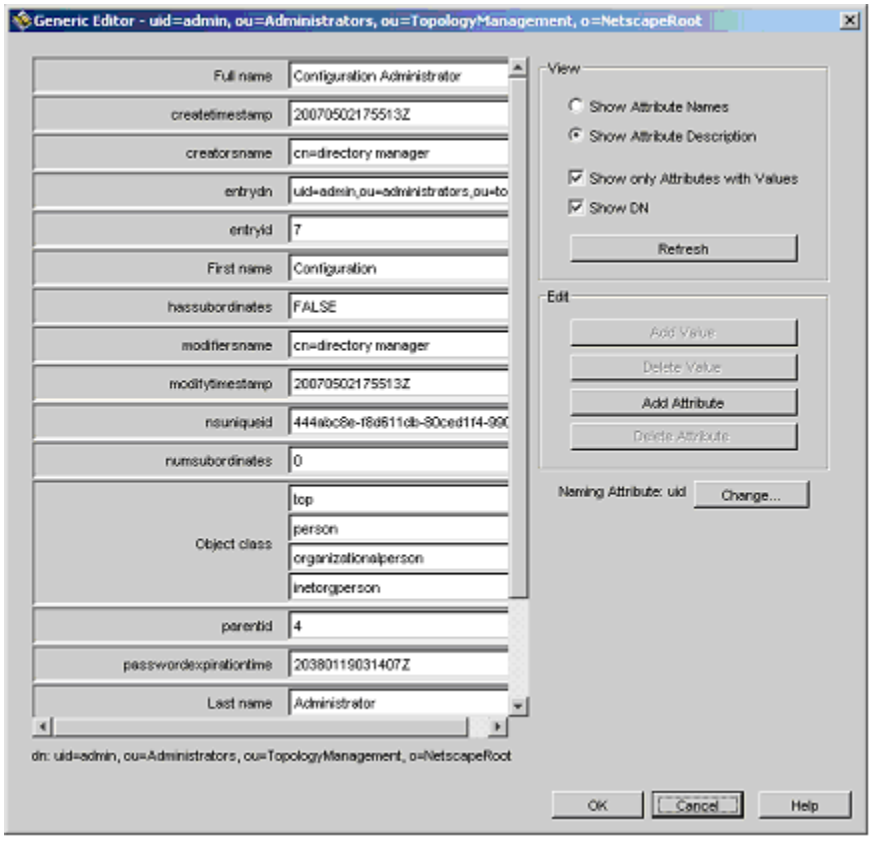


Figure 3-2: Generic Editor – Admin

7. Locate the **entrydn** property, as shown in Figure 3-2, and copy its content to an empty text file (for example, open Notepad and paste the content of entrydn to the Notepad file). Using this example, you would copy the following information from this field:

   uid=admin,ou=administrators,ou=topologymanagement,o=netscaperoot

8. Click **Cancel** to close the Generic Editor dialog box. Next you are going to locate the information for the User Base DN.
9. In the left pane of the **Directory** tab, click **dc=axeda,dc=com** to display its components in the right pane.
10. In the right pane of the **Directory** tab, right-click **People**, and select **Edit with Generic Editor**. The Generic Editor dialog box for the selected organization (People) appears, as shown in Figure 3-3.

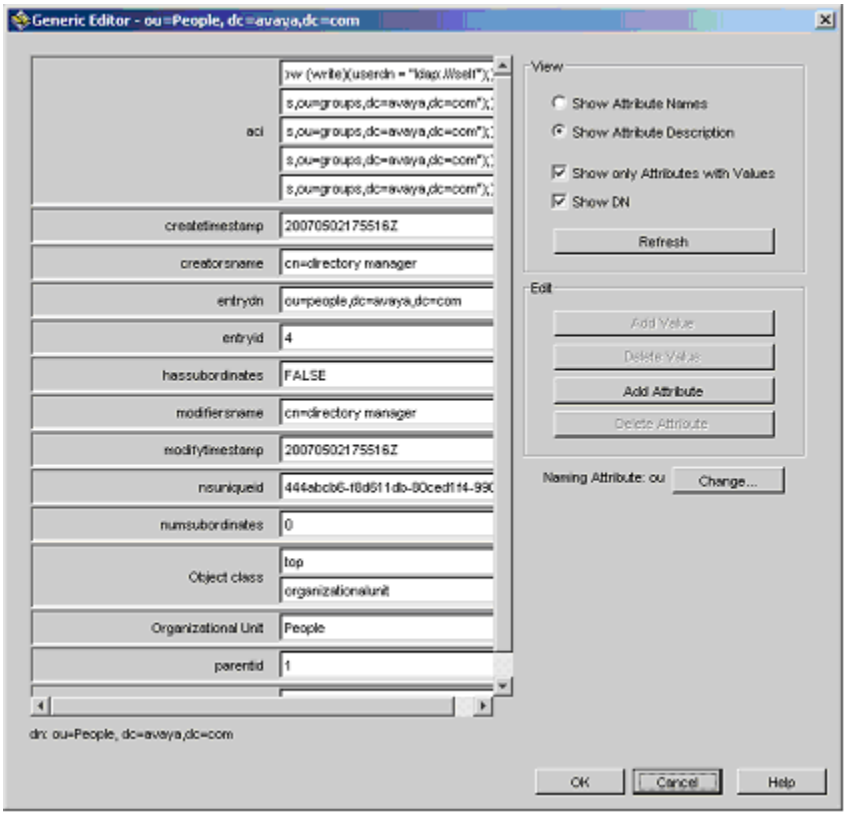


Figure 3-3: Generic Editor - People

11. As shown in Figure 3-3, copy the information in the **entrydn** field and paste it in your Notepad file. In this example, the information is `ou=people,dc=avaya,dc=com`. You will need this information to configure the **UserBaseDN** field when you run the SAL installation program.
12. Click **Cancel** to close the dialog box. Next, you are going to locate the Group Base DN information.
13. If necessary, in the left pane of the **Directory** tab, click **dc=avaya,dc=com** to display its components again in the right pane.
14. In the right pane, right-click **Groups**, and select **Edit with Generic Editor**. The Generic Editor dialog box for the selected organization (Groups) appears, as shown in Figure 3-4.

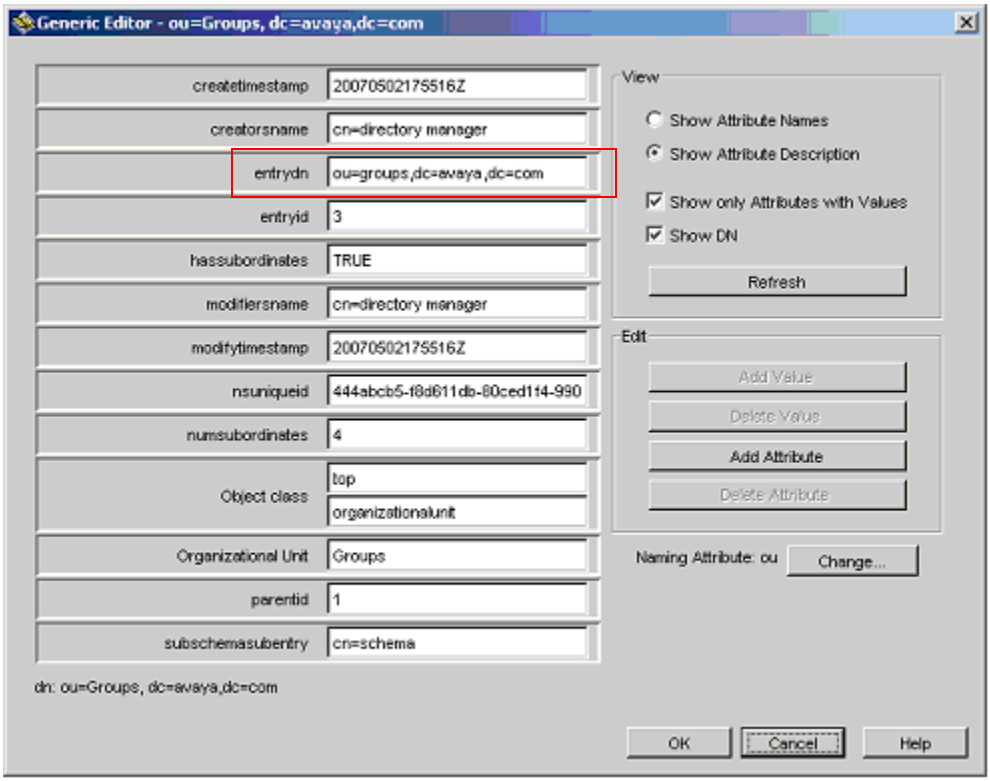


Figure 3-4: Generic Editor - Groups

15. As shown in Figure 3-4, the information you need to copy and paste in the Notepad file is in the **entrydn** field. Using the example shown here, you would copy `ou=groups,dc=avaya,dc=com`. You will need this information to configure the **Group Base DN** when running the SAL installation program.

To configure users and groups for SAL

1. If it is not running, start the Sun Java System Server Console application (`startconsole.sh`).
2. On the **Servers and Applications** tab, expand the node that shows the name of your directory server computer. Using the computer name, ldapServer.avaya.com, expand the node as follows:

   `ldapServer.avaya.com > Server Group > Directory Server`
3. When the information about your Directory Server appears in the right pane, click **Open**.
4. Click the **Directory** tab to display it.
5. In the left pane of the **Directory** tab, click the node, **dc=avaya,dc=com**.
6. In the right pane, right-click the **Groups** organization, and select **New > User** or **New > Groups** to add each required user or group for SAL. Follow the instructions in the section, Using the LDAP Tool to Set Up SAL Users, to make sure that you create all the required users and groups for SAL.

The installation program for SAL automatically sets the appropriate properties for the Sun ONE LDAP Directory Server, as long as you have provided this information while running the

installation program. If you experience any problems, see the documentation for the JBoss Server for information about changing the security realm or authentication configuration and to Appendix C: Editing the DRMConfig.properties File for information about configuring the appropriate LDAP-related properties for the Concentrator Remote Server.

If you want to use SSL for communications among your LDAP Directory Server, the JBoss Server, and the Secure Access Concentrator Remote Server, see Enabling SSL Encryption for Sun ONE/iPlanet Servers for instructions.

Preparing the system to use LDAP

After setting up LDAP users and groups, you need to install the JBoss Server and the Secure Access Concentrator Remote Server. After these installations are complete, you must perform additional configuration steps to ensure that the LDAP directory server provides the desired access to the SAL system. These configuration steps are explained in detail in the appropriate chapters. The following summary describes each step and the chapter that explains the step:

- When installing the Secure Access Concentrator Remote Server, you will need to enter the LDAP server URL and volume as well as the port, administrative search, peoplesearch, and groupsearch properties. The SAL installation program sets these properties based on your entries during installation. If you want to use SSL for communications between the Concentrator Remote Server and your LDAP Directory Server, make sure you enter the appropriate information while running the installation program for the Concentrator Remote Server. Refer also to Enabling SSL Encryption for Sun ONE/iPlanet Servers for instructions to complete the configuration (and installation of certificate files) for SSL. If necessary, see Appendix C: Editing the DRMConfig.properties File for assistance in verifying that the information is correct or in adding a secondary directory server to support Partner Logins.
- When all the server installations are complete, you will need to log in to the SAL system as an administrator and use the Administration application to set up user groups and privileges. You can assign user groups to device groups, data item groups, and reports. When creating packages using the Software Management application, you can assign user groups to individual packages. The Secure Access Concentrator Remote Server uses this information to display or hide device groups, data item groups, reports, packages, and so on for each authenticated user.

  Because the Secure Access Concentrator Remote Server itself performs all the database transactions, you need to set up users, groups, and permissions for the application side only. The Secure Access Concentrator Remote Server works in conjunction with your JBoss Server to deliver Applications to your Web browsers, so you can take advantage of its security features to link into your LDAP service to provide security for your Secure Access Concentrator Remote Server.

Note:
You can change the user and group information stored in a Sun ONE LDAP database from the Administration application. When you attempt to make changes, you must log in with an authorized user name and password for the LDAP Directory Server. If you delete a group using the Administration application, it will also be deleted from the Sun ONE LDAP database.

How authentication works

Applications implement form-based authentication. The application user needs to type a valid user name and password in a secure login page, and submit that information to the Secure Access Concentrator Remote Server for approval. The server matches the user name and password against the information configured in the LDAP database and, for approved users, determines the groups in which the users are defined. Based on the privileges that you assign to the group (Administration application), the Secure Access Concentrator Remote Server displays or hides applications or specific features of applications for an authenticated user.

Application privileges

Within the Administration application, privileges are assigned to specific user groups on the page called Add and remove application privileges for *user_group_name*. These privileges specify what the users in those user groups can do within the applications, including which operations they can perform and which pages or tools they can use or view. For example, the ability to run searches or view the results of database searches is controlled by privileges.

When creating packages using the Software Management application, you can use the Package wizard to select the user groups who has the View and Deploy or the Modify and Delete privilege to the package. In addition, when creating a new action using the Device application, you can assign the privilege to execute the action to user groups independently of assigning the privilege to edit the action.

Application information you can "see"

In addition to security settings, user group configurations created in the Administration application define what information users can view in the various applications and pages to which they have access. The ability to view devices, data from devices, reports, Service application pages, and so forth, is controlled by the privileges set for the corresponding user group.

For example, if User Group A has access to Device Group A, then all users defined in User Group A can see all data for all devices in Device Group A. (User groups are activated on the Create a new User Group page in the Administration application.) This also means that any search or report will only show data or devices or product families to which the logged in user has access.

You can associate the following with the user groups:

- Privileges. The abilities to view and manipulate data from devices are selectable on a group basis. In addition, you can define what the users in the group can do with the various applications. For example, you may want a user group to have access to the Service application only.
- Device Groups. Devices defined in a particular device group can be *seen* only by the users defined in a user group assigned to the device group.
- Data Item groups. Data items defined in data item groups can be seen only by users defined in associated user group. This is another level of security for the device level. In addition, only data items configured with the *Visible* attribute can be seen in any of the applications pages.

Changing passwords and e-mail addresses in the Directory Server database

After you log in to the Secure Access Concentrator Remote Server system, you can use the Preferences option to modify your password and e-mail address.

1. In the upper-left corner of the window, click **Preferences**.
2. On the User Preferences page, click **Edit User Attributes**.
3. On the Update Your E-mail Address and Password page, type your new e-mail address, and press **Tab**.
4. Type your new password and confirm it.
5. Type your current password, and click **Submit**.

If you type a valid current password, the system returns you to the User Preferences page, and presents the message, "Your attributes were updated successfully."

Searching the Directory Server database

From the Administration application, you can search the Directory Server database exclusively for groups within the ServiceLinkAdmins group and ServiceLinkUsers group. Rather than finding all groups containing users who in some way belong to the ServiceLinkAdmins or ServiceLinkUsers group, the search finds only the groups that are explicitly members of these groups. This search will check for a group being a subgroup of itself, preventing infinite recursion.

You can also query the Directory Server using a group's `cn` or a user's `uid` so that you can find organizational units nested within the starting/top-level group and people `ou`'s.

Note:

A user is an administrator only if the user belongs directly to the ServiceLinkAdmins group. You cannot make an entire group ServiceLink (SAL) administrator by just placing the group in the ServiceLinkAdmins group.

Changing the port value for the LDAP Directory Server

To change the port for the LDAP Directory Server using the Sun Java System Server Console

1. Start the Sun Java System Server Console application (`startconsole.sh`).
2. On the **Servers and Applications** tab, expand the node that shows the name of your directory server computer. Using the computer name, ldapServer.avaya.com, expand the node as follows:

   ```
   ldapServer.avaya.com > Server Group > Directory Server
   ```

3. When the information about your Directory Server appears in the right pane, click **Open**.
4. Click the **Configuration** tab to display it.

5. In the right pane of the **Configuration** tab, click the **Network** tab. An example of this tab is shown in Figure 3-5.

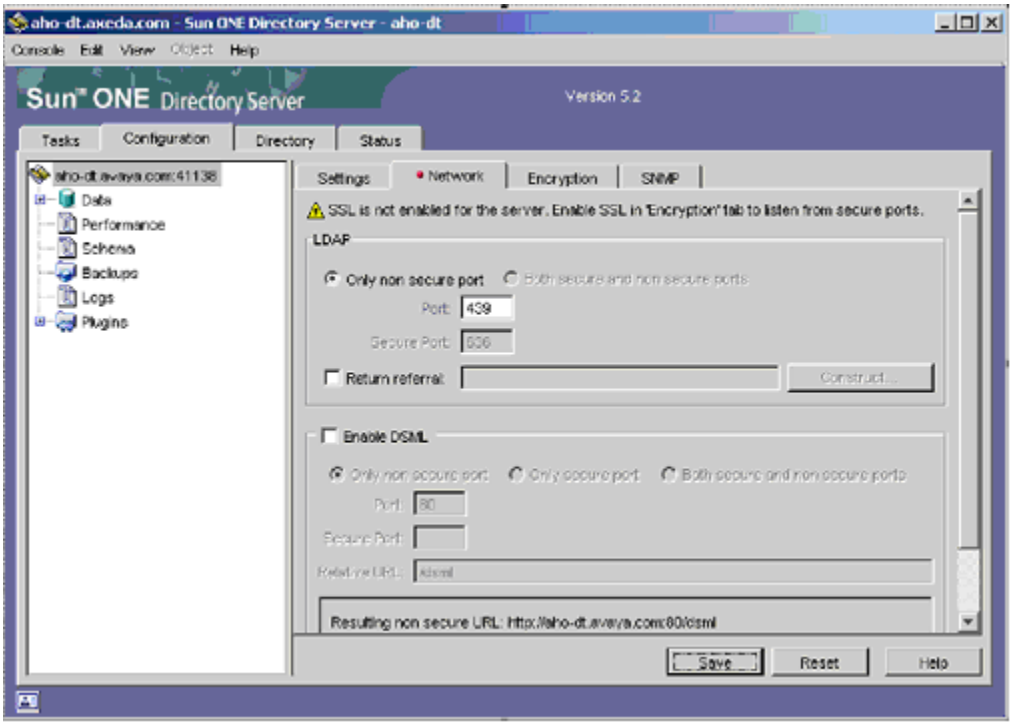


Figure 3-5: Configuration | Network tab for the Directory Server

6. On the **Network** tab, change the current port number to 389.
7. Click **Save**. The Confirmation screen shown in Figure 3-6 appears. These steps are repeated after the screen, so you do not need to write them down.

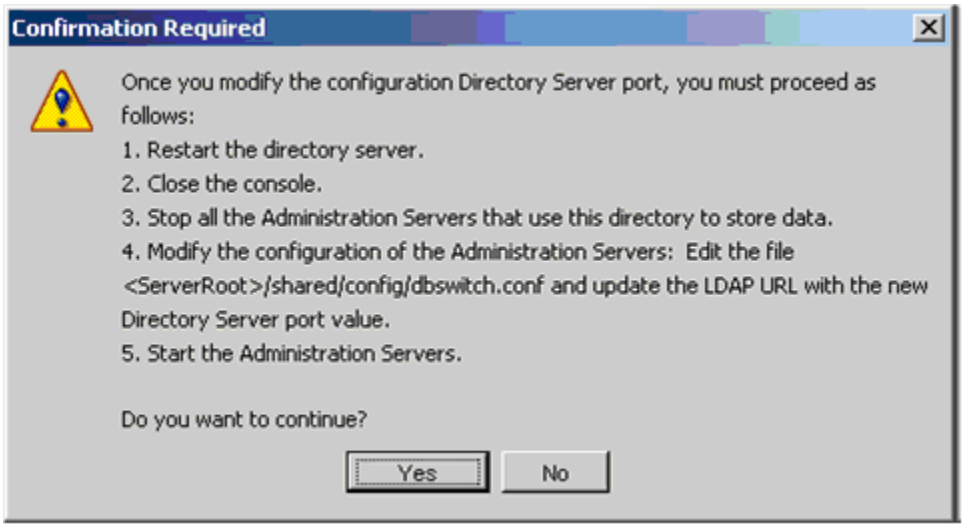
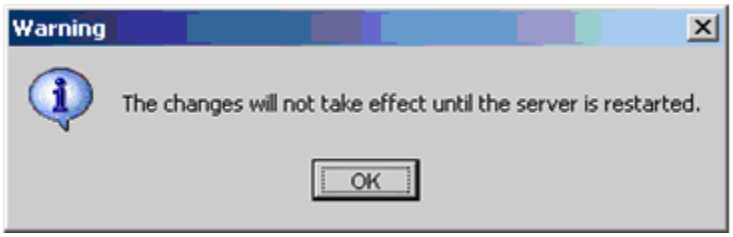


Figure 3-6: Confirmation prompt

8. Click **Yes** to continue or **No** to cancel the change of port number. If you select Yes, the following warning message appears:



As instructed in the Confirmation prompt, complete the change by taking the following steps:

1. Restart the Directory Server.
2. Close the Console application.
3. Stop the Administration Servers that use the directory to store data.
4. For each Administration Server, edit the file `/<ServerRoot>/d/config/dbswitch.conf` and update the LDAP URL with the new Directory Server port value.
5. Start the Administration Servers.

Enabling SSL encryption for Sun ONE/iPlanet Servers

The Secure Access Concentrator Remote Server and the Agents support SSL encryption. By default, SSL is enabled in the configuration of the server and agents. This section explains how to set up the Sun ONE/iPlanet LDAP server and the JBoss Server to support SSL for use with your SAL system.

Note:

If you are switching from non-SSL to SSL for communications with the Concentrator Remote Server, make sure that your LDAP server is working properly with the Concentrator Remote Server before making the change.

To start the Sun ONE directory server

1. Open the Sun ONE Server Console application (or iPlanet Console 5.0)
2. Expand the Tree View for the desired domain (that is, the LDAP server) until the **Directory Server** item is displayed.
3. Right-click **Directory Server** and from the context menu, click **Open**.
4. Click the **Tasks** tab.
5. Click **Manage Certificates** to open the Manage Certificates dialog box.
   - If you are entering this area for the first time, the system prompts you to set a password. Remember this password, as you will need it for all future access to Certificates or server restarts.
   - If you have a password, enter it now.

The next few procedures assume that you are running the Console application for your Sun ONE or iPlanet directory server.

To generate a certificate request

1. Click the **Server Certs** tab.
2. Click **Request** to start the Certificate Request wizard.
3. On the Introduction page of the wizard, click **Next**. This page is the first of four pages (1 of 4).
4. Enter the information on the Requestor Information page (2 of 4).

   Note:

   The "Server name" is the name of the computer that is running the LDAP server, as it appears in the Tree View of the Sun ONE Console application.
5. To display the Token Password page (3 of 4), click **Next**.
6. Type the server password, and click **Next** to display the last page (4 of 4).
7. Click **Copy to Clipboard**.
8. Open Notepad, and from the **Edit** menu, click **Paste**.
9. If the file contains any blank lines, remove them.
10. Save the file as `sunone.cert`.
11. Close Notepad.
12. Click **Done** to close the Certificate Request wizard.
13. Send the `sunone.cert` file to your CA to retrieve a server certificate. Alternatively, if you are using OpenSSL to generate the certificate, see the procedure, To generate a Certificate request.

To install the Server Certificate in Sun ONE

1. Return to the Manage Certificates dialog box. If you need help, see steps 1 through 5 of the procedure To start the Sun ONE directory server. These steps explain how to display this dialog box.
2. To start the Certificate Install wizard, click **Install**.
3. On the Certificate Location page (1 of 4), select **in this local file**.
4. Click **Browse** and then locate and select the server certificate returned by your CA.
5. Back on the Certificate Location page, click **Next**.
6. On the Certificate Information page (2 of 4), review the certificate information to ensure that it is correct.
7. Click **Next** to display the Certificate Type page (3 of 4).
8. To keep the certificate name, server-cert, click **Next**.
9. Enter the Token password (the server password from step 5 of the To start the Sun ONE directory server procedure) and click **Done**.
10. Click the **Server Certs** tab, and verify that the certificate name, server-cert, appears in the list.
11. Click **Done** to return to the main Directory Server page.

To enable SLDAP in Sun ONE

1. Click the **Configuration** tab to display the Directory Server configuration.
2. Edit the port number in the **Encrypted Port** field if desired. The default port is 636 and Avaya recommends that you use this value.
3. On the Configuration page, click the **Encryption** tab.
4. Select the **Enable SSL for this server** check box.
5. Select the **Use this cipher family: RSA** check box.
6. Ensure that the setting for the **Security Device** field is **internal (software)**.
7. Ensure that the **Certificate** listed is the one you just installed, "server-cert."
8. Select **Do not allow client authentication**.
9. Click **Save**.
10. Click the **Tasks** tab to display the list of available tasks for the Directory Server.
11. Click **Restart**.
12. When prompted, type the server password (from step 5 in To start the Sun ONE directory server) to start the Directory Server.

To import the Server Certificate in the JBoss Server

1. Open a DOS command shell.
2. Verify that the JDK bin path is located in your DOS shell command path.
3. Navigate to the location of the JBoss Server Certificate Trusts keystore. You specified this location during the installation of the Concentrator Remote Server. See Appendix C: Editing the DRMConfig.properties File for the value of the com.axeda.drm.remote.server.keystore property defined during installation.
4. Copy the server certificate to a location accessible to the command shell.
5. Run the following command:

```
keytool –import –file <server_certificate_path>
        -alias <unique_name_to_identify_Sun_ONE_server>
        -keystore <Certificate_Trust_File>
        -storepass <Certificate_Trust_File_Password>
```

6. If prompted, confirm the insertion of the server certificate by typing `yes`.

To use SLDAP in the JBoss Server

To configure login-config XML to support SSL

You need to edit the login-confg.xml file provided in the `<JBoss_HOME>/server/<SAL Install>/conf` directory to add support for SSL communications to SAL.

1. Locate the login-config.xml file installed to your JBoss SAL server, within the **conf** directory.
2. Open the file in a text editor.

3. In the file, locate the following alternate LDAP login module within "servicelinkpolicy":

```
com.axeda.drm.jboss.LdapExtLoginModule
```

4. Add the following new SSL module to the login modules:

```
<module-option name="java.naming.security.protocol">ssl</module-option>
```

Note:
For Axeda Partner Login functionality, you may have more than one login module. Add this information to each login module in the login-config.xml file.

The following shows an example of the java.naming.security.protocol module defined in a login-config.xml file; your server would have different settings:

```
<login-module code="com.axeda.drm.jboss.LdapExtLoginModule" flag="required">
         <module-option name="throwEx">true</module-option>
         <module-option
name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory
         </module-option>
         <module-option
name="java.naming.provider.url">ldap://server1.acme.com:636/
</module-option>
         <module-option
name="java.naming.provider.host">server1.acme.com</moduleoption>
         <module-option name="java.naming.provider.port">636</module-option>
         <module-option
name="java.naming.security.authentication">simple</moduleoption>
...
         <module-option name="java.naming.security.protocol">ssl</module-
option>
      </login-module >
   </authentication>
</application-policy>
```

5. Save and close the login-config.xml file.

Now you need to edit the properties.service.xml file to point the JBoss server to the truststore.

To add LDAP keystore to jboss properties.service.xml

You need to point SAL to the truststore. To add the LDAP keystore to the JBoss server, you need to edit the properties.service.xml file provided in the <JBoss_HOME>/server/<SAL Install>/deploy directory. This file allows for the definition of global system properties.

1. Locate the properties.service.xml file installed to your JBoss SAL server, within the deploy directory.
2. Open the file in a text editor.
3. In the file, locate the properties attribute:

```
<attribute name="Properties">
```

4. Add the trustStore information, as follows:

```
<attribute name="Properties">
   javax.net.ssl.trustStore=${jboss.server.home.dir}/conf/my.truststore
   javax.net.ssl.trustStorePassword=mytruststorepassword
```

```
    javax.net.ssl.keyStore=.${jboss.server.home.dir}/conf/my.keystore
    javax.net.ssl.keyStorePassword=mykeystorepassword
</attribute>
```

5. Modify the settings in these lines for your server configuration.
6. Save and close the properties-service.xml.

To generate your own Sun ONE certificate

1. In the file system of the computer running your Concentrator Remote Server, create a directory for the OpenSSL and certificate files.
2. Obtain and decompress the OpenSSL.zip and makecerts.zip files into this directory.
3. Copy the sunone.cert file into this directory.
4. Run the **makecert-sldap** command and enter the information as appropriate. For example, open a Command Prompt window, and change to the OpenSSL directory. At the prompt type:

   makecert-sldap <*server_name*>

   where <server_name> is the name of the LDAP server. This command creates a file using the name of the LDAP server, `<server_name>-cert.pem`.
5. Copy the files <server_name>-cert.pem and SLDAP-CA-cert.pem to the Sun ONE server.
6. Copy the files <server_name>-cert.pem and SLDAP-CA-cert.pem to the JBoss server.
7. Navigate to the location of the JBoss Certificate Trust keystore. You specified this location during the installation of the Concentrator Remote Server. See Appendix C: Editing the DRMConfig.properties File for the value of the com.axeda.drm.remote.server.keystore property defined during installation.
8. Run the following command to import the new CA certificate:

   keytool –import –file <*path*>/SLDAP-CA-cert.pem
   -alias SLDAP_CA
   -keystore <*Certificate_Trust_File*>
   -storepass <*Certificate_Trust_File_Password*>

   If prompted, type `yes` to confirm the insertion of the certificate.
9. To verify that it was actually imported, type:

   keytool –list –keystore <*Trust_File*>
   -storepass <*Trust_File_Password*>

   This command displays a list of all certificates in the keystore.
10. To install the CA certificate into Sun ONE, do the following (do this *before* installing the server certificate):
    a. Open the Console application of the Sun ONE directory server and navigate to the Manage Certificates dialog box. If you need help, see steps 1 through 5 of the procedure To start the Sun ONE directory server.

b. Click the **CA Certs** tab.

c. Click **Install** to start the Certificate Installation wizard.

d. On the Certificate Location page (1 of 4), select **in this local file**.

e. Click **Browse** and locate the SLDAP-CA-cert.pem file.

f. On the Certificate Location page, click **Next.**

g. On the Certificate Information page (2 of 4), verify the CA certificate information.

h. Click **Next**.

i. On the Certificate Type page (3 of 4), click **Next.**

j. Make sure that both the following check boxes are selected: **Accepting connections from...** and **Making connections to other servers**.

k. Click **Next**.

l. On the Intended Purpose page (4 of 4), click **Done.**
The *Common Name* of the certificate appears in the list on the CA Certs page.

m. Return to the procedure, To install the Server Certificate in Sun ONE to complete the installation and configuration of SSL for your Sun ONE (or iPlanet) LDAP directory server.

Chapter 4: Using Microsoft's Active Directory with SAL

About this chapter

This chapter explains the configuration steps required so that the SAL system can use Microsoft's Active Directory for user authentication.

Note:

Avaya does not ship LDAP directory server software with the SAL system software. You must purchase it separately and install it. The instructions in this chapter will help you set up an Active Directory LDAP directory server and the SAL system to use that directory service.

Support for Active Directory explains how this release of SAL system contains support for Active Directory, an LDAP directory service.

Overview of authentication explains how the SAL system employs authentication measures on two levels: for Web Application Server authentication and within Applications.

Configuring Active Directory for the SAL system explains how to set up and configure Active Directory as an LDAP directory service for the SAL system.

Configuring SAL to use Active Directory explains how to set up and configure the Web application and the SAL system to use Active Directory as its authentication provider.

Support for Active Directory

Directory services provide a central repository for storing and managing identity profiles. The SAL system uses the information stored in the repository for authentication and authorization and to ensure secure access to its components, including Web applications. The SAL system currently supports Microsoft's Active Directory implementation of Lightweight Directory Access Protocol (LDAP). LDAP directory servers provide a standard means for scalable, flexible authentication within the SAL system. Use of multiple directory servers is also supported.

Purchase of the SAL system does not include an LDAP directory server. You must purchase an LDAP directory server separately. You should also see the documentation for the administration application of your Web Application Server for details on configuring it to use Active Directory.

Overview of authentication

Two levels of authentication are performed within a SAL system:

- Authentication at the Web Application Server level. For SAL, the Web Application Server is the JBoss Server. The JBoss Server provides this level of authentication to verify the user name and password of an identity profile. This level provides local authentication for the JBoss Server itself.
- Authentication at the Directory query level. The Secure Access Concentrator Remote Server performs this level of authentication when retrieving user and group information from the directory server. This level provides authentication for Applications.

Figure 4-1 illustrates the levels of authentication for SAL.

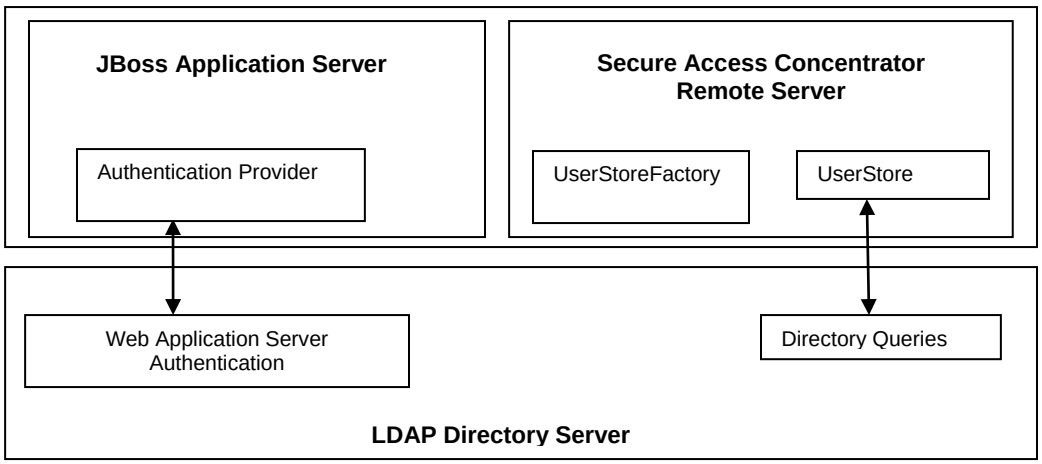


Figure 4-1: SAL System Authentication

Authentication at the Web Application Server level

Web Application Server-level authentication is the first layer of security in the Web Application Server environment. For SAL, the Web Application Server is the JBoss Server. This security layer verifies an entity's identity before completing a connection and protects the JBoss Server environment from unauthorized access.

The default authentication scheme for the JBoss Server is one-way authentication. One-way authentication is common on the Internet when customers want to create secure connections before they share personal data. When the JBoss Server receives a client request, it authenticates the client by comparing the supplied user name and password against the user names and passwords defined in the JBoss Server security realm. If the user name and password can be validated, the client is granted access to the JBoss Server environment.

Authentication at the Directory Query level

After authentication is achieved at the Web Application Server level, the user name is saved as a session attribute available to Web applications. The Secure Access Concentrator Remote Server uses the user name to query the Directory Server and retrieve the user and group information. To be able to support different Directory Server products, the Secure Access Concentrator Remote Server adopts the *Factory* design pattern. This design pattern defines two authentication adapter interfaces:

- UserStoreFactory interface to instantiate the object that implements the UserStore interface.
- UserStore interface for performing all directory queries.

The full class name for the factory is specified in the configuration file, DRMConfig.properties. By default, the class property is set as follows:

```
com.axeda.drm.userStoreFactoryClass=
            com.axeda.drm.user.LdapUserStoreFactory
```

The default authentication adapter, LdapUserStoreFactory/LdapUserStore, is the iPlanet/Sun ONE directory server. To use Active Directory, you need to change the configuration file settings to use the adapter, ActiveDirectoryUserStoreFactory and ActiveDirectoryUserStore. To learn how to change these configuration settings in the DRMConfig.properties file, see Configuring the Concentrator Remote Server for Active Directory.

Note:

You can develop new authentication adapters to support other directory server products, as long as they implement the required interfaces. Contact Avaya for details.

Configuring security

Configuring security entails creating SAL-specific groups, adding users to the various groups, and then assigning to those groups access privileges for the Secure Access Concentrator Remote Server. The rest of this chapter explains how to configure the groups and user accounts in your Active Directory for use with the SAL system. Then the chapter explains how to configure your Web Application Server and the Secure Access Concentrator Remote Server to support Active Directory.

Configuring Active Directory for the SAL System

In addition to specific properties and settings needed in the Web Application Server and the Secure Access Concentrator Remote Server, you need to configure your Microsoft Active Directory installation. Active Directory includes default groups under Builtin. Each of these default groups is included within the Active Directory default folder called *Users*. You need to create specific groups for the SAL system, and create and add users to the selected SAL system groups as needed. Depending upon the needs of your organization, you can create these groups and users under the default Users folder or under a predefined OU (Organizational Unit).

Installing Active Directory

The computer where you install Active Directory must have an assigned DNS domain name (for example, company.com). Active Directory may be installed in one of the two modes: mixed or native. The SAL system supports both modes. Your choice of mode affects domain and group configuration.

Group scope and nesting

The SAL system supports Active Directory installed in either mixed mode or native mode. However, functionality varies with the installation mode, as follows:

- For mixed mode, groups can contain only one level of subgroups. If a subgroup needs to contain another group, the top group must have a domain scope of Domain Local and the subgroup must have a domain scope of Global.
- For native mode, groups can contain an unlimited number and level of subgroups.

For complete information about group hierarchies and domain scope requirements, see your Microsoft Active Directory documentation.

Configuring Active Directory

After installing Active Directory, you need to configure it to support the SAL system. This section explains the changes you need to make to the configuration file for the Concentrator Remote Server, DRMConfig.properties. It then explains the groups you need to add for SAL using the administration application for Active Directory.

Note:

Do *not* configure Active Directory in the Require signing mode by means of the local security setting options. The signing feature in Active Directory through local computer policies is *not* supported in SAL.

To configure Active Directory for use with SAL

1. Open the DRMConfig.properties file in a text editor, and under User Store Settings, remove the # from the following line:

   ```
   #com.axeda.drm.userStore.factory=com.axeda.drm.user.
   ActiveDirectoryUserStoreFactory
   ```

2. Next, insert the # at the beginning of the following line:

```
com.axeda.drm.userStore.factory=com.axeda.drm.user.LdapUserStoreFactory
```

3. Save the DRMConfig.properties file.
4. Use the Administration application for Active Directory to create and add three new groups to the *Users* folder or to your predefined OU:
   - `ServiceLinkAdmins` and `ServiceLinkUsers`. These two groups are specific requirements of the SAL system. The names of the groups are defined in the DRMConfig.properties file, under "User Store Settings". The names entered here must match those defined in DRMConfig.properties. For details about the properties, see User Store Settings (the table of properties in the DRMConfig.properties file).

     Mixed mode: Create these groups with Domain Local domain scope.

     Native mode: You can create these groups with either Universal or Domain Local domain scopes.

     Note:

     This document assumes your Active Directory is using the default group names for the SAL system: ServiceLinkAdmins and ServiceLinkUsers. If you are using different group names for SAL users, make the changes indicated in To specify Active Directory as the authentication provider for the SAL system.
   - A group that will contain the LDAP authenticator account only. This document assumes the group is named LDAPAdminGroup; there are no actual naming requirements.

     Mixed mode: Create this group with Global scope.

     Native mode: Create this group with either Universal or Global scope.
5. Configure the LDAP authentication group (LDAPAdminGroup)
   - For permissions, allow at least Read access.
   - For complete security, deny all other access types (except Full Control, which is blank).

Adding a user account for the LDAP authentication group, (LDAPAdminGroup)

This account will be used to authenticate the Secure Access Concentrator Remote Server with Active Directory during directory service operations. It is recommended, for security purposes, that this account be different from the Web Application Server Administrator account. This chapter assumes the name for this account is admin, although there are no actual naming requirements.

1. Add the LDAPAdminGroup as the primary group for the admin user. Remove the Domain Users group from that user account.
2. Configure the Users group or OU, depending upon which is being used for LDAP authentication for the SAL system.
3. Configure permissions for the admin user by allowing at least Read access.

4. Create or add users and groups to the ServiceLinkAdmins group. Keep in mind that users in the ServiceLinkAdmins group must also be members of the ServiceLinkUsers group. These users will be administrators within Applications. If you nest a subgroup in the ServiceLinkAdmins group, those users will not be administrators *unless* they also happen to be defined directly in the ServiceLinkAdmins group.
5. Create or add users and groups to the ServiceLinkUsers group. These users will be nonadministrative users in Applications.

How applications apply LDAP definitions

Applications can define privileges for only those users and user groups defined in the ServiceLinkAdmins group or ServiceLinkUsers group. Therefore, all individuals who will use Applications must be defined in one or both of these groups.

A group must have at least one member (user) for it to appear in the Administration application's list of LDAP groups. It is not sufficient that the group contain a subgroup.

A user is an administrator within Applications only if the user belongs directly to the ServiceLinkAdmins group. You cannot make an entire group SAL administrators simply by placing the group in the ServiceLinkAdmins group. Each user must be defined directly in the ServiceLinkAdmins group.

Configuring users for the SAL system

When creating a new LDAP user in the Active Directory database, specify the following:

- First Name, Initial, and Last Name of the user. The Full Name field concatenates these strings to show how the name will display in Applications. You can then modify the Full Name directly if you wish.
- User Logon Name. The user types this name when logging in to the SAL system.

  Domain Name is retrieved from the computer upon installation and cannot be changed here. This is the DC name you need to use when configuring your Web Application Server for Active Directory. For example, machineName@company.com.
- Password associated with the user. Confirm by typing the password again.
- E-mail address of the user (optional).
- Phone and fax numbers of the user (optional).

Note:

The SAL system uses the common name (cn), mail, and telephone number properties from the LDAP server.

After creating a new user, you need to modify the properties for that user in order to specify the groups to which that user is assigned. All groups configured in Active Directory are listed for assignment from the Member Groups page of the user's properties. It is on this page that you specify which users are administrators (and thus members of the ServiceLinkAdmins group) and which users are nonadministrators (and thus members of the ServiceLinkUsers group).

Configuring SAL to use Active Directory

To use Active Directory with the JBoss server, you need to select the Active Directory directory service during the SAL installation. Then, after installing the server, you need to modify the DRMConfig.properties file to use Active Directory.

Note:

You cannot use both Active Directory and Sun ONE LDAP directory servers at the same time.

Configuring the Concentrator Remote Server for Active Directory

Even if you specified Active Directory when installing the SAL system software, you need to configure the following settings for Active Directory in the DRMConfig.properties file:

- Change the Authentication Adapter property to Active Directory. Also, if you are not using the default SAL System groups, ServiceLinkAdmins and ServiceLinkUsers, you need to specify the actual group names used in your Active Directory service.
- Set the directory service property to Active Directory.

To specify Active Directory as the authentication provider for the SAL system

1. Open the `DRMConfig.properties` file in a text editor that must be able to save the file in plain text.
2. Search for the string "User Store Settings."
3. In the Primary Authenticator User Store Settings section, scroll down until you see the following lines:

```
# ADS

#com.axeda.drm.userStore.factory=com.axeda.drm.user.ActiveDirectoryUserStoreFactory
#com.axeda.drm.userStore.authenticator.types=ActiveDirectoryAuthenticatorMBean
```

4. Remove the comment symbol (`#`) from the lines that begin with `com.axeda.drm.userStore.`
5. Under `#LDAP`, add the comment symbol to the following lines:

```
com.axeda.drm.userStore.factory=com.axeda.drm.user.LdapUserStoreFactory
com.axeda.drm.userStore.authenticator.types=IPlanetAuthenticatorMBean,LDAPAuthenticato
rMBean
```

6. Following the authenticator properties are the properties that specify the default groups for users, administrators, and LDAP administrators. Change these properties as needed:
   a) The default users group is ServiceLinkUsers. If your Active Directory setup uses another group for SAL users, specify that name here, replacing the default:

      ```
      com.axeda.drm.userStore.group.users=ServiceLinkUsers
      ```

   b) The default administrators group is ServiceLinkAdmins. If your Active Directory setup uses another group for SAL administrators, specify that name here, replacing the default:

      ```
      com.axeda.drm.userStore.group.administrators=ServiceLinkAdmins
      ```

c) The default LDAP administrators group is ServiceLinkLdapAdmins. If your Active Directory setup users another group for LDAP administrators for SAL, specify that name here, replacing the default:

```
com.axeda.drm.userStore.group.ldap.administrators=ServiceLinkLdapAdmi
ns
```

7. The next property in this set enables the SAL system to use your Active Directory server for user authentication. You should not need to change this value; just make sure it is set to `true`:

```
com.axeda.drm.directory-server.on=true
```

8. Scroll down to the next section:

```
#########################################################
#
# Primary authenticator for LDAP, used to identify the Web Server
# security realm which should be used as the primary authenticator
# for users and groups (Example IPlanet).
#
#########################################################
com.axeda.drm.directory-server.primary_authenticator=IPlanet
```

9. Make sure the property value is set to `IPlanet` (set by the installer)

When you are done, these User Store settings sections should appear as follows (`this font` highlights the changes described in the preceding steps):

```
#########################################################
#
# Primary Authenticator User Store Settings
# Authenticator types:
# ActiveDirectoryAuthenticatorMBean
# IPlanetAuthenticatorMBean
# LDAPAuthenticatorMBean
# NovellAuthenticatorMBean
# OpenLDAPAuthenticatorMBean
#
# com.axeda.drm.directory-server.on - Defines whether or not the Secure
# Access Link user can modify the user/user group accounts from Enterprise
# (LDAP Only).
# Default value = true.
#
#########################################################
# ADS
com.axeda.drm.userStore.factory=com.axeda.drm.user.ActiveDirectoryUserStoreFactory
com.axeda.drm.userStore.authenticator.types=ActiveDirectoryAuthenticatorMBean
# LDAP

#com.axeda.drm.userStore.factory=com.axeda.drm.user.LdapUserStoreFactory
#com.axeda.drm.userStore.authenticator.types=IPlanetAuthenticatorMBean,
#LDAPAuthenticatorMBean
#
com.axeda.drm.userStore.group.users=ServiceLinkUsers
com.axeda.drm.userStore.group.administrators=ServiceLinkAdmins
com.axeda.drm.userStore.group.ldap.administrators=ServiceLinkLdapAdmins
com.axeda.drm.directory-server.on=true
#########################################################
#
# Primary authenticator for LDAP, used to identify the
# security realm which should be used as the primary authenticator
# for users and groups (Example IPlanet).
#
```

```
#########################################################
com.axeda.drm.directory-
server.primary_authenticator=ActiveDirectoryAuthenticator
```

To specify the directory server settings for Active Directory

Even if you selected Active Directory while installing the Concentrator Remote Server, you need to edit the DRMConfig.properties file manually. You may also want to see Appendix C: Editing the DRMConfig.properties File.

1. To configure the SAL system to use the Active Directory Authentication Provider, search for the following settings in the `DRMConfig.properties` file:

```
#########################################################
#
# Directory Server Settings, used for UnitTest.
#
#########################################################
com.axeda.drm.directory-server.port=389
com.axeda.drm.directory-server.name=server.avaya.com
com.axeda.drm.directory-server.peoplesearch=ou=People, dc=avaya, dc=com
com.axeda.drm.directory-server.groupsearch=ou=Groups, dc=avaya, dc=com
com.axeda.drm.directory-server.adminsearch=uid=admin, ou=Administrators,
ou=TopologyManagement, o=NetscapeRoot
com.axeda.drm.directory-server.ssl=false
#########################################################
```

   Make sure these settings are accurate for your security environment.

2. Type the number of the port to use for communications with Active Directory:

   ```
   com.axeda.drm.directory-server.port=389
   ```

3. Type the host name or IP address of the machine running Active Directory:

   ```
   com.axeda.drm.directory-server.name=server.avaya.com
   ```

4. Type the User Base DN. This property should contain either `CN=Users` or an OU:

   ```
   com.axeda.drm.directory-server.peoplesearch=ou=People, dc=avaya, dc=com
   ```

5. Type the Group Base DN. This property values should contain either `CN=Users` or an OU:

   ```
   com.axeda.drm.directory-server.groupsearch=ou=Groups, dc=avaya, dc=com
   ```

6. Type the Principal:

   ```
   com.axeda.drm.directory-server.adminsearch=uid=admin,
   ou=Administrators, ou=TopologyManagement, o=NetscapeRoot
   ```

Note:

The SAL system does not support LDAP failovers for Active Directory. Therefore, you can leave the secondary LDAP properties at their default values in the DRMConfig.properties file.

Specifying users and privileges for applications

When all the server configurations are complete, you need to log in to the applications as an administrator and use the Administration application to set up user groups and privileges. These settings specify which devices and device information each user can access, and which tools and functionality in applications are available to the specific user.

To add or remove users or create or delete user groups, you need to do that directly in your LDAP administration tool.

The SAL system with Active Directory supports changing user attributes, e-mail addresses and telephone numbers, from within Applications (User Preferences tool).

Chapter 5: Installing and configuring JBoss and Concentrator Remote Server

About this chapter

The Concentrator Remote Server installation supports the JBoss Enterprise Application Platform and Secure Access Concentrator Remote Server running as a standalone, single server.

Note:

Avaya does not ship the JBoss Enterprise Application Platform software with the SAL system software. You must purchase it separately. The instructions in this chapter will guide you through the installation using considerations for the SAL system.

Preparing to install the JBoss Server provides important information that you should read before attempting the installation.

Before installing JBoss on Linux explains the steps you need to take before installing the JBoss Enterprise Application Platform on a Solaris machine.

Installing the JBoss Enterprise Application Platform guides you through the installation program of the JBoss Enterprise Application Platform server for your platform.

Installing the Concentrator Remote Server Software provides an introduction to this chapter and explains how to install the Concentrator Remote Server software on a Linux machine.

Editing configuration files explains the changes you need to make to configuration files before running the server.

Deploying webservices.war explains how to deploy the webservices.war application that comes with the SAL SDK. The SDK is an option for the system. You can purchase it with your system or later.

What's next directs you to the next steps for installing the SAL system.

Uninstalling the Concentrator Remote Server provides instructions to uninstall the Concentrator Remote Server software.

Importing Certificate Authority certificates provides instructions to import new Certificate Authority (CA) certificates released by Avaya to the Concentrator Remote Server truststore.

Preparing to install the JBoss Server

Before you install the JBoss server, make sure the supported JDK is installed on that machine. See your JBoss EAP server installation documentation for that requirement. If you do not have that documentation readily available, you can browse for that information at http://www.jboss.com.

You can configure the JBoss Server to communicate with the Concentrator Remote Server through SSL or non-SSL communications.

Before installing JBoss on Linux or Solaris

Before installing the JBoss server, you need to perform the following tasks on the Linux computer:

1. Create an account (user) called SAL that will be used to run the JBoss Server. This user should *not* have root access.
2. Create the base directory for the JBoss Server. Although this directory can reside anywhere, you should ensure that the partition where you are going to install it has enough free space. Use the command **`df -k`** to check disk space.
   Avaya recommends that you create the base directory for the JBoss server in one of the following locations, /opt or /usr/local, and that the name of the JBoss home directory does not contain spaces.
3. Ensure the user created in step 1 has the read, write, and execute privileges for the directory created in step 2. To ensure the user has these permissions, log in as the account who created the directory and issue the **`chown`** command:

This command changes the owner of the directory from the account that created it to the SAL account.

Installing the JBoss Enterprise Application Platform

There are three ways to install JBoss Application Server:

- Using the Graphical Installer
- Downloading and running the ZIP installer (see http://www.jboss.org/jbossas/downloads/)
- RPM download for users subscribed on the Red Hat Network (RHN) on http://rhn.redhat.com.

Avaya recommends that you download and run a supported JBoss server ZIP installer. Regardless of the method you choose to install the JBoss Enterprise Application Platform server, you need to keep the following points in mind during and after installation:

- The JBoss server installation creates a server subdirectory within the JBoss home directory. The Concentrator Remote Server installation will install components to the /server subdirectory.

- To install the JBoss EAP server as part of a site server setup, you have to configure the JBoss EAP server after installation to communicate (as a child server) with a parent server. For more information on the configuration, see Enable Federated Communications Support.

To install the JBoss Enterprise Applications Platform server

1. Launch the JBoss EAP installer or open the JBoss server installation archive.
2. Install or extract all files to the directory that will be used as the JBoss Home directory.

If you have any questions regarding the JBoss installation, see your JBoss installation documentation.

Testing the JBoss installation

After you install the JBoss Enterprise Application server, you can test the installation to ensure that the Java Virtual Machine (VM) and operating system are working as expected. You can test the JBoss server installation by running a script included with your JBoss installation.

To test your installation

1. Ensure that the Concentrator Remote Server is not running. If it is, you cannot start the default JBoss server and access the console.
2. Locate and run the **`<JBoss_installation_directory>/bin/run.sh`** script.
3. Open a Web browser on the host computer and browse to http://localhost:8080. Note that you cannot access the link from a remote computer.

   The displayed page should look similar to the following:

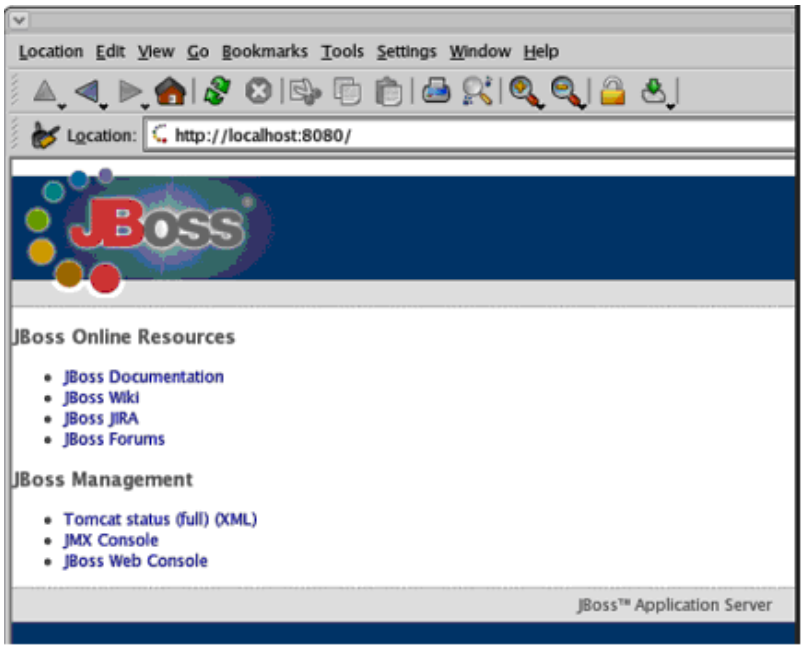


Figure 5-1: Displays if the JBoss server installation test is successful

Installing the Concentrator Remote Server software

You must install the Secure Access Concentrator Remote Server at the same location as the JBoss server. To do this, use the base directory of the JBoss server as the installation location for the Secure Access Concentrator Remote Server. For example, if you use `/opt/avaya` as the base directory for the JBoss server, install the Secure Access Concentrator Remote Server application in the `/opt/avaya` directory, at the same level as the JBoss installation directory.

Note:

For the best performance, install Secure Access Concentrator Remote Server, Oracle database, and LDAP or Active Directory on separate hardware.

The Secure Access Concentrator Remote Server installation program creates a new JBoss server instance using the values that you enter.

Before starting the Secure Access Concentrator Remote Server installation, you have to ensure that the system meets all setup and run-time prerequisites.

Prerequisites for installing the Concentrator Remote Server

Before installing the Concentrator Remote Server, do the following:

- Ensure that the JAVA_HOME environment variable is set and `$JAVA_HOME/bin` is the first entry in the PATH environment variable.
- Identify and create, if required, the base directory in which to perform the installation. This directory should preferably be the base directory for the JBoss server. An example base directory is `/opt/avaya`.
- Ensure that the JBoss server (JBoss 4.3 Enterprise Application Platform) instance is already installed in the base directory. For more information, see Installing JBoss Enterprise Application Platform.
- Create a user account to run the JBoss server. The user should not have root access. (If you have created an account before installing the JBoss server, you do not need to create another account.)
- Ensure that the partition where you are going to install the Concentrator Remote Server application has sufficient free space. Use the command **`df -k`** to check for disk space.
- Ensure that the Secure Socket Layer (SSL) certificates are created and installed on the server.
- For a fresh installation of the Concentrator Remote Server application, ensure that the Oracle software is installed, the database is created, and a database user is created to connect to the database. In addition, ensure that database tables are created and initialized. For more information, see Configuring the Oracle database.

In addition, you require the following information when installing the Concentrator Remote Server:

- SMTP server address.
- E-mail address of the Concentrator Remote Server system administrator.

- JBoss server details, such as server IP address, HTTP and HTTPS listening ports, and keystore key information.
- Sun ONE LDAP or Active Directory server details, such as host name, listening port, principal DN, principal password, user base DN, group base DN, user name attribute, and group name attribute.
- If the Concentrator Remote Server is to be used by business partners, details of the LDAP directory server that supports access by business partners.
- Oracle database server details, such as name of the host computer where the database is located, Oracle System Identifier (SID), and user ID and password to connect to the database.
- Cognos 8 installation details, such as URL for the Cognos 8 report server, listening port for the Cognos 8 application server, the listening port for the Cognos 8 Web server, and the name of the default report folder to which you want the server to publish reports. If you are not using Cognos 8, you can accept the default values. You can install and configure Cognos 8 after installing the Concentrator Remote Server.

  CAUTION:

  After you provide the server name and installation locations to the installation program, you cannot rename these components without doing a complete reinstall.

Installing the Concentrator Remote Server in the Linux console mode

On a Linux platform, you can use the Linux console mode to install the Secure Access Concentrator Remote Server software.

You have to do a complete installation of the Concentrator Remote Server application from the beginning with the installation file for Secure Access Concentrator Remote Server version 5.3.2. After the installation completes for version 5.3.2, you have to install a service pack for version 5.3.3.

1. Download the Concentrator Remote Server software installation package from the Web site at https://plds.avaya.com/poeticWeb/avayaLogin.jsp?ENTRY_URL=/esd/viewDownload.htm&DOWNLOAD_PUB_ID=SAL00000013
2. Open a shell prompt and navigate to the directory where you downloaded the file.
3. Unzip the installation package you have downloaded.
4. Navigate to the 5_3_2 directory and run the following command:

   ```
   ksh ./Axeda_Enterprise.bin
   ```

5. Read the list of prerequisites. If your system meets all of them, press **Enter** to continue.

   Note:

   In the case of a fresh installation, ensure that the JBoss server does not host any older or same version of Secure Access Link server instance.

The console displays the license agreement.

6. Read the license agreement and press **Enter** to go to the next page.
7. Type Y and press **Enter** to accept the license agreement and continue with the installation.
   To continue with the installation, you must accept the license agreement. If you do not accept the license agreement and type N and press **Enter**, the system quits the installation and returns to the shell prompt.
8. When prompted to choose the Java Virtual Machine (VM), do one of the following:
   - Check the list of Java VMs detected on the system and type the number next to the Java VM you want.

   Note:

   The installer uses the JAVA_HOME environment variable to detect the Java VMs on the system. If you do not set the environment variable before running the installer, it does not detect the Java VMs.

   - If no Java VM is detected or you want to use a different Java VM, enter the option for selecting a Java VM and type the absolute path to the Java VM including the Java VM's executable, `$JAVA_HOME/bin/java`.
9. Press **Enter**.

   The installation program prompts you to select the installation location.
10. Do one of the following to choose the installation location for the Concentrator Remote server.
    a. To accept the default location, press **Enter**. The default location is `/home/axeda/ServiceLink`.
    b. To specify a different location, type an absolute path. Press **Enter** when finished. If the specified directory does not exist, the installer creates a new directory.

    Note:

    Avaya recommends that you set the directory path to `/<installation base directory (the one used to install JBoss)>/SAL/CRS`. For instance, if you set the base directory to `/opt/avaya` for JBoss, then the recommended Secure Access Concentrator Remote Server application directory is `/opt/avaya/SAL/CRS`.
11. Specify the Cognos 8 installation information, including the URL for the Cognos 8 report server, the listener port for the Cognos 8 application server, the listener port for the Cognos 8 Web server, and the name of the default report folder to which you want the server to publish reports.
    If you are not using Cognos 8 for the report server, accept the default values by pressing **Enter** after each value.
12. Specify the JBoss home directory that will serve as the central support directory for all JBoss products installed on the target system.

    Do one of the following:
    - To accept the default JBoss home directory, type `next` or press **Enter**.
    - To specify a different location for the JBoss home directory, at the prompt, type the full path to the directory. For example, `/opt/avaya/jboss-eap-`

`4.3/jboss-as`. If the specified directory does not exist, the installer creates the new directory.

13. Type a name for the Secure Access Concentrator Remote Server. You can accept the default value, `ServiceLink`. Press **Enter** when finished.

    Note:

    Conventional practice is to name the Concentrator Remote Server instance as `SecureAccessLink`.

14. Type the following information for the SAL server:

    - Server IP Address (default is 127.0.0.1).

      Make sure that you enter the actual IP address or fully qualified domain name (FQDN) of the SAL server. Using the loopback or local host address is strongly discouraged.

    - Server Listening Port (default is 7001).

      The recommended HTTP listening port for the Concentrator Remote Server is 8080.

    Press **Enter** after each value.

15. Type the port number of the SSL server listening port for remote sessions. The default value is 443. The recommended HTTPS listening port for the Concentrator Remote Server is 8443.

    Press **Enter** when finished.

16. Type the following JBoss keystore key information:

    - Path to the keystore file
    - Password phrase for the keystore
      (You have to enter the password twice to confirm it)

    Press **Enter** after entering each value.

17. Type the following information about the database with which the JBoss Server and the Concentrator Remote Server will communicate:

    - Name of the host computer where the database is located
    - Oracle System Identifier (SID)
    - User ID to connect to the database
    - User password (you have to enter the password twice to confirm it)

    Press **Enter** after each value.

18. Type the address of the SMTP server and press **Enter**.

19. Type the e-mail address of the Concentrator Remote Server system administrator, and press **Enter**.

20. If you want to use a Software Management Server where the Concentrator Remote Server sends and receives Software Management packages, specify the Software Management Server host name, and the listening port.

    If you are not using a Software Management Server, accept the default values by pressing **Enter** after each value.

21. Select a supported directory service. The supported directory service servers are:
    - LDAP (Sun ONE)
    - Active Directory Server

    For Active Directory, you have to edit the DRMConfig.properties file after completing the installation. For complete details on the configuration of the Concentrator Remote Server to use Active Directory for authentication, see Chapter 4, Configuring Active Directory for the SAL System.
22. Provide the following values for the directory server:
    - Host Name - Type the computer name where your directory server is running. You can also type the IP address of the computer.
    - Listening Port - Accept the default value of `389` if you are using the default LDAP port. If not, type the number of the port you are using for LDAP authentication.
    - Directory Server Principal DN - Type the SAL-specific information from your directory server for the `uid` (administrator user name to log in to the directory server), `ou`, and `o` parameters.

      If you use the Sun ONE LDAP directory server environment, accept the following default settings: `uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot`.
    - Directory Server Principal Password - Type the system password for accessing the directory server. This is the password for the administrator user specified in the `uid` parameter. (You have to enter the directory server principal password twice to confirm it.)
    - User Base DN - Type the information appropriate to your directory server setup, as one of the following:
      - If you use the default `Users` group, provide the following settings:
        `CN=Users, DC=machineName, DC=company, DC=com`
        Where you have to replace the values with actual domain for your setup. Keep Users as the CN value.
      - If you use an OU, provide the following settings:
        `OU=Applications, DC=machineName, DC=company, DC=com`
        Where you have to replace the values with the actual OU and domain names.
    - Group Base DN - Type the information appropriate to your directory server setup, as one of the following:
      - If you use the default Users group, provide the following settings:
        `CN=Users, DC=machineName, DC=company, DC=com`
        Where you have to replace the values with actual domain for your setup. Keep Users as the CN value.
      - If you use an OU, provide the following settings:
        `OU=Applications, DC=machineName, DC=company, DC=com`
        Where you have to replace the values with the actual OU and domain names.

- Username Attribute - Type the attribute of a directory server user object that specifies the name of the user. For example, for LDAP you can leave the default value, `uid`. For Active Directory, you can type `sAMAccountName`.
- Static Group Name Attribute - Type the attribute of a static directory server group object that specifies the name of the group. For example, for LDAP you can leave the default value, `cn`. For Active Directory, you can type `sAMAccountName`.
- User From Name Filter - If the user name attribute and user object class is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. You can accept the default, `(&(uid=%u)(objectclass=person))` by pressing **Enter**.
- Group From Name Filter - A search filter for finding a group based on the name of the group. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. You can accept the default, `(|(&(cn=%g)(objectclass=groupofUniqueNames))(&(cn=%g)(objectclass=groupOfURLs))`.

  Press **Enter** after providing each value.

23. To allow external business partners to log in to the Concentrator Remote Server, type `yes`. Otherwise, type `no`. Press **Enter** after providing the option.

    Note:

    Only the Sun ONE LDAP directory server supports access to the Concentrator Remote Server by business partners.

24. If you choose to allow partner login, specify the following Sun ONE LDAP directory server information: host name, listening port, principal DN, principal password, user base DN, group base DN, user name attribute, group name attribute, user from name filter, and group from name filter.
    For more information on the directory server settings, refer step 22.
    Press **Enter** after each value.
25. If you choose to allow partner login, type the URL to log in to the Concentrator Remote Server externally. Press **Enter** after typing the URL.
26. Press **Enter** to start the installation.

    When the installation completes successfully, press **Enter** to quit the Installation program.

Post installation configuration and customization

After the installation of the Concentrator Remote Server completes successfully, you must do some additional tasks for the Concentrator Remote Server application to work properly. You also need to do some Avaya-specific customization of the Concentrator Remote Server application.

Before starting the post installation and customization processes, ensure that the JAVA_HOME environment variable is set and that `<JAVA_HOME>/bin` is the first entry in the PATH environment variable.

⚠WARNING:

Ensure that JBoss is *not* running when executing the post installation and customization instructions. To avoid unpredictable results, stop the JBoss process before executing the post installation instructions.

To extract the contents of the servicelink.ear file

1. Navigate to the `/<JBOSS_HOME>/server/<Secure Access Link server instance>/deploy` directory.
2. Create a new subdirectory with any name and navigate to the directory.
3. In this subdirectory, run the command **`jar xvf ../servicelink.ear`**. This command extracts the following five WAR files along with a SAR file and the META-INF directory:
   - drm.war
   - help.war
   - public.war
   - remote.war
   - rpc.war
4. Create new directories that match the names of each of the WAR files. For example, create a directory with name drm for the drm.war file, and so on for the other WAR files.
5. Navigate to each of these new directories and extract the contents of the respective WAR file by running the command **`jar xvf ../<war file name>`**.
   For example, if you are in the `drm` directory, run the command **`jar xvf ../drm.war`** to extract the contents of the drm.war file to the `drm` directory.

   ⚠CAUTION:

   Always extract the contents of a WAR file in its appropriate directory counterpart. For instance, if you are in the `help` directory, run the command **`jar xvf ../help.war`**, and not **`jar xvf ../drm.war`**.
6. After completing the extraction of all WAR files, return to the directory where you extracted the servicelink.ear file.
7. Remove the WAR files by running the command **`rm *war`**.
8. Rename each WAR directory to have the WAR file extension.
   For example, rename drm to drm.war by running the command **`mv drm drm.war`**.
9. Move up to the deploy directory.
10. Move (*Do not* delete) the servicelink.ear file outside the JBoss server installation directory.
    This step is to prevent any confusion and to keep the file from being potentially redeployed.
11. Rename the temporary directory to servicelink.ear.
12. Copy the axeda-license.xml file to the Concentrator Remote Server installation directory, `/<base directory>/SAL/CRS/config`.

To test the Concentrator Remote Server installation

1. Navigate to the /<JBOSS_HOME>/bin directory.
2. Create a new directory named log in the /<JBOSS_HOME>/server/<Secure Service Link instance> directory to store the output of command from step 3.
3. Run the following command to start the Concentrator Remote Server application:

   nohup ./servicelinkrun.sh > ../server/*<Secure service Link instance>*/log/jboss.out &
4. Run the command **tail –f ../server/*<Secure Service Link instance>*/log/jboss.out** to monitor the progress of the startup of the JBoss process. Look for a line that provides the time taken to start the process in the format XXm:XXs:XXXms. Ensure that there are no errors in the log prior to reaching this point.
5. If the Concentrator Remote Server application starts successfully, run the command **./servicelinkshutdown.sh** to shut down the application.
6. If the log file indicates errors in the installation, identify the JBoss process and shut down the process and its parent process.
   Run the command **ps –ef | grep java** to identify both processes.
7. Remove the following directories from the Web Application Server instance directory:
   - work
   - data
   - tmp

To do Avaya-specific customizations for Concentrator Remote Server 5.3.2

1. Navigate to the directory where you have downloaded the installation package.
2. Navigate to the directory 5_3_2 and create a temporary directory.
3. Navigate to the temporary directory.
4. Run **jar xvf ../*Avaya_SPIRIT_Enterprise_159*.zip** to extract the contents of the zip file to the new directory.

   Five directories and an additional zip file are extracted.
5. Copy the contents of each of the directories to the directory with similar name in the installation directory.

   For instance, if /opt/avaya/SAL/CRS/ is the installation directory, run the following commands to copy the contents of the bin, config, cognos, ddl, and lib directories:

   cp –r bin/* /opt/avaya/SAL/CRS/bin/

   cp –r config/* /opt/avaya/SAL/CRS/config/

   cp –r cognos/* /opt/avaya/SAL/CRS/cognos/

   cp –r ddl/* /opt/avaya/SAL/CRS/ddl/

   cp –r lib/* /opt/avaya/SAL/CRS/lib/
6. Create another directory within the temporary directory.

7. Navigate to the new temporary directory and extract the contents of the axeda-service-webapps.zip file to it. Run following the command:
   jar xvf ../*axeda-service-webapps*.zip.

   Five directories are extracted: drm, public, remote, drmform, and webservices2.

8. Create a new directory, drmform.war, within the directory path /<JBOSS_HOME>/server/<Secure Service Link instance>/deploy/servicelink.ear.

   Note:

   The servicelink.ear directory already has the sub-directories drm.war, public.war, and remote.war.

9. Copy the contents of each of the directories, except webservices2, to the corresponding WAR directory in the /<JBOSS_HOME>/server/<Secure Service Link instance>/deploy/servicelink.ear directory.

   Assuming you used /opt/avaya/jboss-eap-4.3/jboss-as/server/SecureAccessLink as the directory path for the server instance, run the following commands exactly as shown:

   cp –r drm/* /opt/avaya/jboss-eap-4.3/jboss-as/server/SecureAccessLink/deploy/servicelink.ear/drm.war/

   cp –r public/* /opt/avaya/jboss-eap-4.3/jboss-as/server/SecureAccessLink/deploy/servicelink.ear/public.war/

   cp –r remote/* /opt/avaya/jboss-eap-4.3/jboss-as/server/SecureAccessLink/deploy/servicelink.ear/remote.war/

   cp –r drmform/* /opt/avaya/jboss-eap-4.3/jboss-as/server/SecureAccessLink/deploy/servicelink.ear/drmform.war/

10. Navigate to the /<JBOSS HOME>/server/<Secure Service Link instance>/deploy/servicelink.ear/META_INF directory.

11. Open the application.xml file and add the following lines to the file:

```
<module id="ServiceLinkForm_WebModule">
  <web>
    <web-uri>drmform.war</web-uri>
    <context-root>/drmform</context-root>
  </web>
</module>
```

12. Navigate to the Concentrator Remote Server application installation directory, /<base directory>/SAL/CRS/config.

13. Open the CustomConfig.properties file and add the following lines to the file:

```
#trust store used to communicate with parent server
com.axeda.drm.remote.server.truststore=<Java installation directory>/jre/lib/security/cacerts
com.axeda.drm.remote.server.truststore-passphrase=<password>
```

14. Open the jboss-service.xml file located in the /<JBOSS HOME>/server/<Secure Service Link instance>/conf directory. Make the following modifications:

    a. Remove the following lines located towards the end of the file:

    - <classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="oracle-integration-proxy.jar"/>

- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="groovyws-all-0.4.jar"/>`
- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="groovywscustom.jar"/>`
- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="axis.jar"/>`

b. Add the following lines to the <classpath> tags located towards the end of the file. Place them at the start of the <classpath> group of tags.

Note:

Do *not* place them in front of the <classpath> tags located near the start of this file. Look for the group of tags located towards the end of the file, and place these new tags there.

- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="axeda-5.3sp.jar"/>`
- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="bcprov-ext-jdk15-141.jar"/>`
- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="bcprov-jdk15-141.jar"/>`
- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="backport-util-concurrent-3.0.jar"/>`
- `<classpath codebase="file:///opt/avaya/SAL/CRS/lib" archives="ehcache-1.5.0.jar"/>`

15. Test the installation using the steps in the procedure, To test the Concentrator Remote Server installation.

Installing the Concentrator Remote Server 5.3.3 Service Pack

After completing the main installation process for the Secure Access Concentrator Remote Server application, you need to install a service pack for version 5.3.3.

CAUTION:

Before installing the 5.3.3 Service Pack, ensure that the Concentrator Remote Server application is *not* running. If the Concentrator Remote Server application is up, run the command **`./servicelinkshutdown.sh`** to shut down the application.

To install the Concentrator Remote Server 5.3.3 Service Pack

1. Make a copy of the CustomConfig.properties file located in the Concentrator Remote Server application installation directory, `/<base directory>/SAL/CRS/config`.
2. Navigate to the directory where you have downloaded the 5.3.3 service pack.
3. From the `5.3.3` directory, run the following command:

   `ksh ./Axeda_Enteprise_Service_Pack.bin`

   The installation process for 5.3.3 service pack starts.
4. Type y to accept the license agreement, and press **Enter** to continue.

5. Provide the directory information for the installation. Use the same directory path used in the main installation process.

   For example, if `/opt/Avaya/SAL/CRS` is the installation directory for the Concentrator Remote Server application, provide the same directory path for the service pack installation.

6. Press **Enter** to continue.
7. Provide the full directory path of the installed Web Application Server instance as the following:

   ```
   <JBoss_Home>/server/<Secure Service Link_server>/deploy/
   servicelink.ear
   ```

8. Press **Enter** to continue.

   The system asks you whether to override existing configuration files.

9. Type a number shown besides an option and press **Enter**.

   The system prompts you to execute an SQL script for database migration.

10. Do the following to execute the SQL script:

    a. Locate the database_migration.sql file in the ddl subdirectory of the installation directory and transfer it to the Oracle database server.

    b. Using SQL*PLUS, execute the following command:

       sqlplus *<db_username>*/*<db_password>*@*<SID>* @*database_migration*.sql

    Note:

    You can run the script before starting the installation process. Also note that if the script has already been executed successfully, it fails if you try to re-execute it. However, re-execution does not have any impact on the database.

11. Return to shell prompt where the installation process is running and press **Enter** to continue.

    The system prompts you to configure the classpath tags.

12. Open a new shell prompt and do the following:

    a. Open the jboss-service.xml file, located in the `<JBOSS HOME>/server/<Secure Service Link instance>/conf` directory, and look for the classpath tag with the axeda-5.3sp.jar file path.

    b. If the specific classpath tag is not present and assuming you used `/opt/avaya/SAL/CRS` as the install directory, add the following line at the start of the classpath group of tags.

       ```
       <classpath codebase="file:///opt/avaya/SAL/CRS/lib"
       archives="axeda-5.3sp.jar"/>
       ```

    Note:

    Do *not* place the new line in front of the classpath tags located near the start of this file. Look for the group of tags located towards the end of the file, and place the new tag there.

13. Return to the shell prompt where the installation process is in progress.
14. Press **Enter** to start the installation.

15. When the installation completes successfully, press **Enter** to quit the Installation program.
16. After the installation completes, copy the CustomConfig.properties file back to the application directory, `/<base directory>/SAL/CRS/config`.
17. Test the installation using the steps in the procedure, To test the Concentrator Remote Server installation.

To do Avaya customizations for 5.3.3 Service Pack

1. Make a copy of the CustomConfig.properties file located in the Concentrator Remote Server application installation directory, `/<base directory>/SAL/CRS/config`.
2. Navigate to the directory where you downloaded the installation package for 5.3.3 service pack.
3. Navigate to the `5_3_3` directory.
4. Create a temporary directory and navigate to the temporary directory.
5. Run the command **`jar xvf ../Avaya_SPIRIT_Enterprise_160.zip`** to extract the contents of the zip file to the new directory.

   Five directories and an additional zip file are extracted.
6. Copy the contents of each of the directories to the directory with similar name in the installation directory.

   For instance, if `/opt/avaya/SAL/CRS` is the installation directory, run the following command to copy the contents of the `bin` directory to `/opt/avaya/SAL/CRS/bin`:

   ```
   cp –r bin/* /opt/avaya/SAL/CRS/bin/
   ```
7. Create another directory within the temporary directory.
8. Navigate to the new temporary directory and extract the contents of the axeda-service-webapps.zip file to it. Run following the command: **`jar xvf ../axeda-service-webapps.zip`**.

   Five directories are extracted: drm, public, remote, drmform, and webservices2.
9. Copy the contents of each of the directories, except webservices2, to the corresponding WAR directory in the `/<JBOSS_HOME>/server/<Secure Service Link instance>/deploy/servicelink.ear` directory. The WAR directories were already created during the main installation process for Concentrator Remote Server 5.3.2.

   For instance, if you used `/opt/avaya/jboss-eap-4.3/jboss-as/server/SecureAccessLink` as the directory path for the server instance, run the following command to copy the `drm` directory contents to the corresponding `drm.war` directory:

   ```
   cp –r drm/* /opt/avaya/jboss-eap-4.3/jboss-
   as/server/SecureAccessLink/deploy/servicelink.ear/drm.war/
   ```
10. Copy the CustomConfig.properties file back to the `/<base directory>/SAL/CRS/config` directory.
11. Open the CustomConfig.properties file and make the following changes:

a. Change the build information line in the file, as shown below. Make this nonfunctional change to prevent confusion among technicians and engineers who may need to troubleshoot the installation.

```
com.axeda.drm.custom.build-info = Avaya_SPIRIT build160
(2009/03/31 21:05 EDT)
```

b. If the Concentrator Remote Server is a lower stream site server, set the stage creation property's value to false, as shown below.

```
#
# Staged schema name (Oracle) for staged schema queries
#
#########################################################
com.axeda.drm.staged.schema-name = stage


#########################################################
#
# Enforce reading devices from staged schema
#
#########################################################
com.axeda.drm.device.allowStageCreation=false
```

To install 1066 and 1128 hot fixes

1. From the directory where you downloaded the service pack, copy the following JAR files to the application directory, /<base directory>/SAL/CRS/lib.
   - axeda_v5.3HotFixID1066.jar
   - avaya_v5.3HotFixID1128_debug.jar
2. Open the jboss-service.xml file located in the /<JBOSS HOME>/server/<Secure Service Link instance>/conf directory.
3. Assuming that you installed the remote server application in the /opt/avaya/SAL/CRS directory, add the following lines to the <classpath> tags located towards the end of the jboss-service.xml file. Place them at the start of the <classpath> group of tags.

   Note:

   DO not place them in front of the <classpath> tags located near the start of the file. Look for the group of tags located towards the end of the file, and place these new tags there.

```
<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="axeda-service-drm.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="axeda_v5.3HotFixID1066.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="avaya_v5.3HotFixID1128_debug.jar"/>
```

To verify the classpath configuration in the jboss-service.xml file

It is extremely important that the order of the JAR files in the <classpath> tags of the jboss-service.xml file is correct.

1. Review the jboss-service.xml and verify whether the start of the <classpath> group of tags looks like the following:

```
<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="avaya_v5.3HotFixID1128_debug.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="axeda-service-drm.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="axeda_v5.3HotFixID1066.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="axeda-5.3sp.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="bcprov-jdk15-141.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="bcprov-ext-jdk15-141.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="ehcache-1.5.0.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="backport-util-concurrent-3.0.jar"/>

<classpath codebase="file:///opt/avaya/SAL/CRS/lib"
archives="axeda.jar"/>
```

2. If the order of the <classpath> tags does not match the above order, reorder and remove lines as appropriate.
   For the Concentrator Remote Server application to start and run properly, it is important that this order is maintained accurately.

To test and start the Concentrator Remote Server application

1. Navigate to the `/<JBOSS_HOME>/bin` directory.
2. Run the following command to start the Concentrator Remote Server application:

   `nohup ./servicelinkrun.sh > ../server/<Secure Service Link instance>/log/jboss.out &`

3. Run the command **`tail -f ../server/<Secure Service Link instance>/log/jboss.out`** to monitor the progress of the startup of the JBoss process. Look for a line that provides the time taken to start the process in the format XXm:XXs:XXXms. Ensure that there are no errors in the log prior to reaching this point.
4. If the Concentrator Remote Server application starts successfully, test the Web application interface. Use the URL https://<FQDN of the server>:8443/drmform to open the UI.
5. If the log file indicates errors in the installation, identify the JBoss process and shut down the process and its parent process.
   Run the command **`ps -ef | grep java`** to identify both processes.

6. If you have to stop the application, remove the following directories from the Web Application Server instance directory:
    - work
    - data
    - tmp

Editing configuration files

Before your Secure Access Concentrator Remote Server system runs, you need to ensure that the configuration files contain the appropriate installation paths and that you set properties for various applications.

This section explains the configuration file editing you need to perform before you run the Concentrator Remote Server application. Table 5-1 lists configuration files and their locations.

Table 5-1 Locations of Configuration Files

Configuration file	Description	Location
log4j.properties	Logging setup	`/<CRS Application>/config`. If you accepted the recommended location for the Concentrator Remote Server application, the file location is `/opt/avaya/SAL/CRS/config`.
DRMConfig.properties	Concentrator Remote Server setup (see also Appendix C: Editing the DRMConfig.properties File)	`/<CRS Application>/config`. If you accepted the recommended location for the Concentrator Remote Server application, the file location is `/opt/avaya/SAL/CRS/config`.
DRMConfigInfo.properties	Concentrator Remote Server properties that are to be visible in the Administration application (see also Appendix C: Editing the DRMConfig.properties File)	`/<CRS Application>/config`. If you accepted the recommended location for the Concentrator Remote Server application, the file location is `/opt/avaya/SAL/CRS/config`.
startup.xml	SAL system tasks and their parameters. For example, the SynchronizeUsersTask is defined in this file. This task is scheduled to run every 15 minutes by default.	`/<CRS Application>/config`. If you accepted the recommended location for the Concentrator Remote Server application, the file location is `/opt/avaya/SAL/CRS/config`.

Configuration file	Description	Location
Login_config.xml	JBoss server login configuration. Settings in this file are provided by the Concentrator Remote Server installer. You should not need to modify this file.	/<JBOSS_HOME>/server/<server name>/conf
jboss-log4j.xml	Logging setup	/<JBOSS_HOME>/server/<server name>/conf
jboss-service.xml	Server settings, including JNDI, JMX console support, and other settings you may want to modify for performance reasons.	/<JBOSS_HOME>/server/<server name>/conf
web.xml	Filter definitions and mappings, servlet information and mappings for all of the Applications that are part of the *drm* application, session timeout for all user sessions, welcome file, error pages, JSP configuration and encoding (must keep default setting of UTF-8 to work with Cognos 8 Reporting), resource references, and security settings.	/<JBOSS_HOME>/server/<server name>/deploy/servicelink.ear/drm.war/WEB-INF
server.xml	Security and port settings.	/<JBOSS_HOME>/server/<server name>/deploy/jboss-web.deployer

The web.xml file

This configuration file contains filter definitions and mappings, servlet information for all of the Applications that are part of the *drm* application (for example, servlet information for the Site Preparation Utility). All sessions with the Applications, including the Site Preparation Utility, are managed by the session timeout property in the web.xml file, which is listed as follows:

```
<session-config>
      <session-timeout>20</session-timeout>
</session-config>
```

This default setting means that if a session is inactive for 20 minutes, the session is automatically ended, and the user must log in again. To change this timeout, open the

web.xml file in a text editor, and search for the string, `session-timeout`. Change the number `20` to the number of minutes that you want the system to wait for a session to be inactive before timing the session out. Save and close the file.

You can also locate this property in the complete listing of this file in the section, The web.xml configuration file in Appendix B, "Concentrator Remote Server Files." It appears in `this font`.

Adding additional directory services

During the Concentrator Remote Server installation, you are prompted to specify the values of the primary directory service for your SAL system. In addition, you can specify a directory service to use for Partner Login users.

After the installation, you can manually add support for additional directory services to your SAL system. This will provide backup support for your directory service operations in case a primary directory service is unavailable.

To do so, you edit the login-config.xml file provided in the `/<JBoss_HOME>/server/<Secure Access Link Install>/conf` directory.

1. Locate the login-config.xml file installed to your JBoss SAL server.
2. Open the file in a text editor.
3. In the file, locate the section titled "ServiceLink access settings." This section contains the LDAP information for your SAL system, as provided during the Concentrator Remote Server installation.
4. Create a new module in this section. You can copy everything in the existing `<loginmodule>` and paste it in the file, below the existing `<login-module>`.
5. An example of the <login-module> is shown below. You can copy and paste from the example, if needed, and then modify the settings for your environment:

```
<login-module code="org.jboss.security.ClientLoginModule"
flag="required"/>
<login-module code="org.jboss.security.auth.spi.LdapExtLoginModule"
flag="sufficient">
<module-option name = "throwEx">true</module-option>
  <module-option
name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</mod
ule-option>
  <module-option name="java.naming.provider.url">ldap://jmalkan-
dt:389/</ module-option>
  <module-option name="java.naming.provider.host">jmalkan-dt</module-
option>
  <module-option name="java.naming.provider.port">389</module-option>
  <module-option
name="java.naming.security.authentication">simple</moduleoption>
  <module-option name="bindDN">uid=admin, ou=Administrators,
ou=TopologyManagement, o=NetscapeRoot</module-option>
  <module-option name="bindCredential">admin</module-option>
  <module-option name="baseCtxDN">ou=People, dc=Avaya, dc=com</module-
option>
  <module-option name="rolesCtxDN">ou=Groups, dc=Avaya,
dc=com</moduleoption>
  <module-option name="userObjectClass">person</module-option>
  <module-option name="userNameAttribute">uid</module-option>
  <module-option name="userDynamicGroupDNAttribute">null</module-option>
```

```
  <module-option
name="groupStaticObjectClass">groupofuniquenames</moduleoption>
  <module-option name="groupStaticNameAttribute">cn</module-option>
  <module-option name="memberStaticDNAttribute">uniquemember</module-
option>
  <module-option name="java.naming.security.protocol"></module-option>
  <module-option name="providerClassName"></module-option>
  <module-option name = "name">IPlanetPartnerAccess</module-option>
  <module-option name="description">Vendor Authenticator</module-option>
  <module-option name="version">1.0</module-option>
  <module-option name="roleFilter">(uniquemember={1})</module-option>
  <module-option name="baseFilter">(uid={0})</module-option>
  <module-option name="uidAttributeID">uniqueMember</module-option>
  <module-option name="roleAttributeID">cn</module-option>
  <module-option name="roleNameAttributeID">cn</module-option>
  <module-option name="roleAttributeIsDN">false</module-option>
  <module-option name="allowEmptyPasswords">false</module-option>
     </login-module >
     <login-module code="org.jboss.security.auth.spi.LdapExtLoginModule"
flag="required">
   <module-option name = "throwEx">true</module-option>
   <module-option
name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</mod
ule-option>
   <module-option
name="java.naming.provider.url">ldap://leda.avaya.com:389/</
module-option>
   <module-option
name="java.naming.provider.host">leda.Avaya.com</moduleoption>
   <module-option name="java.naming.provider.port">389</module-option>
   <module-option
name="java.naming.security.authentication">simple</moduleoption>
   <module-option name="bindDN">uid=admin, ou=Administrators,
ou=TopologyManagement, o=NetscapeRoot</module-option>
   <module-option name="bindCredential">admin</module-option> Secure
Access Site Server Deploying webservices.war 95
   <module-option name="baseCtxDN">ou=People, dc=Avaya, dc=com</module-
option>
   <module-option name="rolesCtxDN">ou=Groups, dc=Avaya,
dc=com</moduleoption>
   <module-option name="userObjectClass">Person</module-option>
   <module-option name="userNameAttribute">uid</module-option>
   <module-option name="userDynamicGroupDNAttribute">null</module-
option>
   <module-option
name="groupStaticObjectClass">groupofuniquenames</moduleoption>
   <module-option name="groupStaticNameAttribute">cn</module-option>
   <module-option name="memberStaticDNAttribute">uniquemember</module-
option>
   <module-option name="java.naming.security.protocol"></module-option>
   <module-option name="providerClassName"></module-option>
   <module-option name="name">IPlanet</module-option>
   <module-option name="description">Iplanet Authenticator</module-
option>
   <module-option name="version">1.0</module-option>
   <module-option name="roleFilter">(uniquemember={1})</module-option>
   <module-option name="baseFilter">(uid={0})</module-option>
   <module-option name="uidAttributeID">uniqueMember</module-option>
   <module-option name="roleAttributeID">cn</module-option>
   <module-option name="roleNameAttributeID">cn</module-option>
   <module-option name="roleAttributeIsDN">false</module-option>
   <module-option name="allowEmptyPasswords">false</module-option>
     </login-module >
```

```
</authentication>
</application-policy>
```

6. Configure the new module with all information for the additional directory service for your environment.
7. Change the flag for each additional directory service to `sufficient`. See the flag settings highlighted in the previous example. Note that only the primary directory service should be set to `required`.

   The flag should be set as follows for additional or backup directory services:

   ```
   <login-module code="org.jboss.security.ClientLoginModule"
   flag="sufficient"/>
   ```

8. You can create more backup directory services using these steps.

   Note:

   The SAL system will access and use the directory services in the order defined in this file. Make sure you organize each login-module in the order you want the related directory service to be used.

Deploying webservices.war

The SAL SDK is a separate option that provides APIs and enables programmers to develop Web services. To support Web services development, the SDK includes the webservices.war file and the Integration Developer's Guide. After restarting the JBoss Server and verifying that the SAL system is functional, you can deploy the webservices.war file to your Concentrator Remote Server.

To deploy webservices.war on the Concentrator Remote Server

Copy the webservices.war archive from the SAL SDK CD to the following location: `<JBOSS_HOME>/server/<SecureAccessLink_server>/deploy/servicelink.ear`. Now you can verify that the WAR file deployed properly by opening a browser window to the SAL system and the Web services. To view the Web services, type `http://serverurl/webservices/services`. The list of web services appears, indicating that the WAR file has been properly deployed.

What's next

You may need to make some changes to your directory server setup. See Chapter 3, "Using a Sun ONE LDAP Directory Server with SAL." The chapter explains how to configure SSL for use with your LDAP directory server (SLDAP) in your SAL system.

Uninstalling the Concentrator Remote Server

The installation directory for the Secure Access Concentrator Remote Server software contains a subdirectory called `Uninstall Axeda Enterprise`, along with other subdirectories including `bin`, `config`, `ddl`, `lib`, `scm`, and `sessionlogs`. The `Uninstall Axeda Enterprise` directory contains the script to uninstall the Concentrator Remote Server software.

Note:

If you accepted the recommended installation location for the Concentrator Remote Server software, the location of the uninstall script is `/opt/avaya/SAL/CRS/Uninstall Axeda Enterprise`.

To uninstall the Concentrator Remote Server

1. Log in to the computer on which the Concentrator Remote Server software is installed.
2. Open a shell prompt and navigate to the directory where you installed the Concentrator Remote Server software.
3. Browse the folder and locate the `Uninstall Axeda Enterprise` directory.
4. Navigate to the `Uninstall Axeda Enterprise` directory and run the following command:

   `./Uninstall_Axeda_Enterprise`

   The system invokes the Uninstall program.
5. Press **Enter** to continue with the uninstall process.

   You can quit the Uninstall program by typing `quit` and pressing **Enter**.
6. Select an uninstall option from the following:
   - Completely remove all features and components.
   - Choose specific features that were installed.

   To select an option, type the number shown beside an option.
7. Press **Enter**.

   If you select the option to uninstall specific features, the Uninstall program gives you option to choose from the installed features. Press **Enter** after you choose features to be uninstalled.

   The uninstall process starts. When the uninstallation completes successfully, press **Enter** to quit the Uninstall program.

Importing CA certificates

Avaya periodically releases Certificate Authority (CA) certificates packages for all SAL components to avoid any service interruption that might occur due to CA certificate expiration. You can import new CA certificates released by Avaya to the Concentrator Remote Server truststore.

Installing the Certificate Refresh patch

Before importing a CA certificate package to the Concentrator Remote Server truststore, you need to install a patch. This patch creates the CACertificateRefresh directory under the Concentrator Remote Server application installation directory.

1. Log in to the system where your Concentrator Remote Server is installed.
2. Download the Certificate Refresh patch from the Avaya Support site.
3. Navigate to the directory where you have downloaded the patch.
4. Unzip the patch file, `RemoteServerCARefreshPatch.zip`, you have downloaded.
5. Run the command **`./runInstaller.sh`** from the command line.

   The command invokes the GUI-based installer and displays the Language selection panel.
6. From the list, select a language and click **Ok**. English is selected as the default language.

   The system displays the Welcome panel.
7. Click **Next**.

   The system displays the AVAYA GLOBAL SOFTWARE LICENSE TERMS panel.
8. Select **I accept the terms of this license agreement**.

   Note:

   You must accept the terms of the license agreement to continue with the installation. If you do not accept the terms of the license agreement, the installer renders the **Next** button on the panel inactive.
9. Click **Next**.

   The system displays the Executing Task panel.
10. Click **Next**.

    The system displays the Installation path panel.
11. Type the correct path of the Concentrator Remote Server application's installation directory, or click **Browse** and select the directory location.
12. Click **Next**.

    The system displays a warning that the selected directory already exists. If you use the folder, existing files may get overwritten.
13. Click **Yes** to use the existing directory.

The system displays a panel showing the packs that can be installed.

14. Select the pack and click **Next**.

    The system displays the Pack installation progress panel.

15. Click **Next** when all the files are successfully unzipped and installed.

    The system displays the Installation Summary panel. The panel displays the following information:

    - The installation status, which shows whether the installation process is complete or has failed
    - The package or packages that have been installed
    - The location of the Uninstall program

    The installer creates the `CACertificateRefresh` directory in the same location where the Concentrator Remote Server is installed.

16. Click **Done**.The system quits the installer and reverts to the command mode.

Downloading the latest CA certificate package

You can download the latest CA certificate package, delivered as a zip file, from the repository of the Secure Access Concentrator Core Enterprise Server located at Avaya.

1. Log in to the system where your Concentrator Remote Server is installed.
2. Open a Web browser and enter the address of the Secure Access Concentrator Core Enterprise Server as:

   https://*<HOST>:<PORT>*/repository/

3. On the Download Latest SAL Packages page, click the link for the zip file beside the **CA Certificates** field. The system displays the File Download dialog box.
4. Save the zip file to a location on the system and note down the path.

Importing certificates to the Concentrator Remote Server truststore

After downloading the zip file that contains the latest CA certificates, you need to import the certificates to the Concentrator Remote Server truststore.

1. Log in to the system where your Concentrator Remote Server is installed.
2. Open a command prompt.
3. Navigate to the Concentrator Remote Server application installation directory, `/<CRS_install_Path>/CACertificateRefresh`.
4. Run the following command:

   `./importCertificates.sh -packagePath <DOWNLOADED_PACKAGE_PATH>`

   Note:

   Provide the full path of the zip file on the system.

The system validates the certificate files in the zip file and updates the Concentrator Remote Server truststore to include the new certificates.

Chapter 6: Configuring the Oracle database

About this chapter

This chapter explains how to configure the Oracle database for a new installation of the Concentrator Remote Server system.

Configuring Oracle database includes the following:

- Creating the tablespaces
- Creating the database user
- Creating and initializing database tables

Configuring the database for Concentrator Remote Server

After installing the Oracle software and creating the database, you need to set up various components of the database for operation with a new installation of the Concentrator Remote Server. This process requires you to run the SQL scripts located in the `ddl` subdirectory of your Concentrator Remote Server installation directory. For details on the contents of this subdirectory, see "The ddl directory" in Appendix B, "Concentrator Remote Server Files."

To configure the database, you need to perform the following tasks:

1. Ensure that the Oracle software is installed and an Oracle database is created and running.
2. Create the tablespaces in the database.
3. Create a database user or schema (run `create_oracle_user.sql`).
4. Create and initialize the tables used to store device data and the tables used for the reports (run `create_all_tables.sql`).

Creating tablespaces

Before you create the database user and the tables, you must edit and then run one of the following scripts for your installation environment:

- `create_tablespaces_production.sql` (for production environment)
- `create_tablespaces_development.sql` (for development environment)

You can find these scripts in the `ddl/tablespaces` subdirectory of your Concentrator Remote Server installation directory. If you accepted the recommended installation location for the Concentrator Remote Server application, the file location is `/opt/avaya/SAL/CRS/ddl/tablespaces`.

To edit and run the script

1. Log in to the Oracle database server as the Database Administrator.
2. Using a text editor, open the `create_tablespaces_production.sql` script, and change the path information as appropriate, to your Oracle installation.

   The content of the `create_tablespaces_production.sql` script as it comes with the Concentrator Remote Server software in the `ddl/tablespaces` subdirectory is shown below. In this sample script, the paths you may need to edit are shown in red, italic font. All comments to help you edit are shown in blue, boldface font. For this script, you may want to search and replace the path `\ORACLE\ORADATA\ServiceLink` with the path you used for the location of the data for your Concentrator Remote Server database (for example, `d:\oradata`). You may also want to replace the Disk numbers.
3. The size information in this sample script reflects recommended settings for Concentrator Remote Server. If you require different sizes, edit that information.
4. If you require to add data file names, do so as indicated in the script.

5. Remove all the comments (shown in blue, boldface font) from the script.
6. Save the changes to the `create_tablespaces_production.sql` file and close the script file.
7. Run the `create_tablespaces_production.sql` script against your database.
8. Log out of the Oracle database server.

The create_tablespaces_production.sql script

```
--*******************************************************
Production Sample Script
--*******************************************************

CREATE TABLESPACE DRM_DATATABLE_DATA
DATAFILE 'DISK1:\ORACLE\ORADATA\DRM\DRM_DATATABLE_DATA001.DBF' SIZE 2046M,
       DISK1:\ORACLE\ORADATA\DRM\DRM_DATATABLE_DATA002.DBF' SIZE 2046M,
       DISK1:\ORACLE\ORADATA\DRM\DRM_DATATABLE_DATA003.DBF' SIZE 2046M
.. add data files as needed
EXTENT MANAGEMENT LOCAL UNIFORM SIZE 511M;
Note: The amount of storage required should be based on approximately 50 MB of storage
       for every 1 million rows of data.


CREATE TABLESPACE DRM_DATATABLE_INDX
DATAFILE 'DISK2:\ORACLE\ORADATA\DRM\DRM_DATATABLE_INDX001.DBF' SIZE 2046M,
       'DISK2:\ORACLE\ORADATA\DRM\DRM_DATATABLE_INDX002.DBF' SIZE 2046M,
       'DISK2:\ORACLE\ORADATA\DRM\DRM_DATATABLE_INDX003.DBF' SIZE 2046M
.. add data files as needed
EXTENT MANAGEMENT LOCAL UNIFORM SIZE 511M NOLOGGING;
Note: The amount of storage required should be based on approximately 50 MB of storage
       for every 1 million rows of data.


CREATE TABLESPACE DRM_CURRENTDATAVALUES_DATA
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_CURRENTDATAVALUES_DATA001.DBF'
       SIZE 75M AUTOEXTEND ON NEXT 73M MAXSIZE 1024M
       EXTENT MANAGEMENT LOCAL UNIFORM SIZE 73M NOLOGGING;

CREATE TABLESPACE DRM_CURRENTDATAVALUES_INDX
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_CURRENTDATAVALUES_INDX001.DBF'
       SIZE 36M AUTOEXTEND ON NEXT 28M MAXSIZE 511M
       EXTENT MANAGEMENT LOCAL UNIFORM SIZE 28M NOLOGGING;


CREATE TABLESPACE DRM_ALARMS_DATA
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_ALARMS_DATA001.DBF'
       SIZE 75M AUTOEXTEND ON NEXT 73M MAXSIZE 1024M
```

```
        EXTENT MANAGEMENT LOCAL UNIFORM SIZE 73M;

CREATE TABLESPACE DRM_ALARMS_INDX
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_ALARMS_INDX001.DBF'
        SIZE 36M AUTOEXTEND ON NEXT 28M MAXSIZE 511M
        EXTENT MANAGEMENT LOCAL UNIFORM SIZE 28M;

CREATE TABLESPACE DRM_AUDIT_DATA
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_AUDIT_DATA001.DBF'
        SIZE 513M AUTOEXTEND ON NEXT 73M MAXSIZE 2046M
        EXTENT MANAGEMENT LOCAL UNIFORM SIZE 73M;

CREATE TABLESPACE DRM_AUDIT_INDX
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_AUDIT_INDX001.DBF'
        SIZE 513M AUTOEXTEND ON NEXT 73M MAXSIZE 2046M
        EXTENT MANAGEMENT LOCAL UNIFORM SIZE 73M;

CREATE TABLESPACE DRM_DATA
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_DATA001.DBF'
        SIZE 513M AUTOEXTEND ON NEXT 511M MAXSIZE 2046M
        DEFAULT STORAGE (INITIAL 20K NEXT 20K MINEXTENTS 1 MAXEXTENTS 249 PCTINCREASE
        50);

CREATE TABLESPACE DRM_INDX
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_INDX001.DBF'
        SIZE 513M AUTOEXTEND ON NEXT 511M MAXSIZE 2046M
        DEFAULT STORAGE (INITIAL 20K NEXT 20K MINEXTENTS 1 MAXEXTENTS 249 PCTINCREASE
        50);

CREATE TABLESPACE DRM_CUSTOM_DATA
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_CUSTOM_DATA001.DBF'
        SIZE 10M AUTOEXTEND ON NEXT 5M MAXSIZE 100M
        DEFAULT STORAGE (INITIAL 20K NEXT 20K MINEXTENTS 1 MAXEXTENTS 249 PCTINCREASE
        50);

CREATE TABLESPACE DRM_CUSTOM_INDX
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_CUSTOM_INDX001.DBF'
        SIZE 10M AUTOEXTEND ON NEXT 5M MAXSIZE 100M
        DEFAULT STORAGE (INITIAL 20K NEXT 20K MINEXTENTS 1 MAXEXTENTS 249 PCTINCREASE
        50);

CREATE TABLESPACE DRM_SOAP_UPDATE_HISTORY_DATA
        DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_SOAP_UPDATE_HISTORY_DATA001.DBF'
        SIZE 75M AUTOEXTEND ON NEXT 73M MAXSIZE 2046M
        EXTENT MANAGEMENT LOCAL UNIFORM SIZE 73M;
```

```
CREATE TABLESPACE DRM_SOAP_UPDATE_HISTORY_INDX
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_SOAP_UPDATE_HISTORY_INDX001.DBF'
       SIZE 30M AUTOEXTEND ON NEXT 28M MAXSIZE 2046M
       EXTENT MANAGEMENT LOCAL UNIFORM SIZE 28M;

CREATE TABLESPACE DRM_USAGE_INDX
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_USAGE_INDX001.DBF'
       SIZE 10M AUTOEXTEND ON NEXT 5M MAXSIZE 1024M
       EXTENT MANAGEMENT LOCAL UNIFORM SIZE 5M;

CREATE TABLESPACE DRM_USAGE_DATA
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_USAGE_DATA001.DBF'
       SIZE 10M AUTOEXTEND ON NEXT 5M MAXSIZE 1024M
       EXTENT MANAGEMENT LOCAL UNIFORM SIZE 5M;

CREATE TABLESPACE DRM_SCRIPT_INDX
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_SCRIPT_INDX001.DBF'
       SIZE 10M AUTOEXTEND ON NEXT 5M MAXSIZE 1024M
       EXTENT MANAGEMENT LOCAL UNIFORM SIZE 5M;

CREATE TABLESPACE DRM_SCRIPT_DATA
       DATAFILE 'DISK3:\ORACLE\ORADATA\DRM\DRM_SCRIPT_DATA001.DBF'
       SIZE 10M AUTOEXTEND ON NEXT 5M MAXSIZE 1024M
       EXTENT MANAGEMENT LOCAL UNIFORM SIZE 5M;

CREATE TABLESPACE DRM_REPORTING_DATA
       DATAFILE 'DISK1:\ORACLE\ORADATA\DRM\DRM_REPORTING_DATA001.DBF'
       SIZE 513M AUTOEXTEND ON NEXT 511M MAXSIZE 2046M
       DEFAULT STORAGE (INITIAL 20K NEXT 20K MINEXTENTS 1 MAXEXTENTS 249 PCTINCREASE
       50);

CREATE TABLESPACE DRM_REPORTING_INDX
       DATAFILE 'DISK1:\ORACLE\ORADATA\DRM\DRM_REPORTING_INDX001.DBF'
       SIZE 513M AUTOEXTEND ON NEXT 511M MAXSIZE 2046M
       DEFAULT STORAGE (INITIAL 20K NEXT 20K MINEXTENTS 1 MAXEXTENTS 249 PCTINCREASE
       50);
```

Creating the database user

To enable the Concentrator Remote Server to communicate with the database, you must create a user name and password, and assign the user name with permissions to the database.

To create a database user

1. Using a text editor, open the `create_oracle_user.sql` script. You can find this script in the `ddl` subdirectory of your Concentrator Remote Server installation directory. For example, `/opt/avaya/SAL/CRS/ddl`.
2. Change the schema user name in the script by replacing {USERNAME} to the name you want to use for the Concentrator Remote Server.
3. Change the password in the script by replacing {PASSWORD} to the password you want to use. In the following example, the places in the script where you need to make changes are shown in red font:

```
create user ServiceLink
      identified by knil32ecivres
      default tablespace DRM_DATA
      temporary tablespace TEMP;
commit;
...
grant query rewrite, ...
      unlimited tablespace to ServiceLink
```

   where the user name is `ServiceLink` and the password is `knil32ecivres`. This example uses the default tablespace, `DRM_DATA`.
4. Save and close the script file.
5. Log in to the Oracle database server as the Database Administrator.
6. Run the **`create_oracle_user.sql`** script against your database.

   This script creates a user (the name you supplied), defines the default tablespace as `DRM_DATA` and the temporary tablespace as `TEMP`, and then defines the privileges for that user and schema.
7. Log out of the Oracle database server.

The following example changes the default tablespace to `USERS` and creates the user `ServiceLinkadmin` with a password `walnutCreek344`.

```
create user ServiceLinkadmin
      identified by walnutCreek344
      default tablespace USERS
      temporary tablespace TEMP;
commit;
```

When the script runs with these changes, the user `ServiceLinkadmin` is created in the tablespace `USERS`. The temporary tablespace `TEMP` is also created.

The next part of the script grants the user the necessary rights to create sessions, tables, views, sequences, and stored procedures. In addition, it gives the user unlimited tablespace.

```
grant query rewrite,
      create session,
      create table,
```

```
        create view,
        create sequence,
        create procedure,
        create any trigger,
        create any type,
        create any index,
        create materialized view,
        unlimited tablespace to ServiceLinkadmin;
commit;
```

After you create a database user, you must create and initialize the tables in the database.

Creating and initializing database tables for a new system

To create and configure the database tables, you need to log in to the database server as the new user created using the `create_oracle_user.sql` script.

To create and initialize the database tables

1. Log in to the Oracle database server as the database user created for Concentrator Remote Server.
2. Run the `create_all_tables.sql` script. The script is located in the `ddl` subdirectory of your Concentrator Remote Server installation directory (for example, `/opt/avaya/SAL/CRS/ddl`).

   For most installations, all the tables that you need are created and initialized by this script.

Chapter 7: Installing and configuring the Reporting software

About this chapter

The Concentrator Remote Server provides tools for creating, scheduling, generating, and viewing reports and dashboards. Cognos 8 Business Intelligence provides the reporting engine for Concentrator Remote Server. The Cognos 8 reporting and dashboard capabilities are fully integrated with Concentrator Remote Server and used to provide users with powerful tools for report and dashboard operations.

Overview of Cognos 8 integration briefly describes how the Secure Access Concentrator Remote Server can use the Cognos 8 server for reporting, including creating new reports, modifying existing reports, scheduling reports for running, and viewing generated reports.

Reporting tools briefly describes the Query Studio and Report Studio tools that are available with Cognos 8 Business Intelligence.

Licensing options describes the various licensing options for SAL reporting.

Installing Cognos 8 with Concentrator Remote Server explains how to install the Cognos 8 server.

Configuring Cognos 8 to communicate with the Concentrator Remote Server explains how to configure Cognos 8 server for SAL operations.

Modifying properties for the Concentrator Remote Server explains how to modify the DRMConfig.properties so that the Concentrator Remote Server can work with the Cognos 8 server.

Running reports in the applications explains how to use the Report tab in Applications to view and run reports to test the Cognos 8 configuration.

Overview of Cognos 8 integration

Avaya provides a Cognos 8 Business Intelligence package based on server license. The server installation does *not* install the Cognos 8 tools. You must install these tools separately, as explained in this chapter.

When fully installed and configured, the Cognos 8 tools are seamlessly integrated with the Applications UI in the following areas:

- Report - This application uses Cognos 8 tools for creating reports, scheduling reports, viewing reports, and managing report distribution. The Report application is available in all standard server releases; however, to use the Cognos 8 tools, you must purchase a separate license. The standard release includes only the Standard Report Pack and the abilities to run and view these reports.
- Dashboard - This application uses Cognos 8 tools for creating, editing, and deleting dashboards. The Dashboard application is available based on server license.
- Administration - The Report tools of this application enable you to assign privileges to users for the Report and Dashboard applications. Also, from Report Administration you can manage reports, report content, and portal configuration.

Reporting tools

SAL provides two components of the Cognos 8 software for creating reports:

- Query Studio (Cognos 8 Query Studio) - You can use this tool to create or edit Ad hoc reports. Ad hoc reports provide a quick and easy way to access SAL data. Well suited for finding information immediately and displaying it quickly, ad-hoc reports are more limited in formatting and functionality and therefore, less appropriate for wide distribution. For more robust report formatting and functionality, use Report Studio.
- Report Studio (Cognos 8 Report Studio) - Report Studio provides advanced report development tools, including a variety of formatting options and added data processing capability. Professional Reports are appropriate for redistribution. You can create them once, generate them as often as required, and distribute them to many users in multiple languages on a regular basis.

Licensing options

The standard Secure Access Concentrator Remote Server license provides access to the Report application and includes the ability to run and view the standard reports provided with the server. When running reports, users can select the product families, device groups, devices, date and time range, accounts, and so on, that they want to see in the generated report. However, the standard license does not provide access to Cognos 8 Query Studio or Cognos 8 Report Studio, so users cannot edit the reports. Further, they cannot schedule, publish, or delete these reports. The standard reports are all fully documented in the *Report Pack: Standard Reports Reference Guide*, included with your server installation in Adobe Portable Document Format (PDF).

Licenses for reporting tools and dashboard tools are separate. However, a license for Report is a prerequisite for a license for Dashboard. In addition, at least one Query Studio license is required for a Report license.

With the Report license, users can create new reports, modify report content, schedule report generation, configure report distribution, publish reports for access by others, and so on. In addition, SAL administrators can restrict the use of the Query Studio and Report Studio tools to specific *named users*. The number of named users is restricted by license. With the Dashboard license, users can access the Dashboard Application and its tools for creating, editing, and deleting dashboards.

Administration provides the tools for specifying which Applications users can use the Report Studio and Query Studio tools. A SAL administrator who has the appropriate privileges to the Administration application can select which Applications users are named users for Report Studio and which are named users for Query Studio. When these named users display the Report application, they will be able to launch the assigned tool.

Administration application provides for the configuration of three types of named users:

- Named users for Report Studio
- Named users for Query Studio
- Named users for report administration.

Only individuals defined as named users for report administration can specify Applications users as named users for Report Studio or Query Studio. Named users with administrative privilege for Report can use the Content Administration tool, update the report pack, and more.

See the online help for complete details.

Installing Cognos 8 with Concentrator Remote Server

This section explains the following steps to installing and configuring Cognos 8 Business Intelligence Server 8.2:

1. Installing Cognos 8. See Installing Cognos 8 for SAL.
2. Copying required files from JDK and Oracle installations to Cognos 8 installation. See Copying files to Cognos 8 installation.
3. Configuring the Apache Web server for Cognos 8. See Configuring Apache for Cognos 8.
4. Starting the Apache Web server after configuration.
5. Configuring Cognos 8. See Configuring Cognos 8 to communicate with the Concentrator Remote Server.
6. Modifying Concentrator Remote Server properties. See Modifying properties for the Concentrator Remote Server.
7. Selecting and running reports in the Applications. See Running reports in the Applications.

Prerequisites to install the Cognos 8 software

Before you start the installation, consider the prerequisites described in this section.

Cognos Report Server

- Have you allocated the target computer on which you will install the Cognos 8 components? You can use the same computer as the Concentrator Remote Server or a different computer.
- Does your system meet the following requirements for a Cognos 8 server?

RAM	A minimum of 1 GB of RAM available; 2 GB of RAM is recommended.
Disk space	A minimum of 2.5 GB of free space is available for installation, and 1 GB of free space on the drive that contains the temporary directory used by Cognos 8 components.
Web server	You must install and configure a Web server for Cognos 8. The Web server must be started prior to testing the Cognos 8 configuration. Avaya recommends that you start the Web server before starting the Cognos 8 Configuration tool. For UNIX installations, make sure Apache (the recommended Web server) is installed on the Cognos 8 server before starting the Cognos 8 Configuration tool. If Apache is not already installed and configured, see the Apache installation and configuration procedures provided in this chapter.

- Java Runtime Environment (JRE) - Cognos 8 requires the JRE installed with and used by the JBoss Server. Set up a JAVA_HOME environment variable to point to the JDK installation, and then, after installing the Cognos 8 server software, rename the Cognos 8 JRE directory by appending "DO_NOT_USE" to its name. Also, make sure you set the PRINTER environment variable to the name of your printer.
- Sun Java - To run on Linux machines, Cognos 8 requires Sun Java.
- XWindows - For UNIX installations, the intended Cognos 8 server must be installed with an XWindows server (or other Java-based graphical user interface) to run the graphical installation program presented in this chapter.
- Make sure that you append the `c8_install_location/bin` directory to the appropriate library path environment variable. For Linux, that variable is `LD_LIBRARY_PATH`.
- Network - Make sure the Cognos 8 server can communicate with the intended Concentrator Remote Server, Oracle database server, and designated directory server.

Oracle database for the SAL system

- The Oracle database must be in UTF-8 format. Note that UTF-8 format is recommended for SAL as well.
- Before the Cognos 8 tools are installed, the Oracle client must be installed and pointing to the Cognos 8 database schema and SAL database schema.

SAL components

- Avaya recommends that you install and configure all other SAL components first, including the following:
  - The Web server
  - The directory server to use for authenticating user access
  - The database software
  - The JBoss Server
  - The Concentrator Remote Server

Supported platforms

In general, the Cognos 8 software can be installed and run on the Linux platform for operations with Concentrator Remote Server. This book does not provide complete information about the supported software components for SAL and Cognos 8. Contact Avaya for that information, if needed.

Installing Cognos 8 for SAL

This section explains how to install the Cognos 8 server and configure it to work with the Concentrator Remote Server and other components of the SAL system. To ensure that

installation and configuration of the Cognos 8 server are successful, make sure that you install the Avaya customized files for use with Cognos 8 to the correct location.

Install the Cognos 8 server first, and then add the customized files for SAL to that installation, in the following directory: `<Cognos_installation>/cognos`. The customized files include the Report Pack and the authentication provider files. The Report Pack contains Query Objects for reporting, as well as standard reports and dashboards. When you configure Cognos 8 reports, the Cognos 8 Configuration tool needs to access this file.

Depending on whether you received your SAL software through the FTP site or on CDs, the exact location of the installation files is slightly different. See the *Documentation Roadmap* PDF provided with your installation kit to determine the location the report installation files for your operating system.

After you insert the CD, you can find the installation archive for each platform in the `cognos_82_server` subdirectory of the `<platform>_image` directory. Similarly, you can find the SAL customized files in the `_reporting` subdirectory of the `<platform>_image` directory. The <platform> name is linux_x86.
Continue to the installation instructions for your platform.

Note:

Avaya strongly recommends that you install the Cognos 8 server on a dedicated computer (that is, *not* on the same computer as the JBoss and Concentrator Remote Servers). However, if you do install it on the same computer as the JBoss Server and Concentrator Remote Server, then be sure to set up an environment variable, JAVA_HOME, that points to the JDK installation (for example, `/Java/jdk1.5.0_10/bin`) and then append "DO_NOT_USE" to the name of the Cognos 8 JRE directory (for example, change `c:/Program Files/cognos/c8/bin/jre/1.4.2` to be `1.4.2_DO_NOT_USE`).

Cognos 8 for UNIX

Make sure you have reviewed the prerequisites before installing Cognos 8. See Prerequisites to install the Cognos 8 software.

You do not need to have Root access to install and configure the Cognos 8 report server for your Linux servers.

The Cognos 8 installer is provided in a tar gzip file. Separate archives are provided for Linux:

- Linux - *c8bisrvr_linuxi386_8.2.43.128.ml.tar.gz*

Before starting the installation, you need to copy the Cognos 8 archive to the intended Cognos 8 server and extract the content. The archives are located within the SAL installation media. See the *Documentation Roadmap* PDF for help locating the archives.

After extraction, the installation program for a Linux server is located in the `linuxi386` directory.

To install the Cognos 8 server on a UNIX platform

1. If you are installing to a directory with other Cognos 8 components, stop the Cognos 8 service.

2. Set the environment variable to point to the installation location of your Java Runtime Environment (JRE). A typical JRE installation location would be `/directory/java/java_version/jre`.
3. As long as you have extracted the contents of the installation archive for your platform, open a shell and navigate to the directory containing the installation program, `issetup`.
4. To start the installation wizard,
   - If you use XWindows, type **./issetup**
   - If you do not use XWindows, type **./issetupcc**

   Note:

   The installation and configuration procedures in this chapter are written based on using XWindows. Avaya recommends that you use XWindows and the issetup installation wizard.
5. For the most part, follow the directions in the installation wizard and copy the required files to your computer. Read the following information before continuing:
   - Select to install all Cognos 8 components, except for the Cognos Content Database.
   - Make sure you install Cognos 8 components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names; make sure the target directory contains only ASCII characters.
   - By default, the installer will create the Cognos 8 server installation in the `/cognos` directory.

   Before starting the Cognos Configuration tool, you need to perform some additional steps, including copying files to the Cognos installation.
6. On the Finish page of the installation wizard, close the wizard *without* starting the Cognos Configuration tool.

Copying files to Cognos 8 installation

For the Cognos 8 server to run properly and deliver the Avaya reports, you need to copy the Avaya customized files and the JDBC JAR file from the Oracle client installation. The Avaya customized files for the Report and Dashboard applications are located in the subdirectory, _reporting/cognos/c8, for your platform. Within this directory, the files that you need to copy to the Cognos 8 installation are organized into subdirectories of the same names as in the Cognos 8 installation.

The customized reporting files provide the following functionality for SAL:

- Report Pack - The *ServiceLink_CS.zip* file contains the Report Pack files, including reporting Query Objects, standard reports, dashboards, and content store. See the *Report Pack* document for information about the standard reports and query objects.
- Authentication file - The *axeda-cognosauth.jar* file enables the Concentrator Remote Server to pass the user login information to the Cognos 8 report server so that when users log in to the Concentrator Remote Server, they are also logging in to the

Cognos 8 Report server (this dual login assumes that the user group privileges for those users allow them to access Report and its tools).

To copy the files for Cognos 8 operations

1. Navigate to the `_reporting/cognos/c8` directory of your SAL installation media.
2. Copy the entire contents of the `c8` directory to the `c8` directory of the Cognos 8 installation, `cognos/c8`. If you did not use the default location for the Cognos 8 installation, replace `/cognos` with the actual Cognos 8 installation location. If prompted whether to extract an archive and replace existing files, answer Yes.
3. Navigate to the `/jdbc/lib` folder of your Oracle client installation.
4. Depending on your version of Oracle, copy either the jdbc14.jar file or the classes12.jar file from the Oracle client installation to the Cognos 8 directory, `/cognos8/webapps/p2pd/ WEB-INF/lib`. If you did not use the default location for the Cognos 8 installation, replace `/cognos8` with the actual Cognos 8 installation location.

Setting environment variables

Make sure you set the environment variables for your server. You need to ensure the following settings in your /etc/profile file are accurate for your server installation:

- The environment variable must point to your JDK location.
- The ORACLE_HOME environment variable must point to the Oracle (client) installation directory.
- The PATH variable must provide the correct JDK and Oracle home settings.
- The LD_LIBRARY_PATH variable must identify the Cognos 8 */cgi-bin* location and the Oracle home */lib* location.

The exact settings vary based on your server environment. An example set of environment variables is as follows:

```
=/opt/jdk1.5.0_02
ORACLE_HOME=/oracle/product/10.2.0
PATH=$PATH:/opt/jdk1.5.0_02/bin:ORACLE_HOME/bin
export PATH ORACLE_HOME
export LD_LIBRARY_PATH=/opt/cognos/c8/cgi-bin:$ORACLE_HOME/lib
```

You can run ldconfig to make sure all libraries for the module are available. The following would be an ldconfig example for the above example environment variables:

```
ldconfig -l /apps0/cognos/c8/cgi-bin/libhttpdap2_stub.so
```

Configuring Apache for Cognos 8

The Apache Web server should be installed and configured on the Cognos 8 server prior to configuring and running Cognos 8. For the purposes of this procedure, the Apache Web server should be installed already. These notes explain how to configure the Web server for SAL.

Cognos 8 will work with Apache 1.3.x and 2.0. Note that Apache 2.0 is required for Linux installations. The configuration instructions for the versions differ and both are provided in

this chapter. Follow the configuration instructions for your version of the Apache Web server.

1. Stop the Apache Web server.
2. Append the `<cognos8_location>/cgi-bin` directory to the environment variable: LD_LIBRARY_PATH
3. Go to the `<Apache_installation>/conf` directory.
4. Open the `httpd.conf` file in an editor.
5. For Apache 1.3.x only:

   Add the following to the end of the add module list
   ```
   AddModule mod_cognos.cpp
   ```
6. Add the following to the aliases section, where the <*Directory*> directive is optional; quotes are required where shown:

   ```
   ScriptAlias /cognos8/cgi-bin "c8_location/cgi-bin"
   Alias /cognos8 "c8_location/webcontent"
   <Directory "c8_location/webcontent">
   Options Indexes MultiViews
   </Directory>
   ```

Tip:
Ensure that you define the cognos8/cgi-bin alias *before* the cognos8 alias.

7. Add the following to the server status reports section:

   ```
   <Location /cognos8/cgi-bin/cognos_module>
         SetHandler cognos-handler
   </Location>
   ```
8. To enable the gateway diagnostic page, add the following to the server status reports section, where the diag_ string is required.

   ```
   <Location /cognos8/cgi-bin/diag_cognos_module>
         SetHandler cognos-handler
   </Location>
   ```
9. Add support to the user directory section, as follows; quotes are required where shown:
   - For Apache 1.3.x, add the following:

     ```
     <IfModule mod_cognos.cpp>
           CGIBinDir "c8_location/cgi-bin"
     </IfModule>
     ```
   - For Apache 2.0, add the following:

     ```
     <IfModule mod_cognos.c>
           CGIBinDir "c8_location/cgi-bin"
     </IfModule>
     ```
10. Save and close the file.
11. Start the Apache Web server.

12. In the Cognos Configuration tool, configure the **Gateway URI** property to use the apache_mod gateway, as follows:

    http://host_name:port/cognos8/cgi-bin/filename

    where filename matches the name that you used in step 9.

Now you should save and then start the Apache Web server. Avaya recommends that you start Apache before starting the Cognos 8 configuration.

Default installation paths

The Cognos Installer copies the Cognos 8 files to the directory that you specified in the wizard. Table 7-1 lists and briefly describes the default configuration settings and the directories associated with these settings.

Table 7-1 Default Cognos 8 Installation Settings

Setting	Description	Default value
Content Manager URI	The URI to Content Manager	http://localhost:9300/p2pd/servlet
Gateway URI	The URI to the gateway	http://localhost:80/cognos8/cgi-bin/cognos.cgi
Dispatcher URI (Internal, External)	The URI to the dispatcher	http://localhost:9300/p2pd/servlet/dispatch
Dispatcher URIs for Gateway	The URI to the primary dispatcher used by the gateway	http://localhost:9300/p2pd/servlet/dispatch/ext
Log server port	The port used by the local log server	9362
Listening port number	The port used by Cognos Content Database	1527

These settings are all defined in the *cogstartup.xml* configuration file, which is located in the Cognos 8 installation, *configuration* directory. You can modify the settings in this file after installation.

Now you can start the Cognos 8 Configuration Tool. The next section explains how.

Configuring Cognos 8 to communicate with the Concentrator Remote Server

You need to configure the Cognos 8 server to communicate with the Concentrator Remote Server. This configuration enables the Cognos 8 server to use data defined in the SAL database and users defined in the SAL LDAP directory server to access the Cognos 8 report tools. In addition, you need to add the SAL reporting objects (predefined reports and dashboards as well as Query Objects) and authentication files to the Cognos 8 server.

To start the Cognos 8 configuration tool

Go to the *c8_location/bin* directory and type **./cogconfig.sh.**

Note:

To start Cognos 8 from the command line, use one of the following:

- Use the startup script for Cognos 8, which is startup.sh. It is located in the /bin directory of Cognos. The startup.sh script will start the JVM and will also start Tomcat. Startup.sh must be run by the same user who owns all of the Cognos 8 files. (If the server is started by another user, issues with permissions may occur).
- Use the command and argument **`cogconfig.sh -s`** to start Cognos 8 automatically as a daemon on Linux.

The Cognos Configuration tool appears, as shown in Figure 7-1.

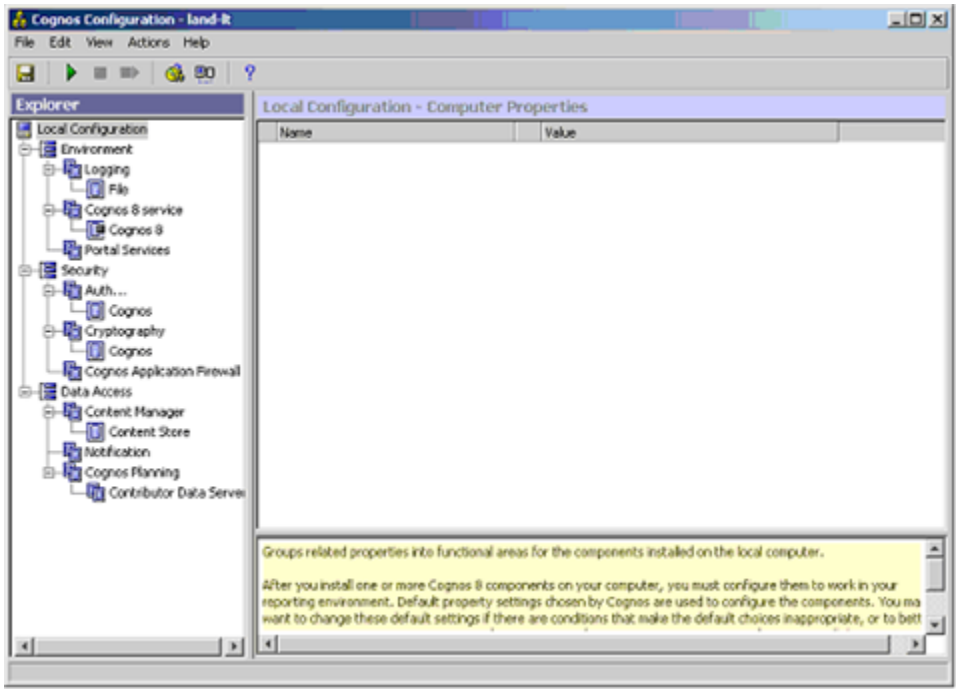


Figure 7-1: Opening the Cognos Configuration tool

The Cognos 8 installer creates a default Content Store. For the purposes of your SAL system, you will **not** be using this default Content Store. Your first step is to delete the default Content Store.

To delete the default content store

1. In the Explorer pane of the Cognos Configuration tool, navigate to **Data Access > Content Manager > Content Store**.
2. Right-click **Content Store** and click **Delete** to remove the default Content Store, as shown in the following figure.

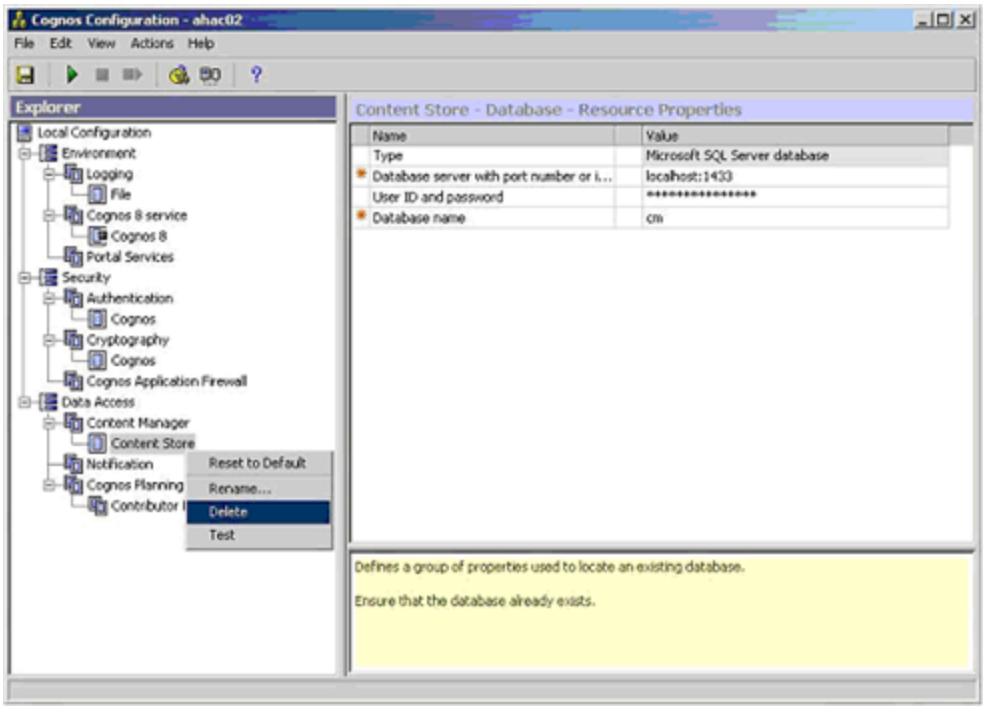


Figure 7-2: Deleting the default Content Store

3. When prompted to confirm the deletion, click **Yes**.

After deleting the default content store, you need to create the content store (a *database resource*) for the SAL system.

To create the Content Store for SAL

1. In the Explorer pane, navigate to **Data Access > Content Manager**.
2. Right-click **Content Manager**, and on the context menu, point to **New Resource** and then click **Database**, as shown in the following figure.

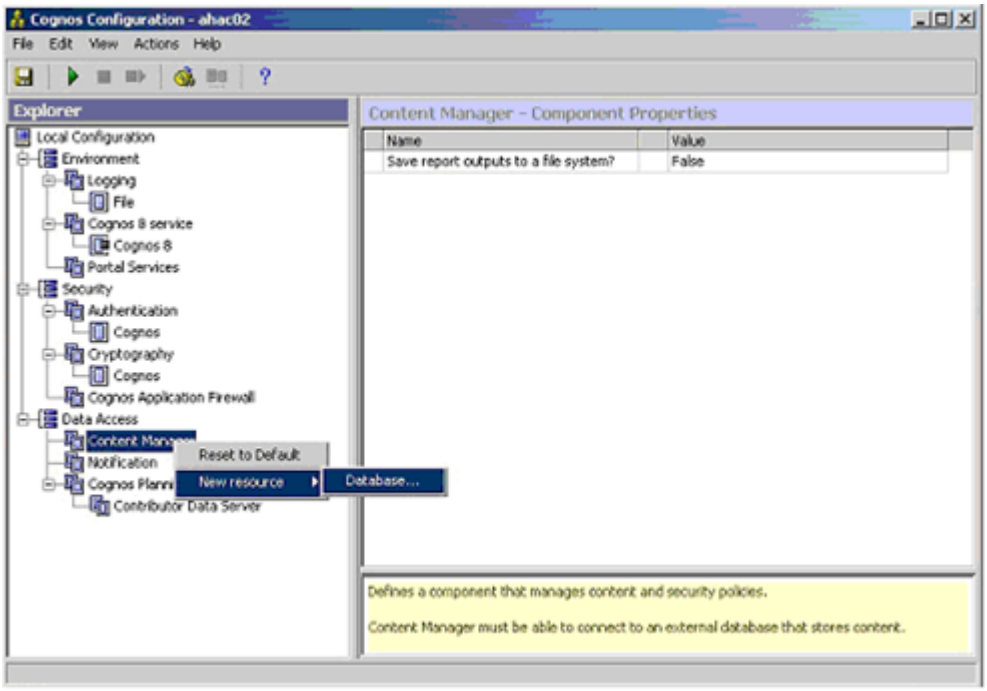


Figure 7-3: New Resource - Database selection

Figure 7-4 shows an example of the New Resource - Database dialog box, with the information you need to enter:

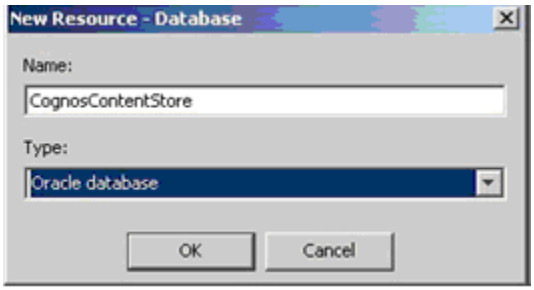


Figure 7-4: Creating a new data source

3. In the New Resource - Database dialog box, type the name for the resource: CognosContentStore.
4. From the **Type** list, select **Oracle database**.
5. Click **OK** to create the new Content Store.

The name, CognosContentStore appears under Content Manager in the Explorer pane, and its properties appear in the right side of the window, as shown in the following figure.

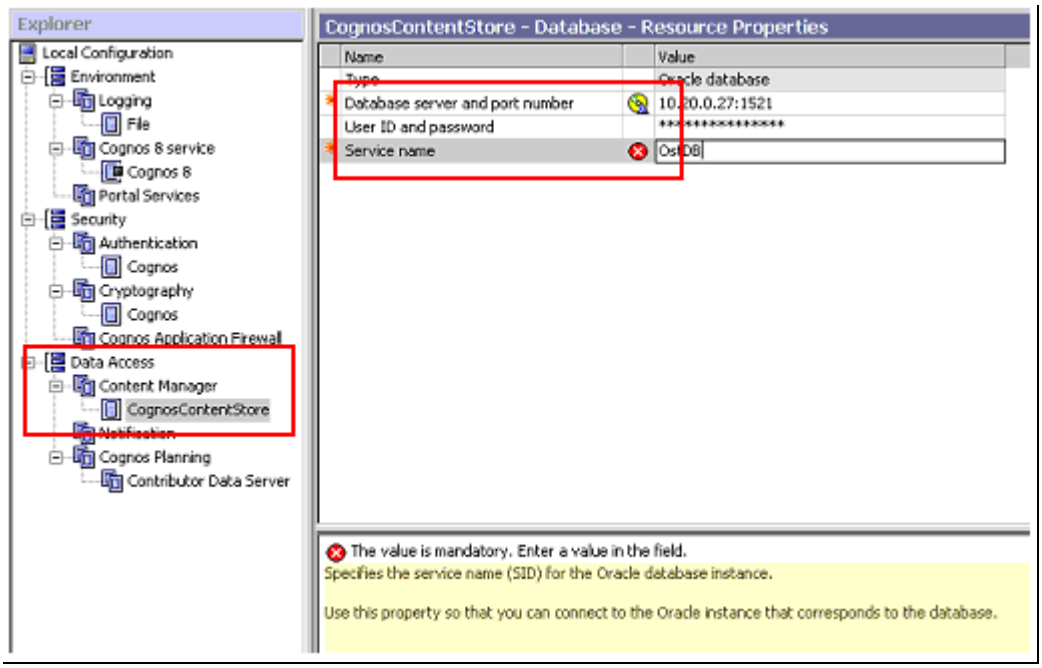


Figure 7-5: CognosContentStore properties

6. In the **Database server and port number** field, type the actual IP address or system name and the port number for your database server, as provided by your Database Administration team. This information is required. Use the following format: `address:port`. If the database is located on the same system, you can use *localhost.*
7. In the **Service name** field, type the SID defined in *TNSnames.ora* for the SAL schema. Obtain this information from your Database Administration team. This field is required.
8. As shown in the following figure, select the **User ID and password** field and then click the icon at the end of the field to bring up the Value - User ID and password dialog box.

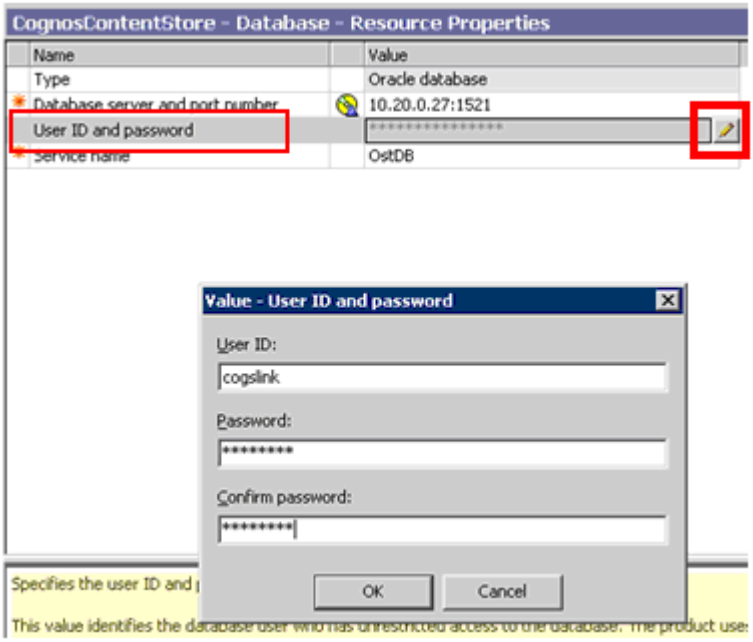
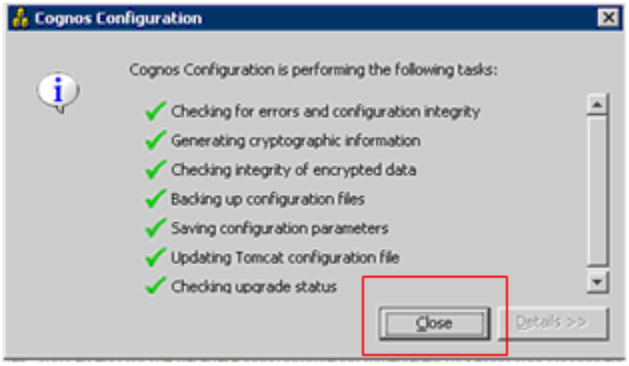


Figure 7-6: User name and password for content store

9. In the Value dialog box, type the user name and password information that you want to use for the Cognos 8 account.
10. Click **OK** to save the information and close the dialog box.
11. Click the Save icon ( ) to save the configuration to this point. The following figure shows the location of this icon.

A screen showing the progress of the save process appears, as shown in the following figure.

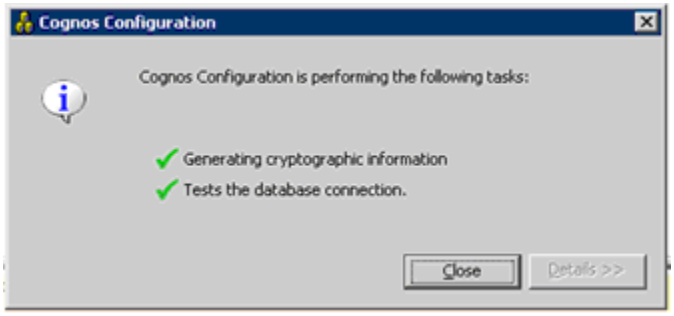


12. When the save process is complete, click **Close**.

Now you can test the database connection.

To test the configuration

1. In the Explorer pane, right-click **CognosContentStore**, and on the context menu, click **Test**. The Cognos Configuration tool displays the following dialog box:



You should see that the test is successful.

To set the environment

1. In the Explorer pane, click **Environment** to display the Environment - Group Properties page. Figure 7-7, which follows, shows an example of this page.
2. The only settings that need to change are those relating to the Web server that currently points to `http://localhost:80/` and should be replaced with `http://localhost:8080/`, as shown in the following figure.
3. To save your changes, click ( ).

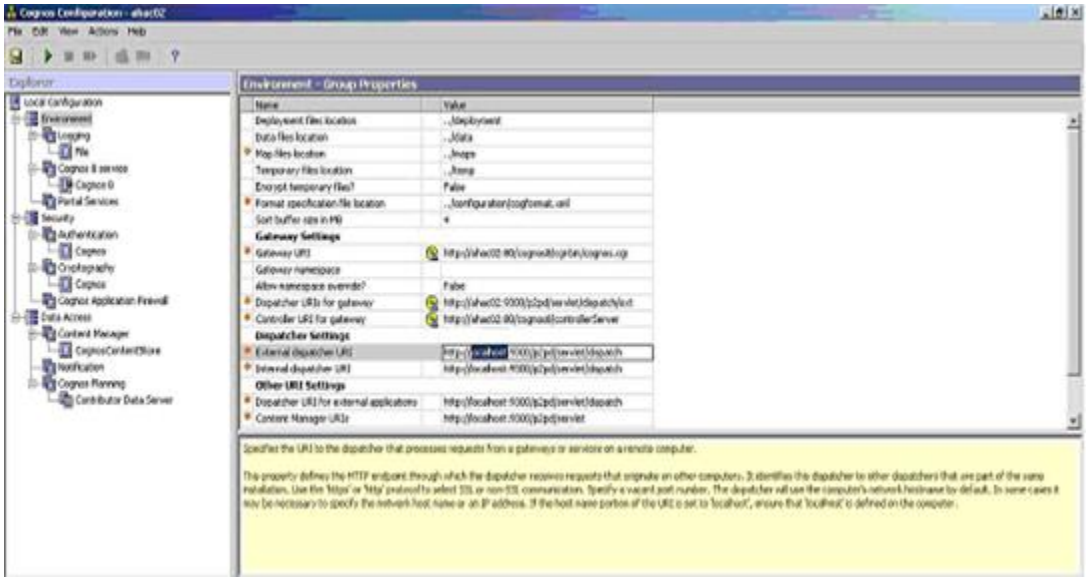


Figure 7-7: Update all Environment - Group Properties to actual system name

To disable the Cognos 8 application firewall

1. In the Explorer pane, browse to **Security > Cognos 8 Application Firewall.**

   The Cognos 8 Application Firewall - Component Properties page appears in the right pane, as shown in Figure 7-8.

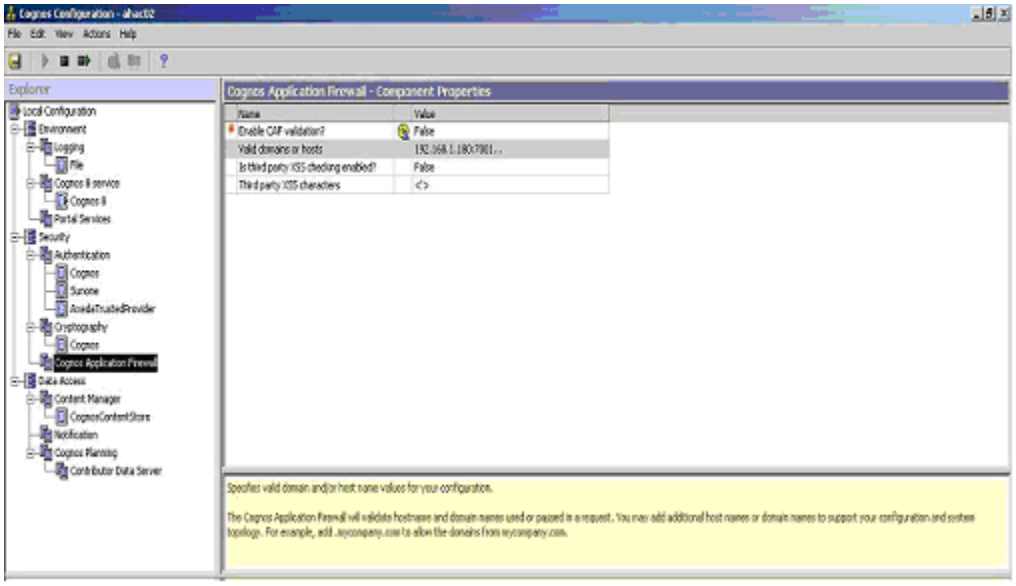


Figure 7-8: Firewall configuration properties

2. Specify the following values:
   a. Set **Enable CAF Validation?** to `False`.
   b. Select **Valid domains or hosts** and click the Pencil ( ) icon.
   c. In the displayed dialog box, click **Add** and specify each of the addresses (*ip address:port*) with which this Cognos 8 server will communicate. These addresses can include Concentrator Remote Servers, LDAP Authentication servers, and Oracle database servers.
   d. Click **OK**.

   Next, you need to disable the anonymous authentication and change the inactivity timeout setting.

To start the Cognos 8 server

1. To start the Cognos 8 server, click . A window appears, showing the status of checking the upgrade and then registering and starting the Cognos 8 service. If any of these fail, see the information in the error pane (lower part of the screen) to troubleshoot a problem.
2. After the service starts successfully, open a Web browser and browse to the Cognos 8 server; for example, type *http://cognos_server/cognos8* in the URL line. The Welcome screen appears:

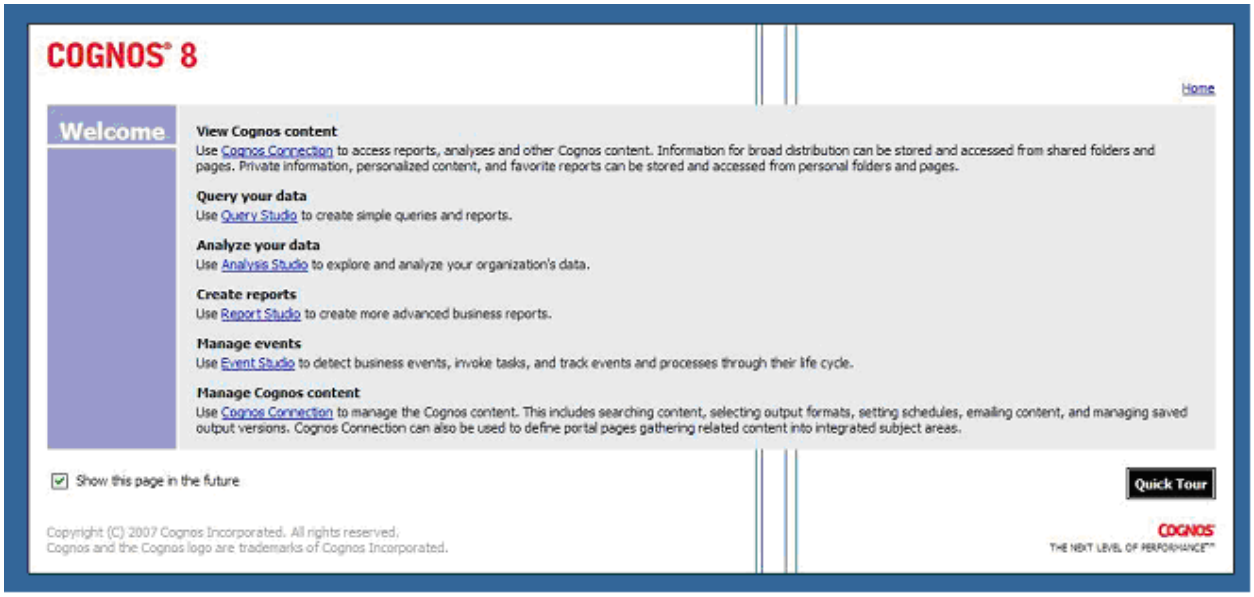


Figure 7-9: Cognos 8 Server - Welcome screen

3. On the Welcome screen, click **Cognos Connection** to display its UI, which should look similar to the following figure.

Figure 7-10: Run Cognos Connection to verify configuration

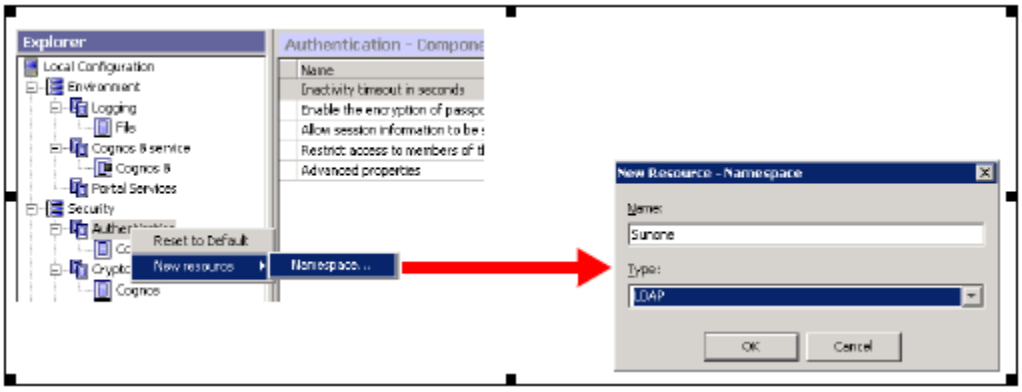
Next, continue with the Cognos Configuration Tool to define the authentication provider.

To configure the AxedaNameSpace namespace/authentication provider

Important:

You must use the name, AxedaNameSpace, no matter which directory server you are using.

1. Change back to the Cognos Configuration tool.
2. In the Explorer pane, navigate to **Security > Authentication**.
3. Right-click **Authentication** and select **New resource > Namespace** to display the New Resource - Namespace dialog box. The following figure illustrates the step.



4. In the **Name** field, type `AxedaNameSpace`.
5. From the **Type** list, select the type of Authentication provider used for SAL, `LDAP` or `Active Directory`.
6. To create the authenticator resource, click **OK**:

   The new authentication provider resource appears in the Explorer pane, under the **Authentication** component.
7. On the Namespace - Resource Properties page that appears in the right pane, enter the namespace ID (`AxedaNameSpace`) and all other values so that Cognos 8 can locate and use the defined authentication provider.

   You can enter some values directly on this page. For the others, click the pen icon to open a separate dialog box and then enter the values in the displayed dialog box. The information you enter here includes:

   - The **Namespace ID** field displays `AxedaNameSpace`.
   - In the **Host and port** field, type the IP address, or domain name, and port number of the Directory Server host used for the SAL system.
   - In the **Base Distinguished Name** field, type the same Base Distinguished Name as the one defined for SAL; the default required for SAL follows:

     ```
     dc=avaya, dc=com
     ```
   - In the **User lookup** field, type the User ID as defined for the SAL Directory Server:

     ```
     uid=${userID},ou=People,dc=avaya,dc=com
     ```
   - Select **Use external identity mapping?** and in the displayed list, select **true** to use external identify mapping.
   - In the **External identity mapping** field, set the external identity mapping to that used for the SAL Directory Server, by default:

     ```
     uid=${environment("REMOTE_USER")},ou=People,dc=avaya,dc=com
     ```
   - Select **Bind user DN and password**, click the Pencil icon ( ), and in the displayed dialog box, specify the following:

- In the **User ID** field, type a value that matches the values set for the LDAP Principal User for SAL:

  `uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot`

- In the **Password** field, type the Administrative user password defined for the SAL directory server.

8. Click **Save** ( ) to save the configuration to this point.

Additional steps for Active Directory

If you are using Active Directory, you need to configure additional properties for sign on. If you are using Sun ONE LDAP, you can skip these steps and continue with the procedure, To test the AxedaNameSpace authentication provider.

1. On every computer where you installed Content Manager, open the Cognos Configuration tool.
2. In the Explorer pane, under **Security - Authentication**, click **AxedaNameSpace.**
3. Click in the **Value** column for Advanced properties and then click **Edit**. The Value - Advanced properties page appears.
4. Click **Add**.
5. Specify the following values:
   - Name — type *singleSignonOption*
   - Value — type *IdentityMapping*
6. Click **OK**.
7. Click in the **Value** column for Binding credentials and then click **Edit**. The Value - Binding credentials page appears.
8. Type a user ID and password and click **OK**.

   The Active Directory provider now uses REMOTE_USER for single sign in.

Tip:

To switch back to Kerberos delegation, edit Advanced properties and, in the **Value** column, type `KerberosAuthentication`.

You now need to test the connection to the SAL Directory Server.

To test the AxedaNameSpace authentication provider

1. In the Explorer pane, navigate to **Security > Authentication > AxedaNameSpace**.
2. Right-click **AxedaNameSpace** and click **Test**, as shown in the following figure.

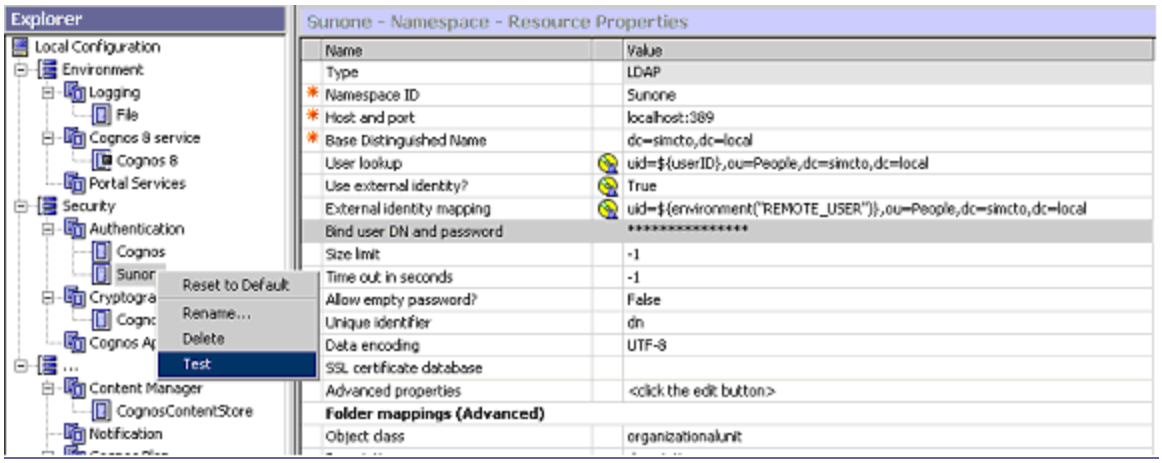
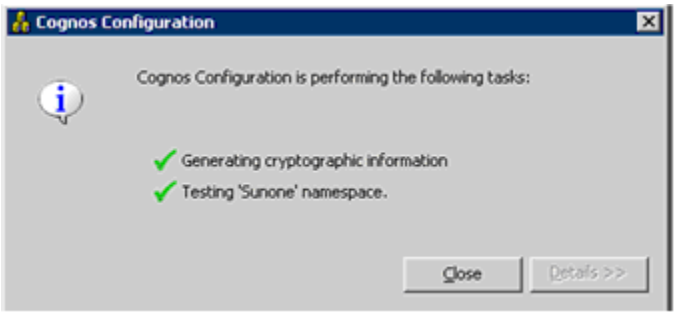


Figure 7-11: Testing the AxedaNameSpace authentication provider

3. A window appears, showing the progress of the test. If the test fails, verify that all configuration values entered up to this point are correct. Refer to the error pane (lower portion of page) for help in roubleshooting any problems.

   If the test is successful you should see the following:



Now you can create the second new authenticator, which is a custom authenticator.

To create the Remote AxedaTrustedProvider namespace

1. In the Explorer pane, browse to **Security > Authentication**.
2. Right-click and select **New Resource** > **Namespace**.

The New Resource - Namespace dialog box appears. Figure 7-12 shows an example of this dialog box.

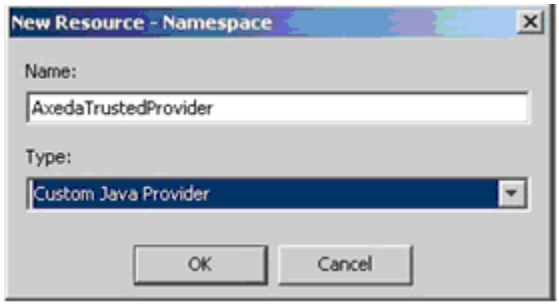


Figure 7-12: Configuring new namespace

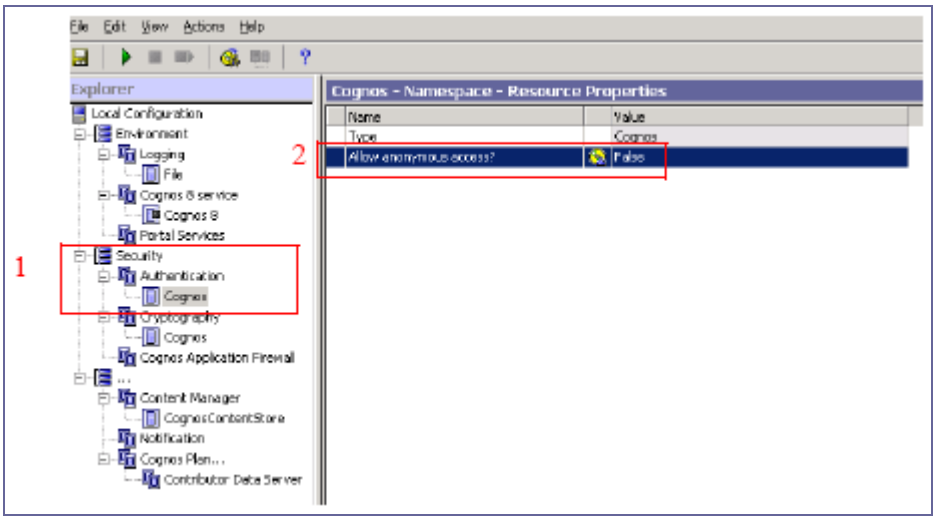
3. Enter the following information and click **OK**:
   - **Name** - Type AxedaTrustedProvider
   - **Type** - From the list, select **Custom Java Provider**

   The AxedaTrustedProvider - Namespace - Resource Properties page appears in the right pane.
4. Specify the following values:
   - **Namespace ID** - AxedaTrustedProvider
   - **Java class name** - com.axeda.cognos.security.AxedaTrustedProvider
5. Click **Save** ( ) to save the configuration.

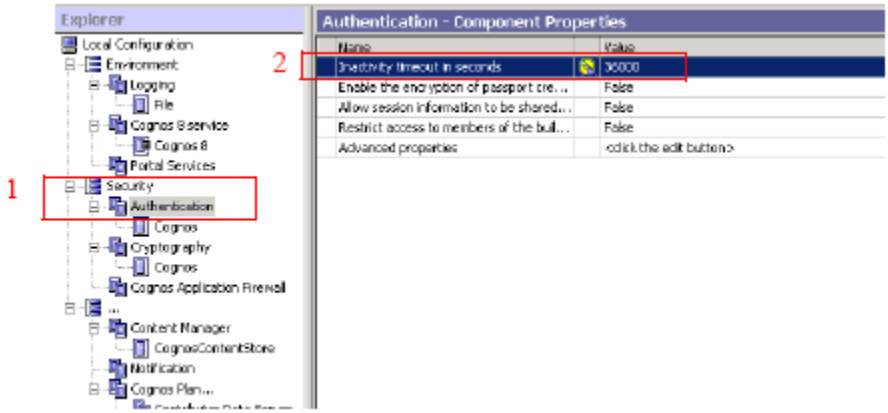
   Next, you will disable anonymous authentication and change the inactivity timeout.

To disable anonymous authentication and change the inactivity timeout

1. In the Explorer pane, navigate to **Security** > **Authentication** > **Cognos**.
2. When the properties appear in the right pane, change the setting for **Allow anonymous access?** to False. The following figure illustrates these steps.



3. In the Explorer pane, navigate back up to **Security** > **Authentication**. The properties for Authentication appear in the right pane, as shown in the following figure.



4. To prevent logouts over a longer time period, change the value in the **Inactivity timeout in seconds** field to 18000 seconds (5 hours).

   Now you can restart the Cognos 8 server.

To restart the Cognos 8 server

Click  to restart the Cognos 8 server. A window similar to the one shown in Figure 7-13 appears, indicating that the Cognos 8 service is stopping, the upgrade is being checked, and then, the service is starting. If any of these fail, refer to the information in the error pane (lower part of the screen) to troubleshoot a problem.

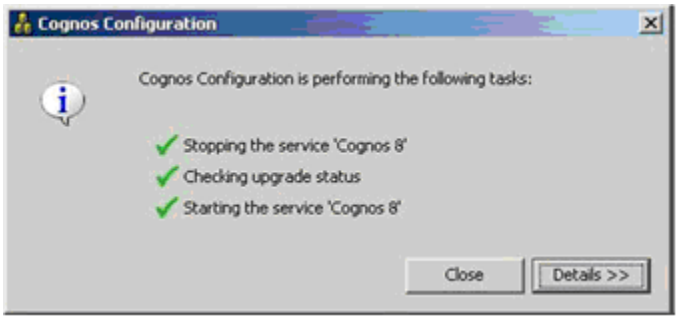


Figure 7-13: Cognos 8 server started successfully

Continue to the next section to configure the SAL reports.

Configuring SAL reports using Cognos Connection

At this point, you have completed the configuration using the Cognos Configuration tool and copied the SAL report files (after installing the Concentrator Remote Server). You are ready to complete the reporting configuration using the Cognos Connection application. The steps you need to follow are:

1. Start the Cognos Connection application, select the AxedaNameSpace for authentication, and log in.
2. Configure the Data Source for the reports (the database connection) and test the connection.
3. Import the SAL Report Pack.
4. Set permissions for Cognos.
5. Confirm that the reports and objects are available and test the installation.

To start the Cognos Connection application and log in

Important:

You must log in as `admin` user in the AxedaNameSpace to import the SAL Report Pack.

1. Open a Web browser and browse to the Cognos 8 server.
   For example, type *http:// cognos_server/cognos8* in the URL line. The Log on screen appears.

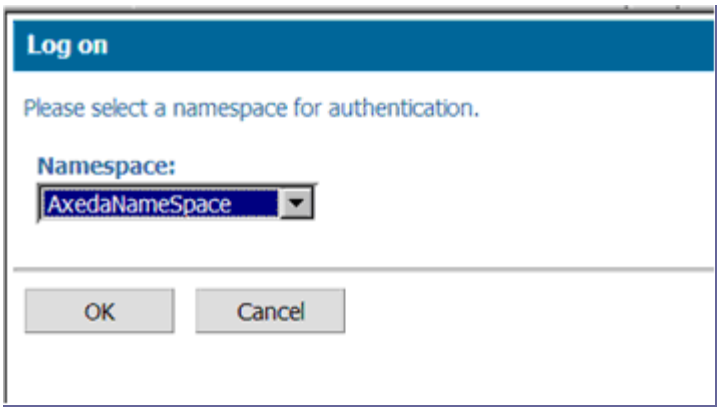


Figure 7-14: Cognos Connection Log on screen - Select AxedaNameSpace

2. If it is not already shown under **Namespace**, select **AxedaNameSpace** from the list.
3. Click **OK** to display the credentials component of the Log on screen:

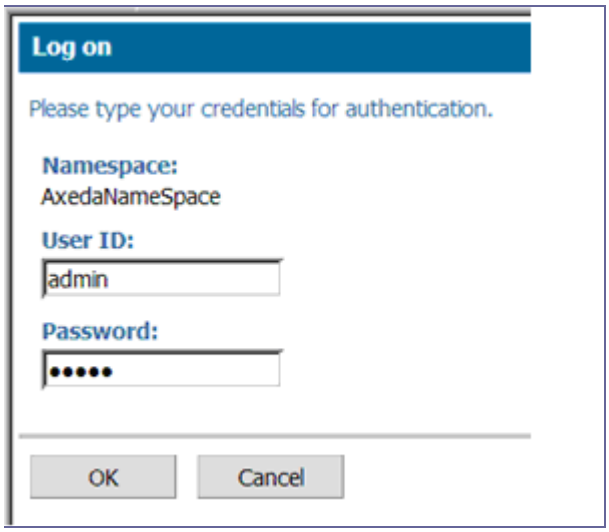


Figure 7-15: Cognos Connection Log on screen - Specify "admin" as the User ID

4. Under **User ID**, type `admin`, as shown in Figure 7-15.
5. Under **Password**, type the password for the admin user and click **OK** to log in. The Welcome page appears.

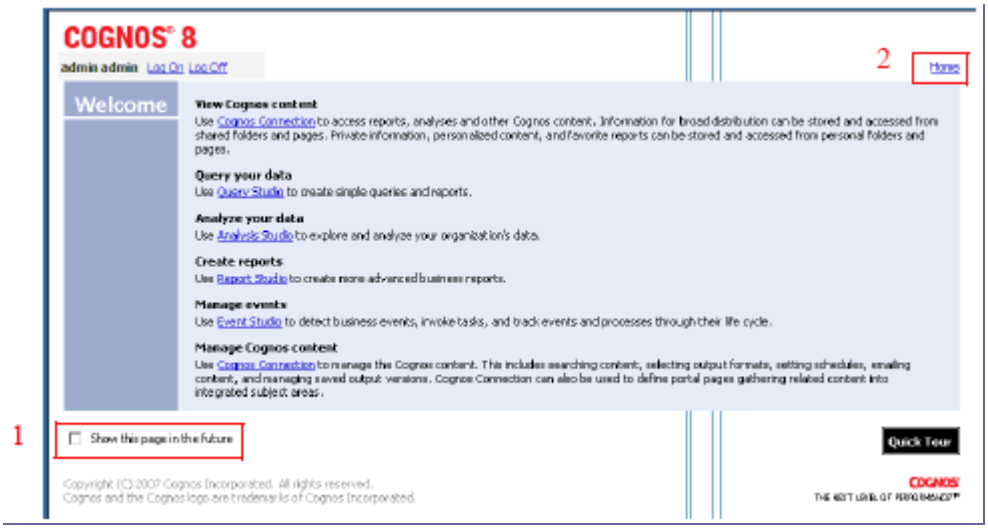


Figure 7-16: Cognos 8 Welcome page

6. As shown in Figure 7-16, clear the **Show this page in the future** check box, and then click **Home** to display the Public Folders page of the Cognos Connection application.

   The following figure shows this page as it first appears.

To configure the data source for the reports

This procedure begins under the assumption that you have just logged in to the Cognos Connection application and displayed the Home page. Return to To start the Cognos Connection application and log in if you need to start the application and log in.

1. On the **Tools** menu, click **Directory**.

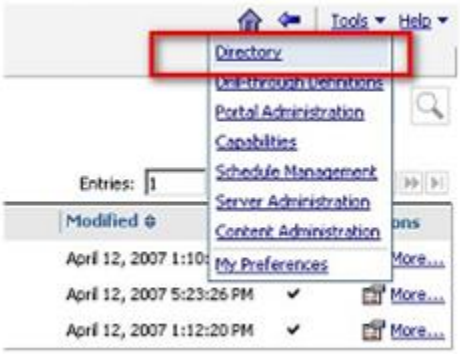


Figure 7-17: Select Cognos 8 Tools link, and then Directory

2. On the Directory page that appears, click the **Data Sources** tab.
3. Click the **New Data Source** icon, as shown in the following figure.

Figure 7-18: Cognos Connection - Data Sources tab

4. The New Data Source wizard starts. In the first step, type `ServiceLink` as the **Name** of the data source, as shown in the following figure.

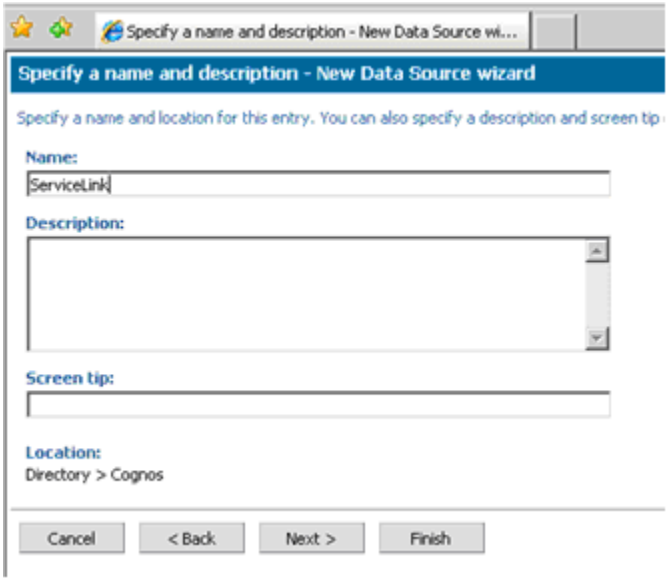


Figure 7-19: New Data Source wizard - Name must be ServiceLink

Note:

The name of the data source must be ServiceLink for the Report application to generate reports from the ServiceLink system database.

5. Click **Next** to display the Specify the connection step, as shown in the following figure.

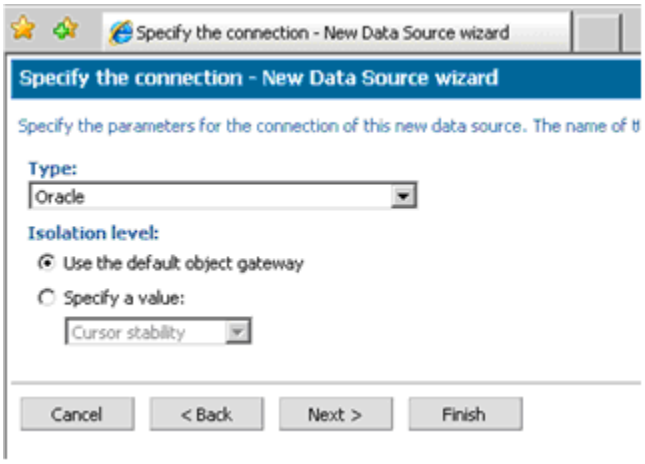


Figure 7-20: New Data Source wizard - Specify the connection

6. From the **Type** list, select **Oracle**.
7. For the **Isolation level**, select **Use the default object gateway**.

8. Click **Next**. The Specify the Oracle connection string step appears, as shown in the following figure.

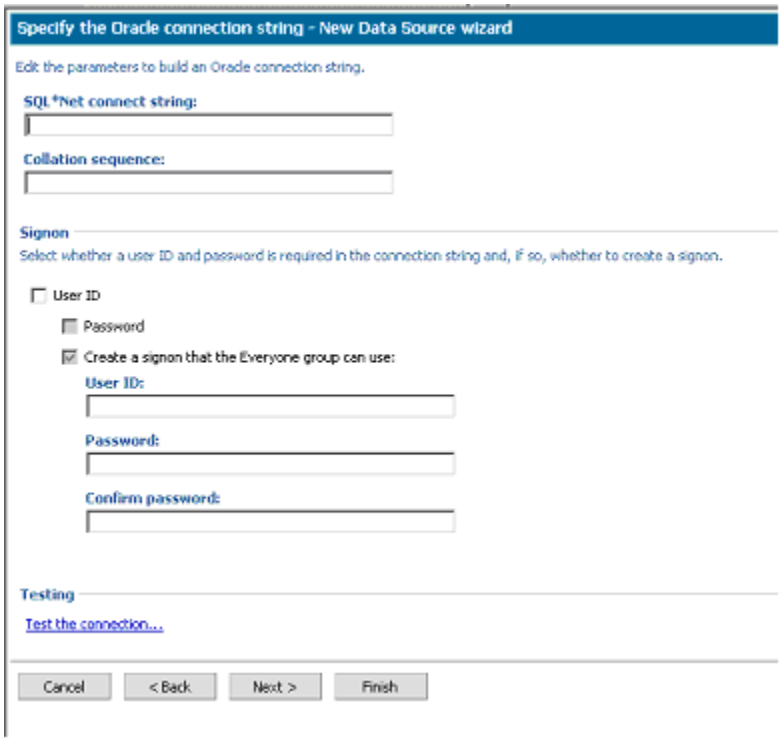
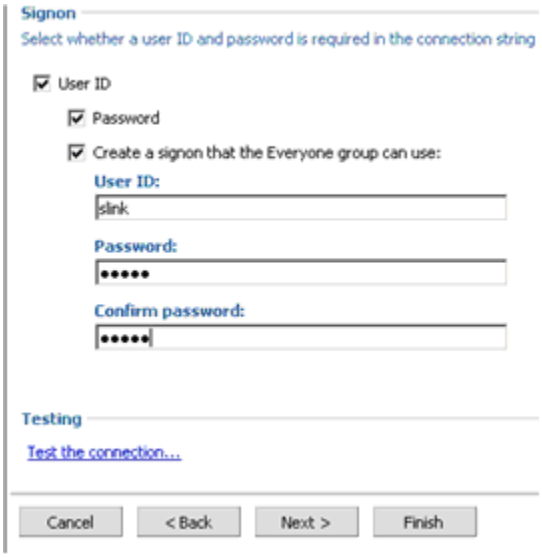


Figure 7-21: New Data Source wizard - Specify the Oracle connection string

9. Under **SQL*Net connect string**, type the connection string specified in the *tnsnames.ora* file in the Oracle client installation. Obtain this information from your Database Administrator.
10. Under **Signon**, select the **User ID** and **Password** check boxes.

11. After the **User ID**, **Password**, and **Confirm password** fields become available, type the database user name and password for the SAL system (*not* for the Cognos 8 system). The Cognos 8 server needs to pass these credentials when connecting to the SAL database. The following figure shows an example for configuring this section.



Note:

Be sure that you enter the user name and password for the SAL database, not the Cognos 8 database.

12. Under **Testing**, click the link, **Test the connection**. The following page appears:

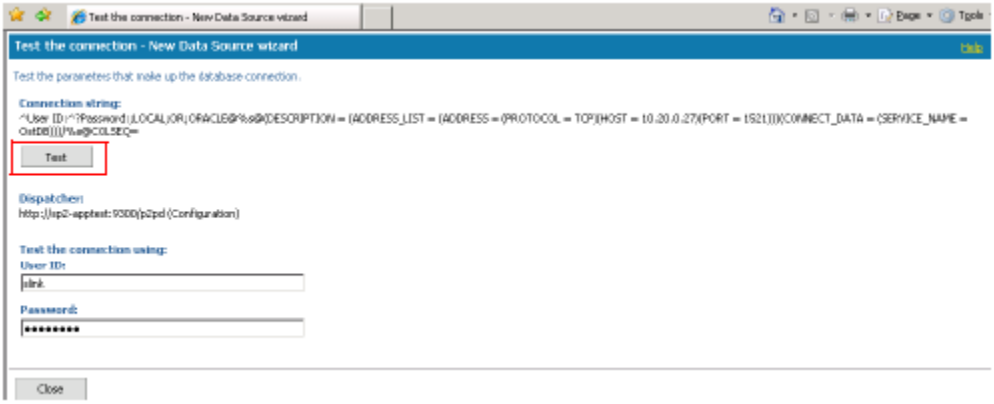
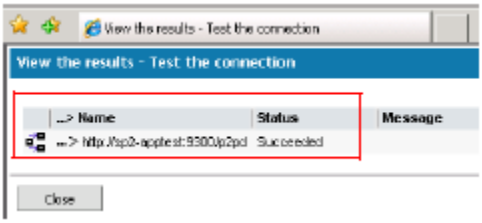


Figure 7-22: Testing the database connection

13. Verify that the Connection string, User ID and Password are correct, and click **Test**. The results are displayed on a page similar to the one in the following figure.



14. If the connection test succeeds, click **Close**. On the next screen, click **Close** again. You return to the Specify the Oracle connection string page.
15. On the Oracle connection string page, click **Next** to display the Specify the commands page, as shown in the following figure.

Figure 7-23: New Data Source wizard - Specify the commands

16. Click **Finish** on this page to return to the main Data Sources page, where the SAL data source now appears in the table.

Figure 7-24: Data Sources tab, showing new SAL data source

Next, you will import the SAL Report Pack.

To import the SAL Report Pack

The SAL Report Pack file (*ServiceLink_CS.zip*) was one of the files you copied to the Cognos 8 installation before starting Cognos 8 configuration. (See Copy Files to Cognos 8 Installation.)

1. On the **Tools** menu, click **Content Administration**, as shown in Figure 7-25.

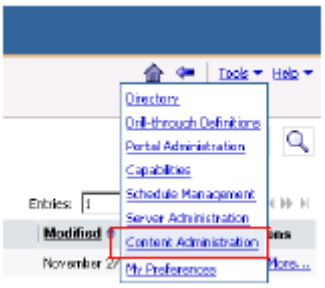


Figure 7-25: Selecting Content Administration from the Tools menu

This link displays the Administration page, which shows the files available for import (that is, the files stored in the Cognos 8 *c8/deployment* directory). The Administration page has a toolbar, from which you can select to import a new report package.

Note:

If you do not see the ServiceLink_CS archive listed on this page, then return to the Copying files to Cognos 8 installation section to copy the Report Pack archive to the Cognos 8 c8/deployments directory.

2. If the ServiceLink_CS archive is listed on this page, click the **New Import** icon, as shown in the following figure.

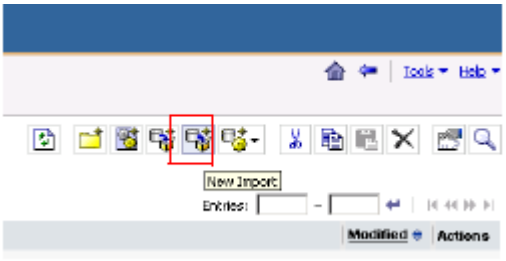


Figure 7-26: New Import icon in the Content Administration toolbar

The New Import wizard starts, displaying the Select a deployment archive page. On this page, you should see the SAL report package ready to import, as shown in the following figure.

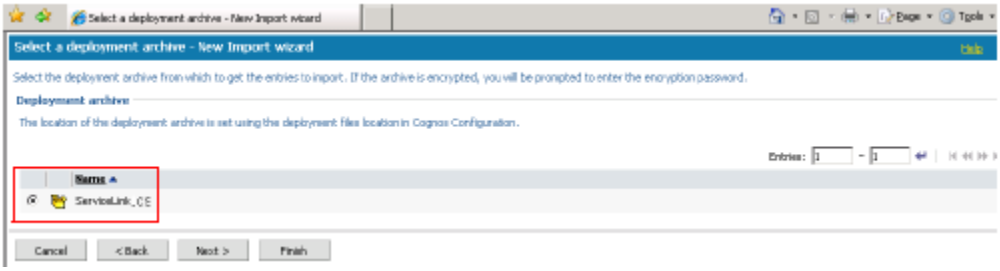


Figure 7-27: New Import wizard - Select a deployment archive

3. Make sure that the **ServiceLink_CS** archive is selected, and click **Next** to display the page, Enter the encryption password.

4. For the password, type `servicelink`, and then click **Next** to display the next page, Specify a name and description, as shown in the following figure.

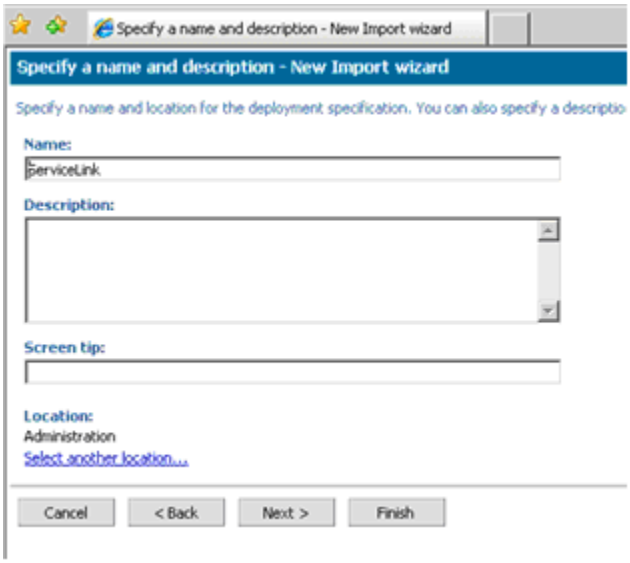


Figure 7-28: New Import wizard - Specify a name and description

5. As shown in Figure 7-28, type **ServiceLink** in the **Name** field. If desired, you can add a **Description** and **Screen Tip**. Then, click **Next**.

   The next page, Select the public folders content, appears, as shown in the following figure.

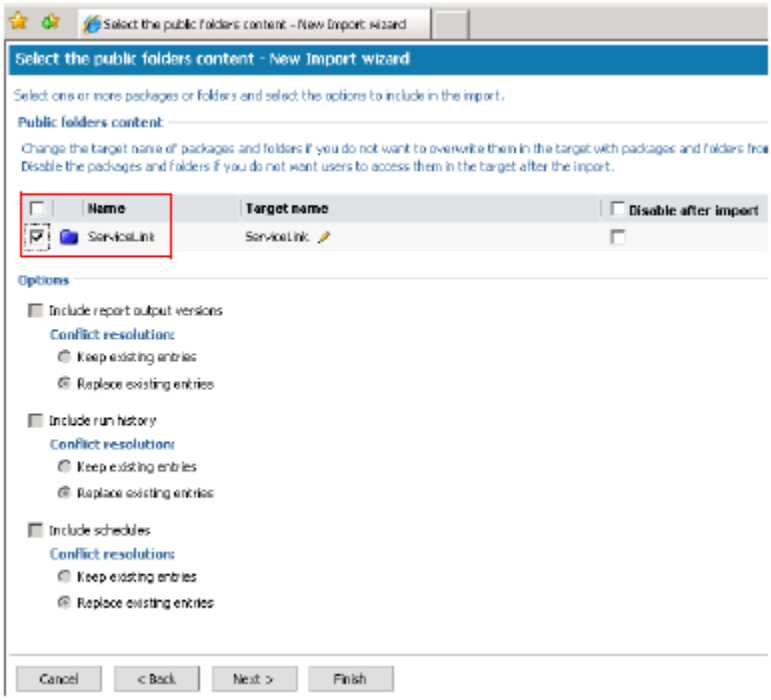


Figure 7-29: New Import wizard - Select the public folders content

6. On this page make sure that the check box next to the **ServiceLink** folder is selected, as shown in Figure 7-29, and then click **Next.**

   The next page of the wizard appears, as shown in the following figure.

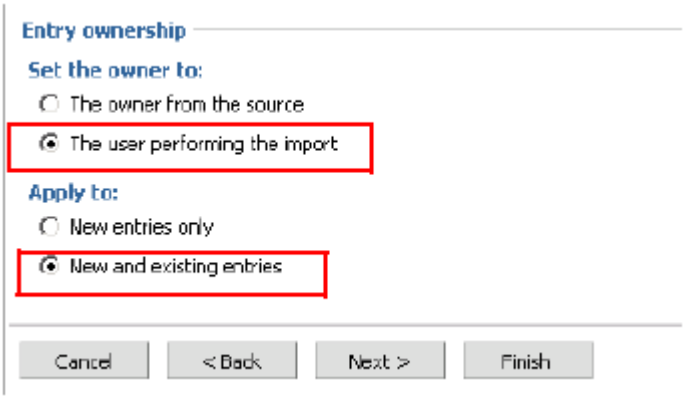


Figure 7-30: New Import wizard - Entry ownership and Apply to

7. Under **Set the owner to**, select **The user performing the import** (which should be `admin`).
8. Under **Apply to,** select **New and existing entries**.
9. Click **Next** to display the Review summary page, as shown in the following figure.

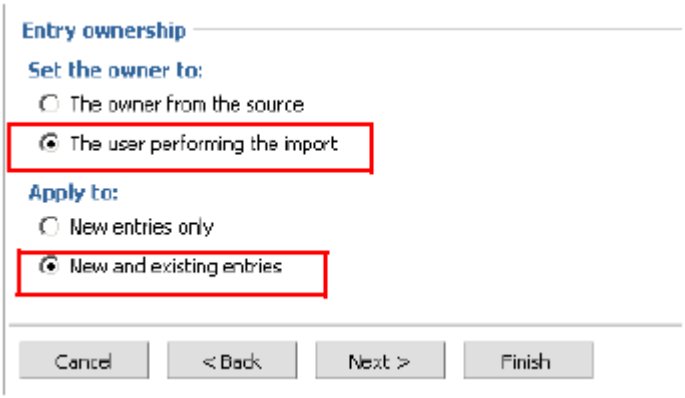


Figure 7-31: New Import wizard - Review summary

10. Review the settings on this page and, if they are correct, click **Next**. If they do not match those shown in Figure 7-31, click **Back** to make changes and then return to this page and click **Next**.

The Select an action page appears, as shown in the following figure.

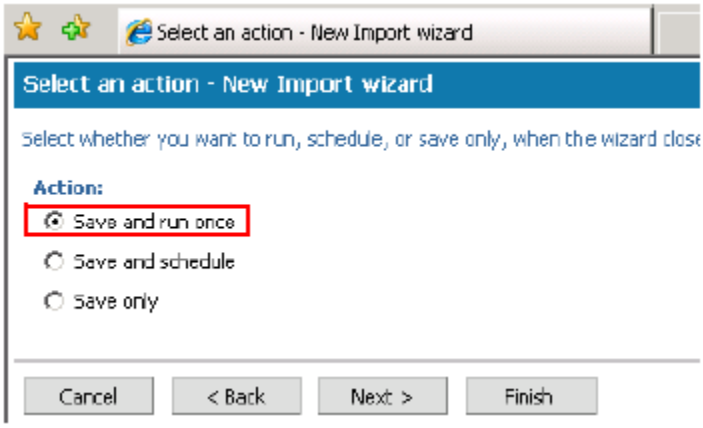


Figure 7-32: New Import wizard - Select an action

11. Under **Action** on this page, make sure that the **Save and run once** option is selected and click **Finish**.

    The Run with options page appears, as shown in the following figure.

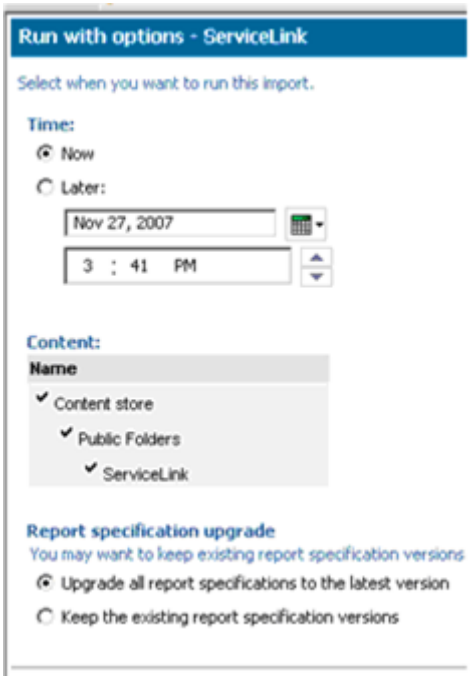


Figure 7-33: Run with options page

12. To run the report immediately, retain the default settings and click **Run**. The following page appears.

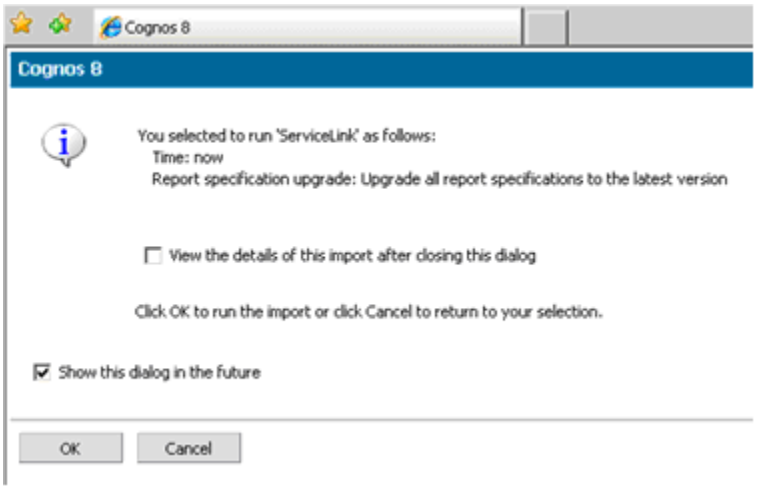


Figure 7-34: Completing the import task

13. On this page click **OK** to complete the import task.

    After the file is imported successfully and the Administration page is refreshed, the SAL report pack is displayed, as shown in the following figure.

Figure 7-35: Cognos Connection - Administration

14. Click the Home icon ( ). The Home page with the Public Folders tab appears.

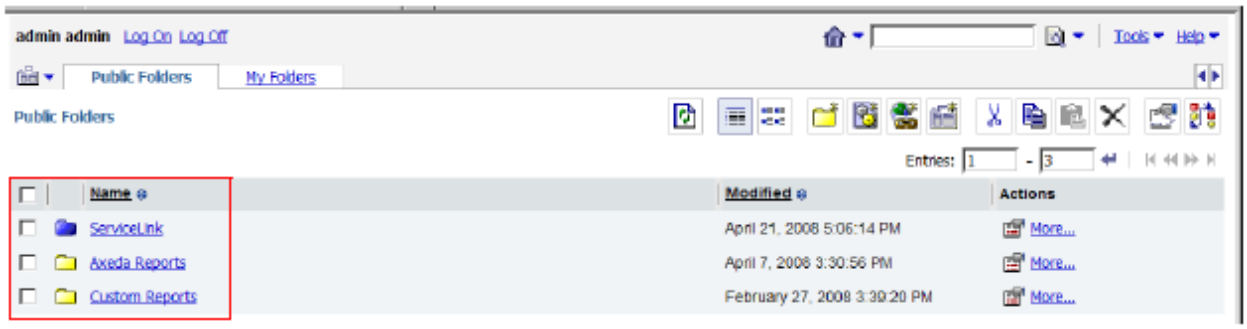


Figure 7-36: Cognos Connection — Home page

15. In the table on the Home page, check that the SAL, Reports, and Custom Reports folders appear in the Public Folders tab (see Figure 7-36). If they do, you can continue to the next procedure to set permissions.

To set permissions

By default, Cognos 8 gives every user System Administrator privileges. You need to limit access to the System Administrator role, as explained in the following procedure. This procedure assumes that the Cognos Connection application is running.

1. On the **Tools** menu, click **Directory**.

   On the Directory page, you should see the content of the Users, Groups, and Roles tab, as shown here.

2. In the Name column, locate Cognos, and in the **Actions** column, click the Properties icon ( ).
3. On the Set properties - Cognos page, click **Permissions** to display the Permissions tab, as shown in the following figure.

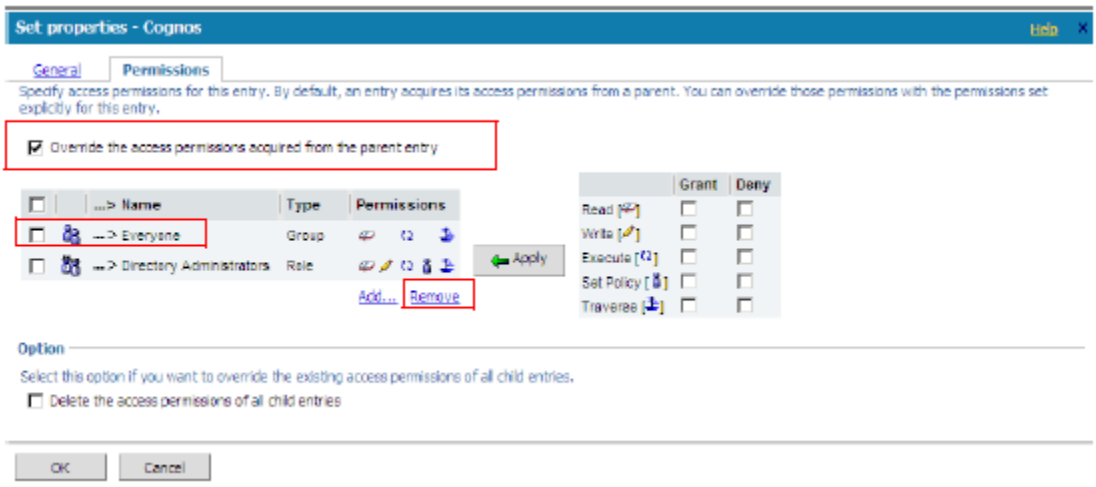


Figure 7-37: Cognos Connection - Set properties - Cognos - Permissions tab

4. As shown in Figure 7-37, select the **Override the access permissions acquired from the parent entry** check box.

5. In the **Name** column of the table, select the check box next to **Everyone**, and click **Remove**. You should have only one entry for the System Administrators role. By default, Cognos 8 gives every user the System Administrator privilege.
6. Click **OK** to save the changes and return to the Users, Groups, and Roles tab of the Directory page.

To confirm reports and objects, and to test

1. Click the Home icon ( ). The Home page appears with the Public Folders tab open. You should see the following folders on this tab.

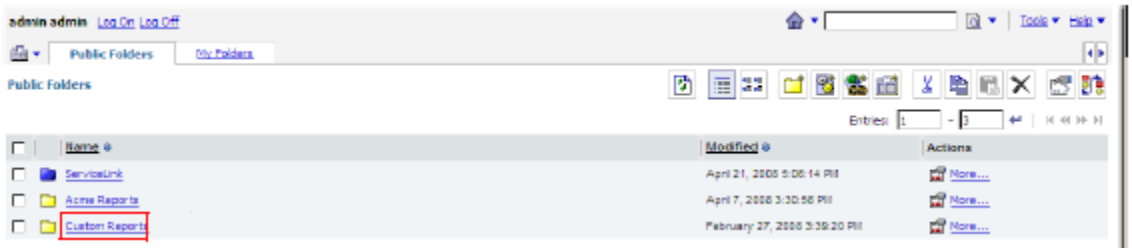


Figure 7-38: Select ServiceLink file from Public Folders

2. Under **Name** in the table, click the **Reports** link. The following list of types of Reports is displayed:

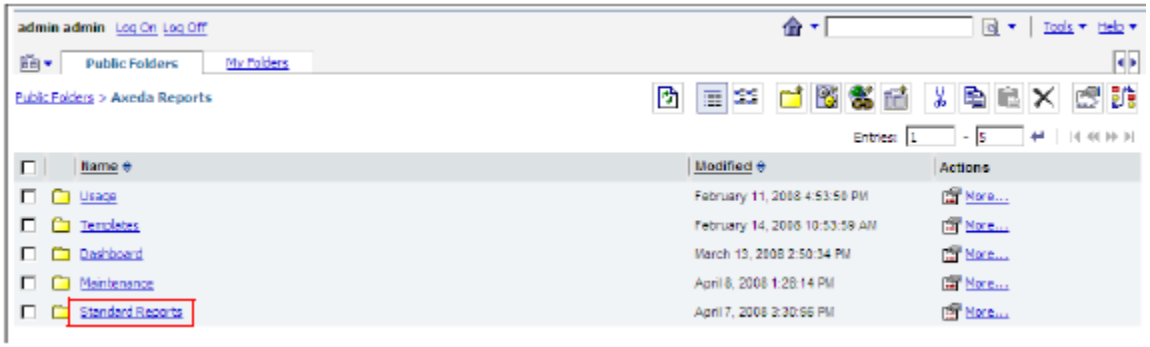


Figure 7-39: Example of reports and objects imported to Cognos 8 server

3. Click the **Standard Reports** link to display the list of Reports (which will appear on the home page of the Report application), as shown in the following figure.

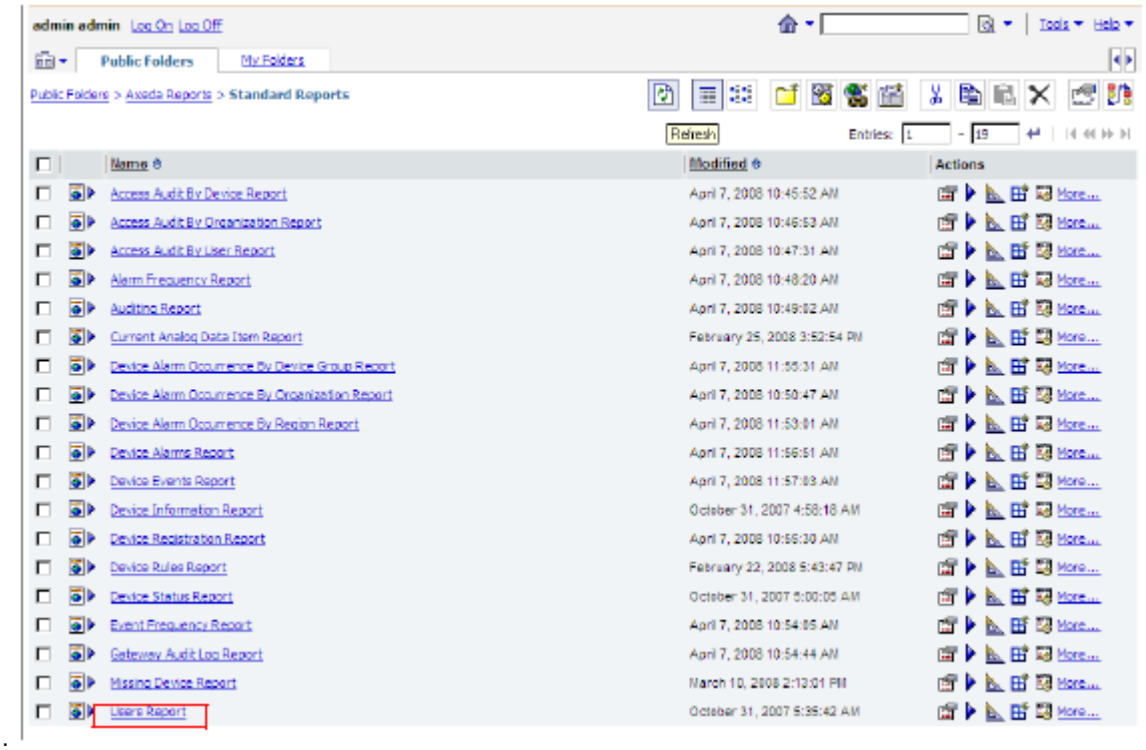


Figure 7-40: Public Folders > Axeda Reports > Standard Reports

4. Test the installation to this point by selecting the link for the Users Report.

Note:

If you are upgrading an existing system and you have devices registered, you may want to run the Device Registration report instead. To minimize the time needed to collect all the data, when prompted for report parameters, be sure to limit the number of devices that the report needs to gather.

5. When prompted, select a column name and click **Submit** to run the report.

   The report is displayed in the Cognos Viewer, as shown in the following figure.

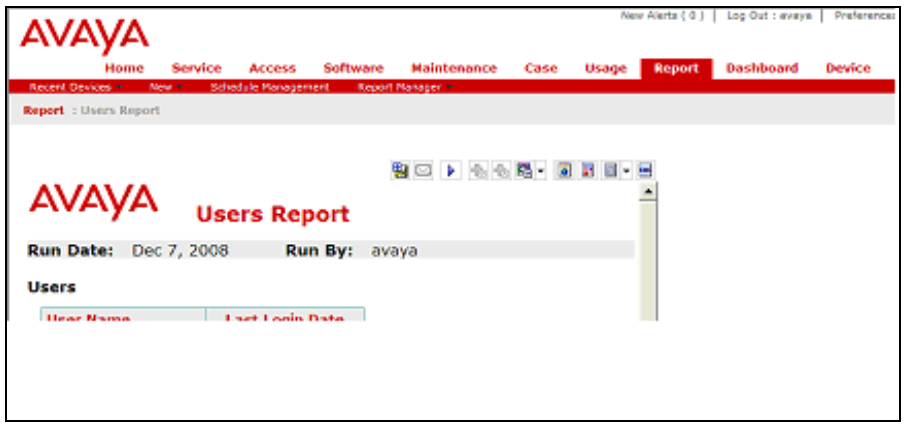


Figure 7-41: Users Report results in Cognos Viewer

6. Next, you need to test the LDAP configuration, so click the **Log Off** link at the top of the Cognos Viewer window, as shown in Figure 7-41.

Continue to the next section.

Testing the directory server configuration

If you have not already tested the directory server configuration, click the **Log Off** link at the top of the Cognos Viewer window. If you are elsewhere in the Cognos Connection application, click the **Log Off** link as shown in the following figure.

When prompted, make sure that **AxedaNameSpace** is selected. Then log in again with the user name and password for any user configured in the Directory Server.

If the login is successful, it means that you have completed the configuration of the Cognos 8 server.

Next, if you accepted the defaults for Cognos 8 when installing the Concentrator Remote Server, you may need to update the properties related to the Cognos 8 server for the Concentrator Remote Server (in the configuration file, *DRMConfig.properties*) and the *web.xml* file for the *public* application to enable support for Cognos 8 reporting. If you entered the Cognos 8 information when installing the Concentrator Remote Server, the Installer sets these properties and the configuration is complete. Otherwise, you can modify the Concentrator Remote Server properties and the *web.xml* file after installation, as explained in the following section.

Modifying properties for the Concentrator Remote Server

If not already configured during the Concentrator Remote Server installation and configuration, you need to modify the *DRMConfig.properties* for the Cognos 8 operations. In addition, you need to modify the *web.xml* file for the *public* application in the Concentrator Remote Server installation.

To edit properties in the DRMConfig.properties file for Cognos 8 operations

1. In an ASCII-based text editor (such as Notepad), open the `DRMConfig.properties` file located in the `avaya/SAL/CRS/config` directory, by default.
2. Search for the section, **`Cognos Report`**.
3. Specify the values shown in Table 7-2.

Table 7-2 Cognos 8 Report settings for Concentrator Remote Server

For this property	Specify
`com.axeda.drm.cognos.report.serverurl = http://cognos_server.avaya.com`	The URL of the Cognos 8 server. For example, `http://cognos_server.avaya.com`.
`com.axeda.drm.cognos.report.port = 9300`	The port for the Cognos 8 server.
`com.axeda.drm.cognos.publish.folder = ServiceLink`	The default directory on the Cognos 8 server to which reports, queries, and other Cognos 8 objects are saved. The Cognos 8 user can select to save Cognos 8 objects to a different directory location.

4. Save and close the file.
5. Continue to the next procedure to edit the *web.xml* file of the *public* application.

To edit properties in the web.xml file of the public application for Cognos 8 operations

1. In an ASCII-based text editor (such as Notepad), open the `web.xml` file located in the public.war, web-inf directory, in the servicelink.ear (<JBoss_HOME>/server/<SAL Install>/deploy) directory.
2. Locate the `redirectURL` parameter for the `ProxyServlet` and change its value to the actual URL that you use for the Cognos 8 reporting server. This parameter occurs in the following section of this file; the value you need to change is shown in red typeface:

```
<servlet>
   <servlet-name>ProxyServlet</servlet-name>
   <servlet-class>com.axeda.drm.cognos.servlets.HttpProxyServlet</servlet-class>
   <init-param>
       <param-name>redirectURL</param-name>
       <param-value>$COGNOS_SERVER_URL_1$:$COGNOS_WEB_PORT_1$</param-value>
   </init-param>
  </servlet>
<servlet-mapping>
   <Servlet-name>ProxyServlet</servlet-name>
   <url-pattern>/cognos8/*</url-pattern>
</servlet-mapping>
```

For example, you might type `http://111.2.1.111:80` for the `redirectURL` parameter.

Running reports in the Applications

After the Cognos 8 report server is installed and configured and the Concentrator Remote Server is configured to support the Cognos 8 installation, you can start the Concentrator Remote Server and run the reports defined in the imported SAL reports file. In addition, if you are a named user, you can use the Query Studio and/or Report Studio tools to create new reports or edit the existing reports.

1. Start the Concentrator Remote Server.
2. Open a Web browser and point to the SAL server on the port configured for your system (by default, port 80).
3. On the Applications home page, click the **Report** tab.

   The Report Home page appears, as shown in the following figure.

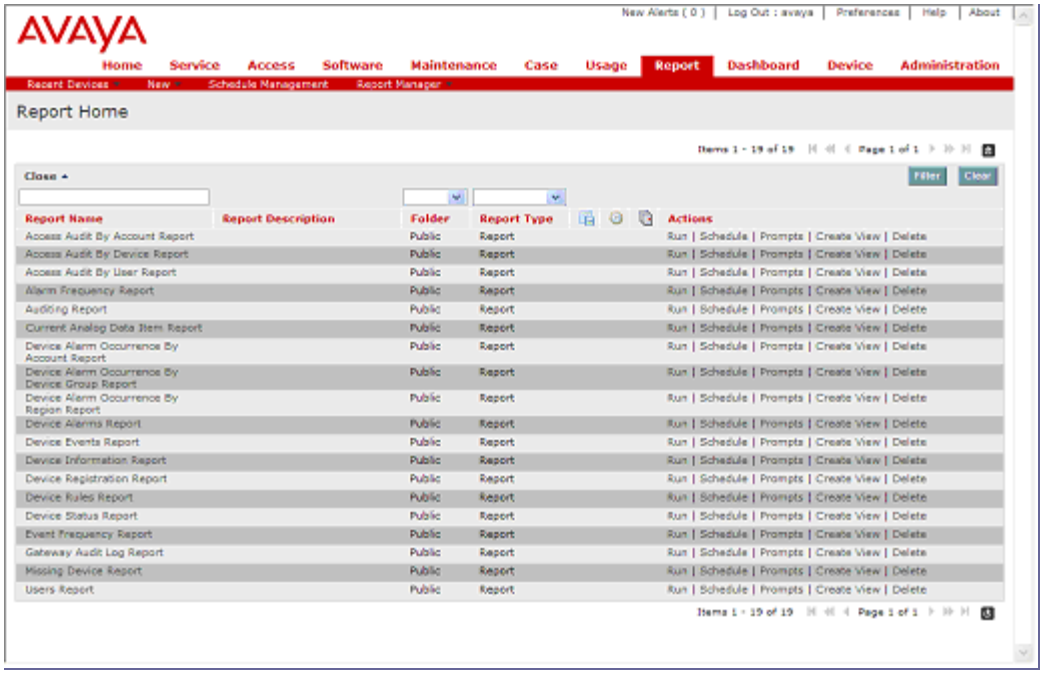


Figure 7-42: Report Home page

4. Verify that the names of the reports loaded from the SAL import file appear on the Report Home page. For information about these standard reports, see *Report Pack: Standard Reports Reference Guide*.
5. Scroll down to the Users Report and click the **Run** link under **Actions** (on the right side).

The Run with options screen appears, as shown in the following figure.

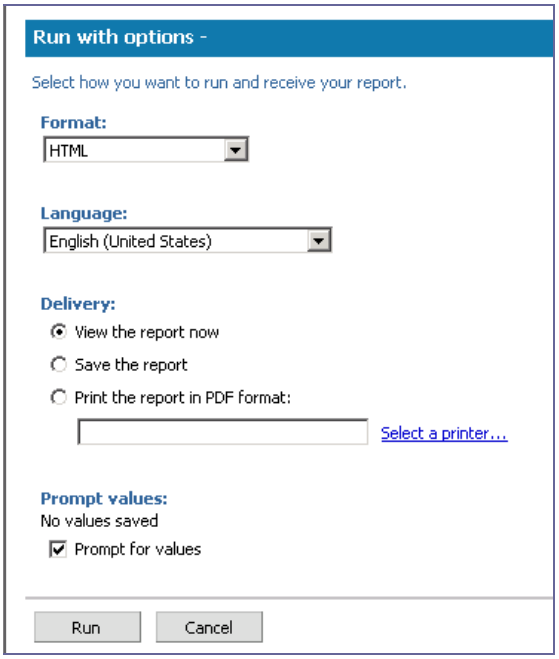


Figure 7-43: Run with options

6. Leave the default settings on the Run with options screen, and click **Run.**

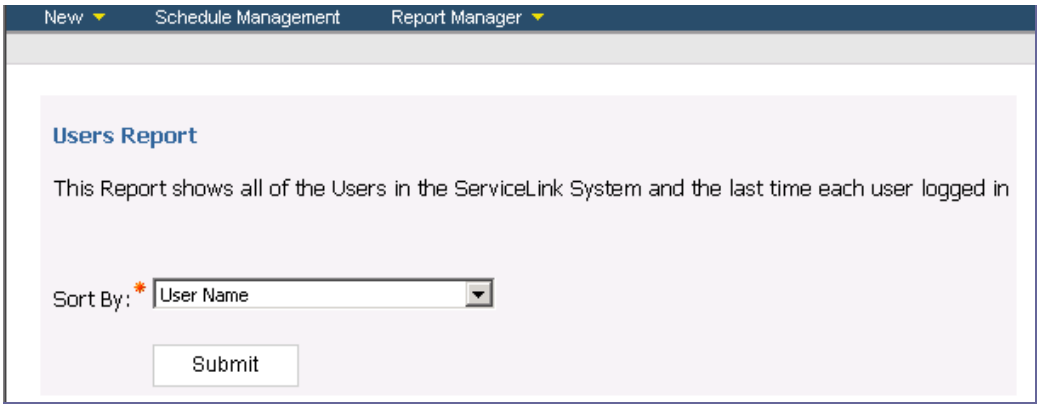


Figure 7-44: Users Report - choose Sort option

7. From the **Sort By** list, select **User Name** and click **Submit**. The report runs and displays the results.

   The report should show the users defined in your directory server for SAL.

8. Finally, to check that the dashboards are loading, click the **Dashboards** tab. You should see the default dashboard with devices reporting data.

As long as the default dashboard appears, the installation was successful.

This completes the procedure for installing and configuring the Cognos 8 Report server for Concentrator Remote Server.

Chapter 8: Configuring the Applications

About this chapter

This chapter explains how to perform the steps necessary to configure the Web-based applications that require it. For details on using the pages of this application, see the online help. This chapter is organized as follows:

Setting up Internet Explorer for the applications explains how to set up Internet Explorer for the applications.

The Software Management application provides important information about what you need to do before using the Software Management application to communicate with Agents running on your devices.

Setting up Internet Explorer for the Applications

The Concentrator Remote Server Web-based applications run in an Internet Web browser.

If you access the applications through Internet Explorer, you need to make a few adjustments in the configuration options for Internet Explorer before accessing the applications in order to avoid any potential problems in running the applications. The following instructions were written using Internet Explorer 7.0.

1. Start Internet Explorer.
2. Select **Page** | **Encoding**, and make sure that the option Auto-Select is selected.
3. Select **Tools** | **Internet Options**.
4. Under Browsing history on the **General** tab, click **Settings**.
5. In the **Temporary Internet Files** in the displayed dialog box, ensure that the **Never** option is *not* selected.

   Otherwise, you will have a logout/login problem with the applications, where the Login window for a new user will never come up and logging in will send you directly to the last application page prior to logging out. Refreshing, then logging out and in does solve the problem. However, changing the setting in this dialog box will avoid it altogether.
6. Select **Every time I visit the webpage** to solve this problem without the users needing to refresh.
7. On the **Advanced** tab, scroll down to Java (Sun), and make sure that the **Use JRE 1.6.0_03 for <applet>** check box is selected. This option requires a restart of the browser.

   To avoid seeing any run-time problems in the online help for the Access application, you also need to modify the **Advanced** tab in the same dialog box, as follows:

   a. If you closed the dialog box, select **Tools** | **Internet Options**.

   b. In the dialog box, click the **Advanced** tab.

   c. Under **Browsing**, clear the **Display a notification about every script error** check box. You may also want to select the **Disable script debugging (Internet Explorer)** and **Disable script debugging (Other)** check boxes.

   d. Click **OK** to save your changes and close the dialog box.

The Software Management application

Before using this application, make sure the following requirements are met:

1. The project running on the Agent device is configured with appropriate Software Management settings as well as the data source and data items that you want to use in a package (either to set them or to test their current value).
2. Any files less than 2 GB in size that you want to download to the Agent devices are archived and compressed first, using the tar and gzip tools. You can use the Software Management Download instruction to download these files. The Agents recognize the .tar.gzip extensions and can extract the files from the archive. Files larger than 2 GB should not be archived and compressed. Refer also to the online help for the Software Management application.
3. If the *dependencies.xml* file does not exist in the Agent, you cannot select any registry dependencies when creating or editing a package. Use any text editor to create the dependencies.xml files that each device will upload to the Secure Access Concentrator Remote Server upon registration and at intervals specified in the Agent's project. Then, from the Applications, download the files to the devices and save them in the working directory of the agent. When the Agent starts up, it registers with the Secure Access Concentrator Remote Server and uploads this file automatically. As an alternative, you may want to write a script that will generate this file for each device.

   Tip:

   You can use the Service application to verify that the dependencies.xml file was uploaded.
4. If you require any custom components, write them using the appropriate toolkit documentation, and set them up in the Software Management application so that they are available in the lists of dependencies and instructions. If the custom component is to be a dependency, it will need to be set up to return a pass or fail for the test it performs. If the custom component is to be an instruction, you need to set up the parameters to pass to it.
5. Start the Agent at the device level. This starts the project. If the project is not running, and you did not create any data items for the product family, you will not see any data items in the lists of Data Item dependencies or in the list of Data Items for the instruction, Set Data Item.
6. After the Agent has started and registered the device with the Secure Access Concentrator Remote Server, you can create and deploy a package.

Chapter 9: Testing the installation and setting up your system

About this chapter

Determining the Concentrator Remote Server version explains how to obtain the version information for the installed Secure Access Concentrator Remote Server, including any information provided for installed customizations, if applicable.

Starting the Concentrator Remote Server explains how to start the Secure Access Concentrator Remote Server.

Testing the installation explains a test you can do to ensure that the Secure Access Concentrator Remote Server and the Applications are functioning properly.

Setting up security explains how to use the Administration application to set up additional security.

Checking the system configuration explains how to find the system configuration page in the Administration application.

Determining the Concentrator Remote Server version

At some point after installing the server, you may need to determine the server version. SAL provides a command line script, `serverVersion.sh`, that you can run to obtain the Concentrator Remote Server version. The script is installed to the /bin directory under your Concentrator Remote Server installation.

The serverVersion script operates by reading the build number set in the server properties, `config/DRMConfig.properties`, and, if applicable, any custom information set in the custom configuration session, config/CustomConfig.properties.

To obtain the version information for your server, open a command prompt on that computer, navigate to the bin directory of the installation directory, and run the `serverVersion.sh` script from the command line.

Example:

> **/JAVA_HOME/bin/serverVersion.sh**

Where JAVA_HOME identifies the installation directory of your Concentrator Remote Server. The default installation directory path is /jboss-eap-4.3/ jboss-as.

When the script finishes, information similar to the following will be shown in the console window:

`"Avaya Secure Access Link version 1.5 build530125 (2008/12/21 21:32 EDT)"`

The actual information shown depends on your server version and any custom information.

Modifying the labels for the displayed information

The Output preface section of the serverVersion script file defines the labels that are applied to the version information.

The section with that information and the default labels are:

```
# Output preface
CORE_VERSION_LABEL="Avaya Secure Access Link version"
CUSTOM_VERSION_LABEL="Custom Implementation version"
```

You can modify the labels "Avaya Secure Access Link version" or "Custom Implementation version" to reflect the name of your own server information.

Starting the Concentrator Remote Server

At this point, the Secure Access Concentrator Remote Server should be completely installed and configured. To start the Secure Access Concentrator Remote Server, use a batch file that starts your application server.

To start the Concentrator Remote Server

1. At a command prompt, change to the directory where you installed the JBoss application server.
2. At the prompt, type `secureaccesslinkrun.sh`.

See Troubleshooting the Installation and Configuration if the server does not appear to start as intended.

Testing the installation

You can test the installation and configuration by accessing the applications and reading and writing data to the Secure Access Concentrator Remote Server.

1. In a browser window, access the applications log-in page of the Secure Access Concentrator Remote Server. For example, in the browser's URL address box, type the following to log in to the computer running the Web Application Server and the Secure Access Concentrator Remote Server:

   `http://localhost:port_number`

   where:

   - `localhost` is the IP address or name of the machine where you installed the Web Application Server and the Secure Access Concentrator Remote Server.
   - `port_number` is the port number for accessing the Secure Access Concentrator Remote Server.

   The log-in page appears automatically.
2. Log in to the application as the system administrator. To create a product family and set up security, you need to log in as the system administrator. The Applications Home page appears.

Note:

The Concentrator Remote Server Web-based application opens in the following browsers: Internet Explorer and Mozilla Firefox.

To test reading from the SAL database

1. Click the **Service** tab to display the home page for the Service application.
2. In the right pane, click the arrow for the Product Family list. Your new product family, X_100t, appears in the list, as shown in Figure 9-1:

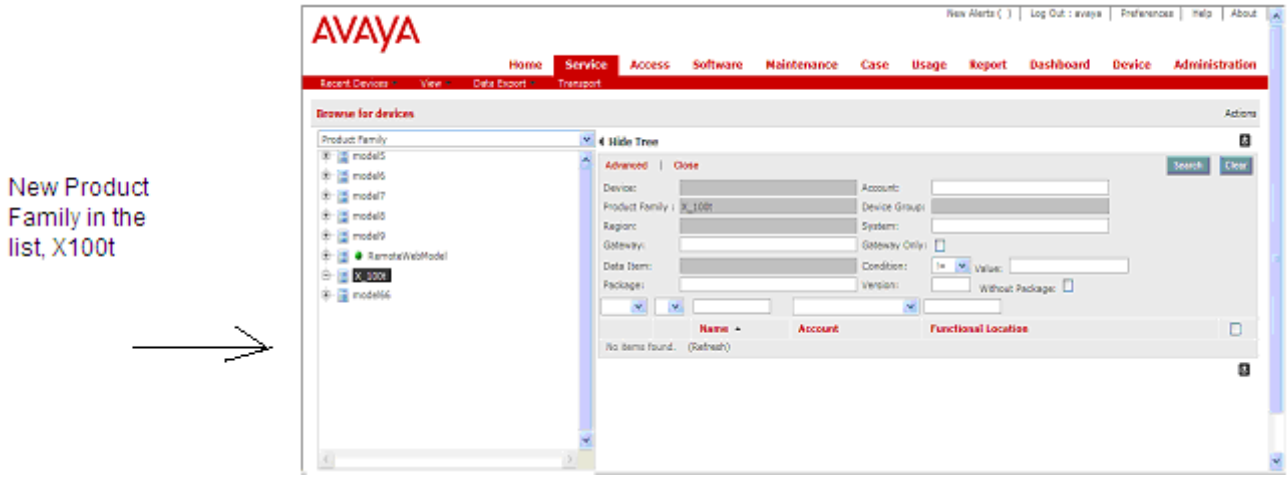


Figure 9-1: Service application home page, showing new product family

If you have any problems using the applications, see the online help or go to the next section to confirm the Secure Access Concentrator Remote Server installation and configuration.

At this point, you can add more product families and gateway product families. You can also add devices, such as gateway, gateway-managed, and standalone devices. In addition, you can add customers and manufacturers, and then add actions, rules, and e-mail notifications.

If needed, you can also click the **Administration** tab, and use the Administration application to set up device groups, data item groups, roles, reports, and security. To set up device groups and data item groups, see the online help. The next section explains how to set up security.

Setting up security

The procedures in this section explain how to set up the users and groups defined in your LDAP directory service so that they can access the Applications and information in the database.

Note:

The ServiceLinkUsers group and all users in the ServiceLinkUsers group for the Concentrator Remote Server must be defined in LDAP first. This section assumes that you have all of your users and groups configured on the LDAP server. If not, you need to do that first. See the documentation for your LDAP directory service for assistance.

Essentially, you need to use the Administration application to:

- View the users and user groups configured on the LDAP server
- Edit the assignments of privileges, users, reports, device groups, data item groups, or other user groups for a selected user group

If you are not already logged in, you must log in to the Applications as the administrator and from the Home page, navigate to the Administration application before you can perform any of these tasks.

Displaying user accounts configured on the LDAP server

You may want to verify that the Secure Access Concentrator Remote Server is communicating properly with the LDAP server. One way to do this is to display the users and user groups, using the View menu in the Administration application.

To view the user accounts configured on the LDAP server

1. On the **View** menu of the Administration application, click **Users**.

   The **View and remove application users** page (Figure 9-2) shows all users defined in the `ServiceLinkUsers` group, or, if you use the filter, a list of users whose information matches the filter setting. Users are listed in alphabetical order, based on their LDAP user IDs. From this page, you can search for specific users in the Secure Access Concentrator Remote Server. Then, you can select a user to view more information for that person.

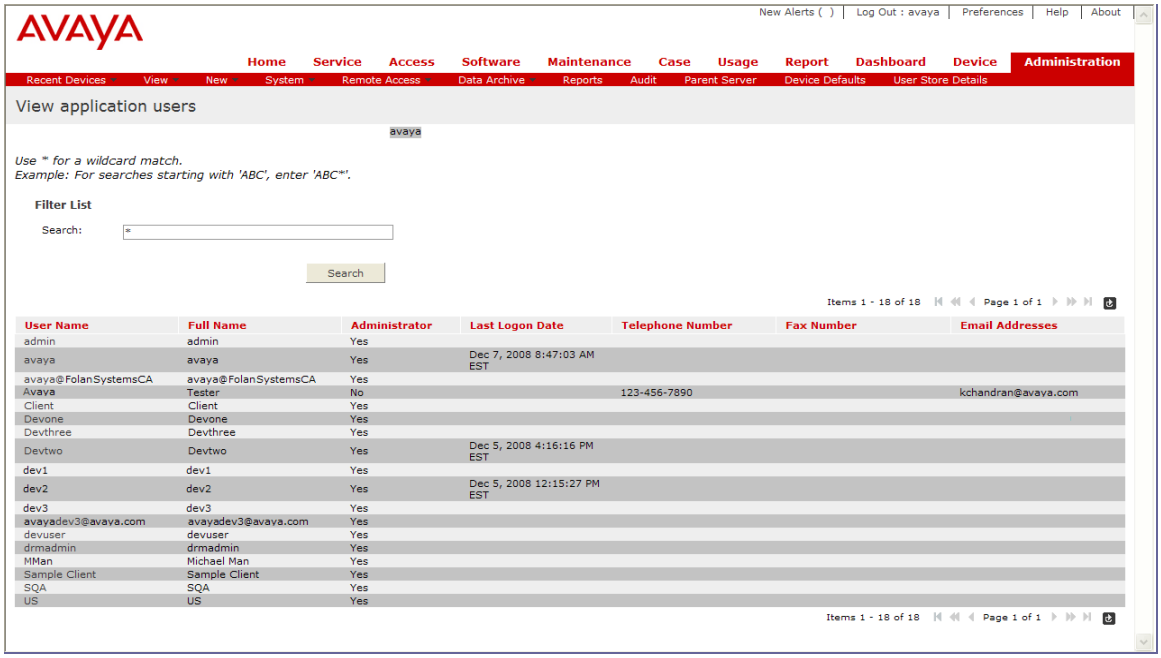


Figure 9-2: View and remove application users page

2. Under **Filter List**, in the **Search** field, type part of the user's name and use the "*" wildcard in place of the remaining portion of the name.

   For example, type "s*" to view all users whose names begin with "s". By default, the "*" wildcard shows all users in the default group, ServiceLinkUsers.

To view information for a user

1. Under the **User Name** column, select the name of the user. The system displays a summary page, as shown in Figure 9-3.

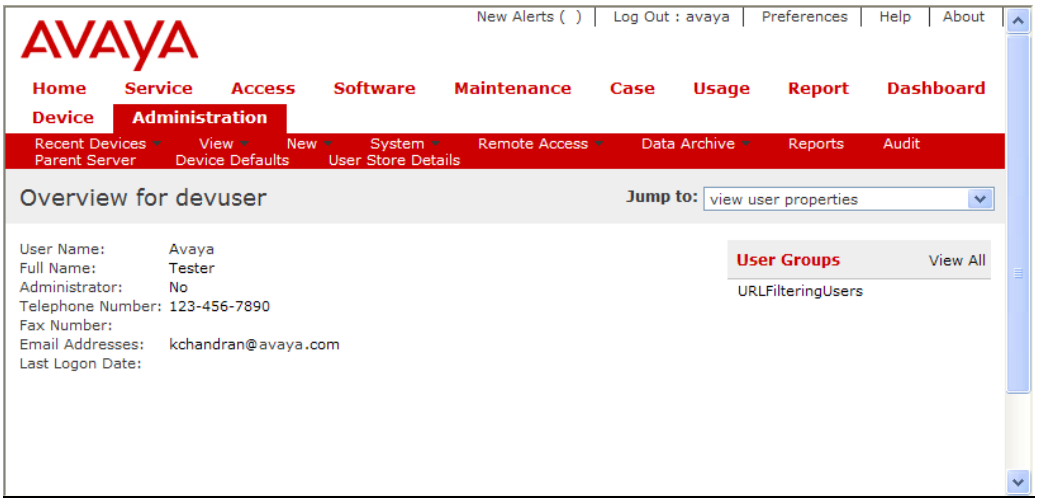


Figure 9-3: Overview of user page

The user summary page provides the following information about the user.

Field	Description
User Name	Displays the login name of the user.
Full Name	Displays the first and last names of the user.
Administrator	Displays Yes if the user is a system administrator or No if the user is not a system administrator.
Telephone Number	Displays The voice telephone or cellular telephone number of the user.
Fax Number	Displays the number to user for sending faxes to the user.
Email Addresses	Displays the e-mail addresses to use for notifying the user.
Last Logon Date	Displays the date on which the user last logged in to the Secure Access Concentrator Remote Server.
Notes	Displays any additional information about the user.
User Groups (module)	Displays the set of user groups to which this user is assigned.

From this page, you can edit the properties or the set of user groups to which the user is assigned. Click the appropriate link or select the appropriate option from the **Jump to** list.

Viewing user groups

From the Administration application, you can view all the user groups currently defined in LDAP and then assign privileges to those user groups so that individual users who are members of the group can access the appropriate Applications and the data in the database. You can create new user groups and remove existing groups. To do this, you must provide

an administrator user name and password for the LDAP service. In addition to creating and removing user groups, you can assign or remove application privileges, users, other user groups, device groups, data item groups, and reports to or from user groups. Users who want to access data for a particular device must be a member of a group that has been assigned the device group to which that device belongs. Otherwise, they cannot see the data for that device.

Displaying user group information

When you select a user group on the View and remove user groups page, the system displays a summary page, similar to the one shown in Figure 9-4.

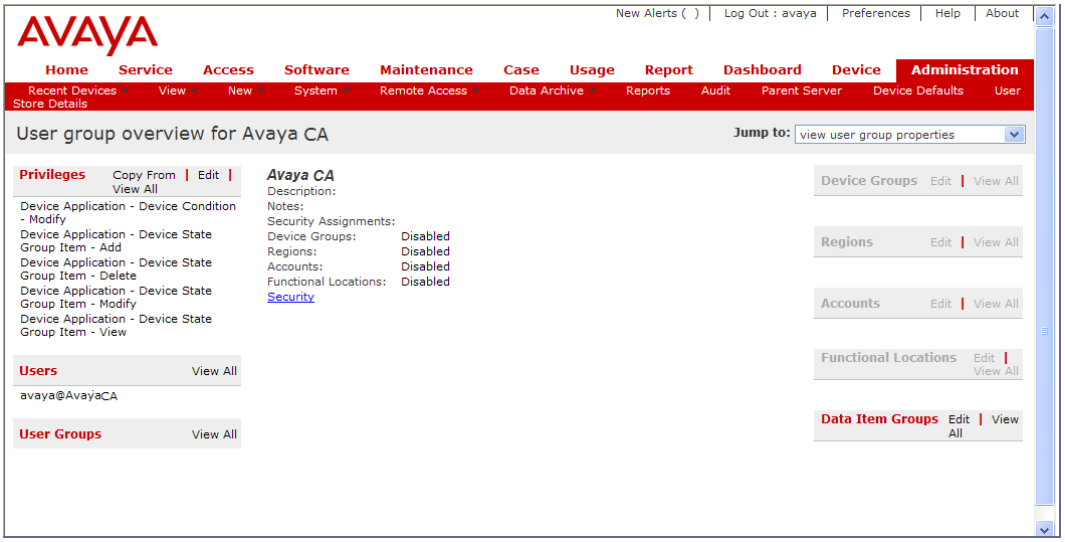


Figure 9-4: User group overview page

This page provides the following information about a user group in modules.

Module	Description
Privileges	Displays a list of privileges assigned to this user group.
Users	Displays a list of users assigned to this user group.
User Groups	Displays a list of user groups assigned to this user group.
Device Groups	Displays a list of device groups assigned to this user group.
Regions	Displays a list of the regions assigned to this user group.
Accounts	Displays a list of the accounts assigned to this user group.
Functional Locations	Displays a list of the functional locations assigned to this user group.
Data Item Groups	Displays a list of data item groups assigned to this user group.

Note that each module can show up to five of the items assigned to the user group. To view or edit all items in a module, click the appropriate link in the module (**Edit** or **View All**).

Alternatively, you can select an option in the **Jump to** list. For assistance in editing user groups, see the online help.

Checking the system configuration

To view the system configuration parameters (set in the DRMConfig.properties file), you can use the Administration application.

To view the system configuration

1. Click the **Administration** tab.

   The home page of the Administration application appears, as shown in Figure 9-5.

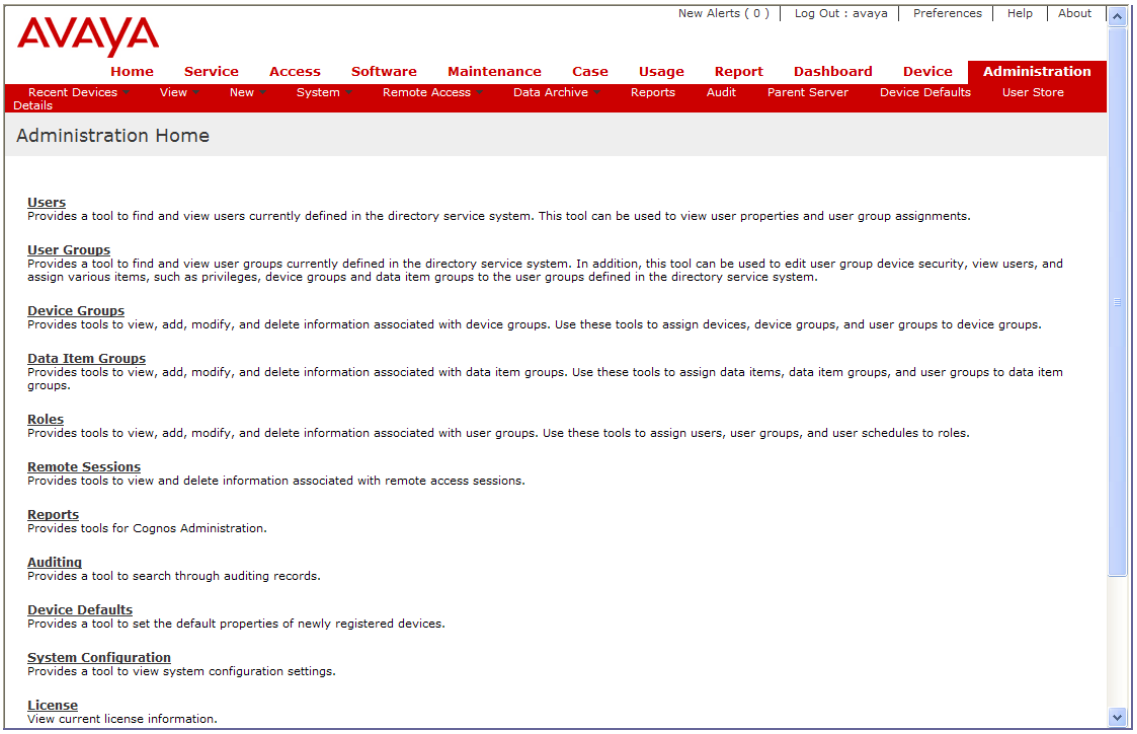


Figure 9-5: Administration home page

2. On the **System** menu, click **System Configuration**.

   The system displays the System Configuration page (Figure 9-6).

3. On the System Configuration page, use the navigation tools provided to view the entire list of configuration parameters. If you need to change a property value, you can change it only by editing the DRMConfig.properties file. See Appendix C: Editing the DRMConfig.properties File, for assistance in editing the property values.

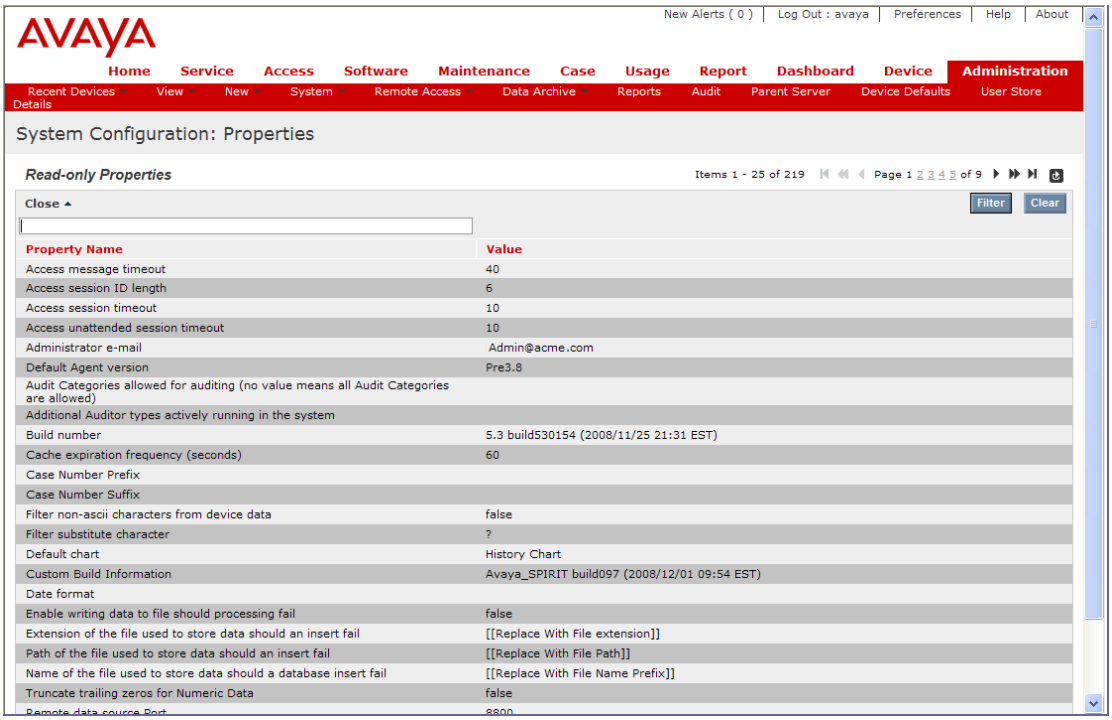


Figure 9-6: System Configuration page – Example

Chapter 10: Maintaining the SAL system

About this chapter

Starting up and shutting down the system explains the order in which you need to start up and shut down the components of the SAL system, starting with the Oracle database and the LDAP server, followed by the Web Application Server and the Secure Access Concentrator Remote Server.

Communicating with Agents explains how the Secure Access Concentrator Remote Server and Agents communicate failures, and how those messages are processed. Explains maintenance mode, error handling, and other SOAP/HTTP response message processing. Presents the Agents' support for multiple servers and the ability for an Agent to dynamically redirect its data communications to another Secure Access Concentrator Remote Server at run time.

Enabling Federated Communications support explains how to configure this Concentrator Remote Server as part of Federated Communications (also known as parent server communications).

Support for multiple Concentrator Remote Servers explains how Agents can communicate with more than one Secure Access Concentrator Remote Server.

Dynamic redirection and maintenance mode explains how Agents use dynamic redirection to communicate with a different Secure Access Concentrator Remote Server when the primary server is in the maintenance mode.

Error handling extensions explains how SAL error handling works.

Configuring Concentrator Remote Server to use a Syslog server explains how the Concentrator Remote Server can dispatch audit messages to a defined syslog server. Provides instructions for setting up syslog server support.

SOAP command status notification for Secure Access Policy Server explains how the Secure Access Policy Server works with the Concentrator Remote Server.

Database administration tools presents an overview of the database administration tools available to you that can prove useful for monitoring the system and troubleshooting problems.

Backing up and restoring applications explains how to back up and restore files for each component of the SAL system.

Troubleshooting installation and configuration introduces common problems encountered during testing.

Troubleshooting a new installation provides troubleshooting tips for installation problems. For troubleshooting information concerning connections with Agents, see the user guides for the Agents. Each guide has a troubleshooting section that provides tips for connectivity problems with the Concentrator Remote Server.

Preventive maintenance provides best practices information, including a table of routine tasks for monitoring the system and its performance.

Troubleshooting problems using log files explains what to look for in the log files generated by the system (Concentrator Remote Server and JBoss Server) for troubleshooting problems (performance) as well as how to configure and view the log files.

Making properties visible by editing DRMConfigInfo.properties explains how to make property information from the DRMConfig.properties file visible in the System Configuration page of the Administration application.

Troubleshooting after reinstalling SAL system components explains how to resolve problems that may occur after you reinstall system components.

Tuning performance of Web Visualization Applet explains how to get better results using the Web Visualization Applet.

Customizing applications explains where to put files that will customize your SAL system and what to do to make them work with the system.

Starting up and shutting down the system

To start successfully, the SAL system depends on several applications. To initialize properly, the SAL system requires a connection from the Web Application Server to both an LDAP directory server and a relational database server. Although these applications are both configured to run as UNIX or Linux daemons on production systems, it is possible to verify that they have started successfully, as the following list explains.

1. Oracle relational database server

The Oracle relational database server consists of both a database instance and a listener. They are separate processes and are listed separately in the daemon monitor. On a server with an Oracle home named `OraHome90` and a database instance named `SecureAccessLink`, the database instance daemon is named `OracleServiceSecureAccessLink`, and the listener is named `OracleOraHome`*`vn`*`TNSListener`. Both these daemons can be started manually if they are not configured to start automatically. Similarly, these daemons can be stopped manually. If the daemons are not shut down manually, they shut down automatically when the host machine is rebooted.

2. LDAP Directory Server

An LDAP Directory Server may consist of both a directory server and an Administration Server. In this case, the two servers can be separate processes and listed separately in the daemon monitor. On a server with a directory server named `AecureAccessLink_directory_server.avaya.com`, the directory server daemon might be named `LDAP Directory Server (SecureAccessLink_directory_server.avaya.com)`, and the Administration Server daemon might be named `Administration Server`. Both these daemons can be started manually if they are not configured to start automatically. Similarly, they can be stopped manually. If the daemons are not shut down manually, they shut down automatically when the server is rebooted.

3. JBoss application server and the Concentrator Remote Server

After you verify that the Oracle database and the Directory Server have started, you can start the JBoss application server and, with it, the Secure Access Concentrator Remote Server. If you chose not to configure the application server to run as a daemon, you can use a batch file, *secureaccesslinkrun*, to start the server in the home directory of the JBoss installation. On a server with a home directory of `JBoss_Home`, this batch file is located in the directory, /`<JBoss_Home>/bin`.

If you have configured to run the application server as a daemon, you will likely find a daemon named `SecureAccessLink` in the daemon monitor. You can start this daemon from the monitor if it is not configured to start automatically. Similarly, this daemon can be stopped manually. If the daemon is not shut down manually, it shuts down automatically when the server is rebooted. To verify that the application server is running correctly, view the following files on the server:

- Application server log files (*<JBoss_Home>/server/<SecureAccessLink_server>/log*)
- SAL log file
- JDBC log files

These files contain a history of the activity on the server and indicate problems in the form of error messages and exceptions. See the documentation supplied with your application server for further assistance.

Communicating with Agents

The SOAP protocol is used for communications between the Secure Access Concentrator Remote Server and Agents. The messages include status information concerning the processes running on the device. When a process running at the Secure Access Concentrator Remote Server fails at the device level, the server sets the status to an error code value and provides information about the error as well as an instruction for the Agent. For example, if a non-Registration message contains an unregistered device, the process continues until all devices are processed. However, the SOAP/HTTP response sets the status value to "1" and adds the information about the unregistered device as well as the instruction (Registry message) that the Agent needs to take.

If a process running on the Secure Access Concentrator Remote Server failed at post-device level, such as processing data items or alarms, the process continues, and the status remains "0" (successful). The SAL system generates an Error Alert and sends it to the designated user.

If no failure occurs during all the processing for all devices, the status is "0" and no instruction is sent to the Agent.

Each response from the SAL system to an Agent contains a status. The status contains a value to indicate the message processing status. These values are explained below.

Element

Status - The status of message processing

Value

- 0 – All devices processed successfully
- 1 – The device needs to register with the SAL system
- 2 – Due to problems in the database or LDAP, the device will be put to the maintenance mode

Attributes

- mn – Optional, product family number
- sn – Optional, solution element/asset ID
- ow – Optional, owner

Child element

Inst – Required when status value is "2"

Attributes

- intv – Time interval with the time unit of second
- url – The URL (IP address of the Secure Access Concentrator Remote Server) to which the Agent sends a maintenance ping

Examples:

- All devices were processed successfully

```
<EEnterpriseProxy.Response msgid=”1”>
      <Status>0</Status>
</EEnterpriseProxy.Response>
```

- Process failed because the devices need to register first

```
<EEnterpriseProxy.Response msgid=”1”>
      <Status mn=”Product_family_1” sn=”Serial_1” ow=”acme”>
            1
      </Status>
      <Status mn=”Product_family_2” sn=”Serial_2” ow=”acme”>
            1
      </Status>
</EEnterpriseProxy.Response>
```

- Process failed because of SAL system errors: database or LDAP

```
<EEnterpriseProxy.Response msgid=”1”>
      <Status mn=”Product_family_1” sn=”Serial_1” ow=”acme”>
            2
            <Inst intv=”120” url=”201.20.2.200” />
      </Status>
      <Status mn=”Product_family_2” sn=”Serial_2” ow=”acme”>
            2
            <Inst intv=”120” url=”201.20.2.200” />
      </Status>
</EEnterpriseProxy.Response>
```

- Mixed cases

```
<EEnterpriseProxy.Response msgid=”1”>
      <Status mn=”Product_family_1” sn=”Serial_1” ow=”acme”>
            1
      </Status>
      <Status mn=”Product_family_2” sn=”Serial_2” ow=”acme”>
            2
               <Inst intv=”120” url=”201.20.2.200” />
      </Status>
</EEnterpriseProxy.Response>
```

Configure the time interval value and URL in the *DRMConfig.properties* file; the unit of time for the interval is seconds. The following lines show the default settings

```
com.axeda.drm.devcon.emessage.instruction.maintenance.interval = 120
com.axeda.drm.devcon.emessage.instruction.maintenance.url = 123.45.57.9
```

Handling maintenance status

When a device receives a maintenance status, a maintenance ping at predefined intervals is sent to the Secure Access Concentrator Remote Server in XML. The server returns the status `1000` to indicate that the device is to exit the maintenance mode. It returns the status `1001` to instruct that the device is to stay in the maintenance mode.

Maintenance ping by Agent to Secure Access Concentrator Remote Server

The Agent sends a maintenance ping in XML format to the Secure Access Concentrator Remote Server.

Element

MtMessage – Indicates that this is a maintenance ping

Attribute

id – Maintenance ping ID

Child element

De – Device

Attributes

- mn – Product family
- sn – Solution element/asset ID
- ow – Owner

Example:

```
<MtMessage id="1">
      <De mn="Product_family_1" sn="Serial_1" ow="acme" />
      <De mn="Product_family_2" sn="Serial_2" ow="acme" />
</MtMessage>
```

Handling maintenance ping

A servlet on the Secure Access Concentrator Remote Server (`MaintenancePingServlet`) handles the maintenance ping as follows:

1. The servlet receives the maintenance ping message.
2. It passes the message to other components for further parsing and system checking.
3. When the processing is complete, the servlet sends the response (check status) to the Agent.

Response to maintenance ping

The response from the Secure Access Concentrator Remote Server uses the SOAP/HTTP response command. When a device completes the maintenance tasks, the server sends the status with a value of `1000` to instruct the device to exit the maintenance mode. After a device exits the maintenance mode, the Agent retries posting an electronic message to a URL provided by the instruction.

If a device is to stay in the maintenance mode, the Agent keeps the maintenance ping.

Examples:

- Devices exit the maintenance mode

```
<EEnterpriseProxy.Response msgid=”1”>
      <Status mn=”Product_family_1” sn=”Serial_1” ow=”acme”>
            1000
            <Inst url=”123.45.67.9” />
      </Status>
            <Status mn=”Product_family_2” sn=”Serial_2”
ow=”acme”>
            1000
            <Inst url=”123.45.67.9” />
      </Status>
</EEnterpriseProxy.Response>
```

- Devices remain in the maintenance mode

```
<EEnterpriseProxy.Response msgid=”1”>
      <Status mn=”Product_family_1” sn=”Serial_1” ow=”acme”>
                  1001
            </Status>
      <Status mn=”Product_family_2” sn=”Serial_2” ow=”acme”>
                  1001
            </Status>
</EEnterpriseProxy.Response>
```

- Mixed case

```
<EEnterpriseProxy.Response msgid=”1”>
      <Status mn=”Product_family_1” sn=”Serial_1” ow=”acme”>
            1000
            <Inst url=”123.45.67.9” />
         </Status>
      <Status mn=”Product_family_2” sn=”Serial_2” ow=”acme”>
            1001
         </Status>
</EEnterpriseProxy.Response>
```

Handling reposting of accumulated data from the Agent

When the SAL system errors are fixed and the Secure Access Concentrator Remote Server has responded to maintenance message requests with a `1000` status (exit the maintenance mode), it may be that the Agent now has a large amount of accumulated data to post to the Secure Access Concentrator Remote Server. If the amount of data is too large, the server could incur an overflow burden. You need to track the amount of data the Agents send after the maintenance mode and make sure to limit the impact to the server.

SOAP Response Execution Status Message

When the Secure Access Concentrator Remote Server sends a SOAP/HTTP response to an Agent, that Agent responds by sending a message to the server. This message contains the status of the execution of the SOAP command. The server processes this message to check whether the status is successful, and then responds with a valid status or SOAP response command.

Elements

SOAPStatus – SOAP Response Execution Status message.

Attributes

- t - Timestamp of when this SOAP command is executed on the device.
- cmdId - SOAP command ID that is stored in the SAL database.
- userId - User ID sent in each SOAP command for auditing purpose. The default user ID is axeda.ServiceLink.
- sc - status code list as follows:

  0: Successful

  1: Error

  2: Denied

  3: Denied-timeout

  4: Unsupported

  5: Asking

  6: Ask denied

  7: Ask accepted

  8: Denied-APMOffline

Note:

Sometimes a given SOAP response generates multiple statuses. For example, when the command requires that the Secure Access Policy Server give permission, the statuses may include asking, ask accepted, and successful.

The statuses, asking (5) and ask accepted (7), are not final status. They could be followed by other statuses.

- xsc – Optional, string-formatted explanation of unsuccessful status.

Example:

```
<eMessage id=”2” rc=”0” v=”3.9”>
  <De mn=”Product_family_1” sn=”Serial_1” ow=”acme”>
       <SOAPStatus cmdId=”12” sc=”2” t=”2005-1-1T14:12:50-05:00” userId=”acme” />
       <SOAPStatus cmdId=”13” sc=”3” t=”2005-1-1T14:12:50-05:00” userId=”acme” />
  </De>
<eMessage>
```

SOAP Response Execution Status Trigger

When a server SOAP response sent to an Agent does not run successfully, the Agent sends a SOAP response execution status message with a status code value (value from 1 to 6, see Attributes) and a SOAP command ID. You can use the rules feature of the Device application to configure Agent Command Status rules for the server to evaluate status codes and perform actions based on the results.

Description

To configure an Agent Command Status rule from the Device application, select **New | Rule**, and follow the prompts in the Create new rule wizard. For assistance with any step of the wizard, display the step page, and click the **Help** link.

Status type

Several execution status types can be evaluated. When creating an Agent Command Status rule, you select one type for the rule. Among the types are Successful, Error, Inhibited by Agent, Not Retrieved by Agent, and Not Processed by Agent. See the online help if you need assistance configuring the status type.

SOAP Response Audit

When the SOAP Response Execution Status Message is sent to the Secure Access Concentrator Remote Server, the server audits the status of SOAP command execution on the Agent. The audit can be viewed from the Audit page of the Administration application, and from the Audit Log module on the device dashboard for the selected device (Service application).

Date

The timestamp of auditing

Detail

String representation of SOAP Command ID + status + extension status + executing time + userId

Example:

```
Soap command (id=s5) status: Denied-timeout (denied-timeout...),
executed at 2002-05-15T18:00:00 by user avayaSecureAccessLink.
```

Device

The device name or solution element / asset id that executes the SOAP command

Redundant Gateways mode

For environments that require more than one Gateway to monitor the same set of devices, the Concentrator Remote Server provides a *redundant-gateways* mode, which you can set in the Concentrator Remote Server configuration file, *DRMConfig.properties*. By default, the Concentrator Remote Server runs in the *nonredundant* mode, such that only the first Gateway that registers the device manages the device. For information about setting the property that enables this mode, see the description of the property,

com.axeda.drm.device.redundantgateways, in Appendix C: Editing the DRMConfig.properties File.

To avoid duplicate data being sent through redundant Gateways, the device itself must maintain its state and ensure that it sends data to only one Gateway at a time. No connectivity exists between the Gateways, so the device must ensure that no duplicate data is sent to the Concentrator Remote Server.

After you select the redundant-gateways mode, you can see changes on the pages of the Applications that allow you to assign more than one Gateway to the managed devices. The Device dashboard for a managed device displays information for multiple Gateways in the Device Connectivity module. This module shows the connection between the device and each Gateway as well as between the Gateways and the Concentrator Remote Server. The names of the Gateways are links that display the Device dashboards for the Gateways. The following figure shows an example of this module.

Figure 10-1: Device Connectivity module, showing redundant gateways

The Device Connectivity module includes the tool tips for the icons. For more information, see the online help for the Service application.

When running in the redundant-gateways mode, you can use the Add Devices (to Gateway) page to add the same devices to more than one Gateway. Specifically, the list of Available Devices includes *all* devices to which you have privileges and does not exclude devices that have been assigned to another Gateway.

When running in the redundant-gateways mode, two additional device events become available for configuration as device conditions:

- Concentrator Remote Server to Gateway connection partially compromised
- Device to Gateway connection partially compromised

When one or more connections, either between the Concentrator Remote Server and the Gateway or between the Gateway and the device, are lost but not *all* connections are lost, the Concentrator Remote Server treats the connections as *partially compromised*. To create a device condition for either or both of these events, you assign a name, a severity, and an image.

When the event occurs, the Concentrator Remote Server sets the condition for the device. See the online help for the Device application for more information about configuring device conditions.

In addition to the device events, you can configure a Connectivity rule for devices when running in the redundant-gateways mode. This rule allows you to configure actions that you want to take when changes in the connectivity between managed devices and Gateways or between the Gateways and the Concentrator Remote Server occur. See the online help for the Device application to get information about configuring rules.

Note:

Avaya recommends that you use the Connectivity rule when running in the redundant mode instead of the Is Missing and the Device Returned rules.

Reverting to the nonredundant-gateways mode

While enabling the redundant-gateways mode does not require any changes to the database, subsequently reverting to the nonredundant-gateways mode does require you to run an SQL script to remove any rules and device conditions that are available exclusively in the redundant-gateways mode. After reverting and updating the database, all Gateways must be restarted by sending a package that includes a Restart instruction. Then, when a Gateway registers with the Concentrator Remote Server and associations of many Gateways to one device are found in the database, the associations are removed before the device is registered. In this way, the system reconfigures itself over time until all Gateways have been restarted and the devices reregistered. During the period of restarting and reregistering, the Device dashboard shows only the first Gateway in the original list as the managing Gateway.

For more details about the redundant-gateways mode, see the online help for the Applications.

Notifying the Concentrator Remote Server about the status of SOAP commands

To enable Agents to provide feedback to the Secure Access Concentrator Remote Server about the status of SOAP commands, a thread that processes SOAP commands asynchronously has been added to the Agents. When it receives a SOAP command, the Agent places the command in a queue for the SOAP processing thread. The thread processes the commands as follows:

1. For each command received, a SOAP parser object is created.
2. The SOAP manager calls a registered handler.
3. The handler sends the status of the SOAP command to the Secure Access Concentrator Remote Server.

To support the Secure Access Policy Server, SOAP commands include attributes for user identification (userId) and command identification (cmdId).

The SOAPStatus element notifies the Secure Access Concentrator Remote Server of the status of SOAP commands. As a response to a SOAP command, SOAPStatus also contains user and command identification attributes. The EnterpriseProxy component exports a corresponding interface method to facilitate delivery of this element to the Secure Access Concentrator Remote Server.

Agent-generated package status codes

From the Software Management application, users can send packages to the Agents. These packages can contain instructions for the Agents to run scripts, update software, retrieve files, and perform other maintenance and diagnostic tasks. In response, the Agents send Package Status codes as a PackageStatus POST to the Secure Access Concentrator Remote Server. The numbers of these codes correspond to values on the server. When a status is psError, the Agents send additional information (error codes) as a PackageStatus POST. The error codes are attributes of the psError code.

The table below provides the Agent-generated package status codes.

Table 10-1 Agent Package Status Codes

Agent sends	# Concentrator Remote Server displays...	What it means...
psQUEUED	0 **Queued**	The Agent has put the package in a queue for processing.
psSTARTED	1 **Started**	The Agent has started processing the package.
psSUCCESS	2 **Complete**	The Agent has successfully processed the package. No errors occurred during processing.
psERROR	3 **Error**	The Agent did not complete processing the package, some errors occurred. The Agent sends error information, using the error codes shown in Table 10-2 Package Error Codes.
psCANCELED	4 **Canceled**	The Agent received a SOAP command that canceled the package. The agent did not finish processing the package.
psTIMEOUT	5 **Timed Out**	The package timed out either while waiting in the queue to be processed or while the agent was processing it. If the package contained dependencies that could not be run because information could not be obtained, this situation could arise.
	7 **Missing**	The package is missing. The Software Management application uses this status code internally. Most likely, the device is missing. It may be that the Agent shut down unexpectedly and has not been restarted. Download the package again.
psROLLING_BACK	8 Rolling Back	The Agent is in the process of rolling back the package. Wait until the rollback is complete. If the rollback is successful, check the audit log for any potential problems. Then, download the package again. If the rollback is not successful, check the errors and resolve them before attempting to retry the package.
psROLLBACK_ERROR	9 Rollback Failed	The Agent attempted to roll back the package, but some errors occurred so the rollback failed.
psROLLBACK_ SUCCESS	10 Rollback Successful	The Agent completed the rollback without any errors.
psDEPENDENCY_ FAILED	11 Dependency Failed	A pre-process dependency for the package failed.

Agent sends	# Concentrator Remote Server displays...	What it means...
	12 Cancel Pending	The Software Management application on the Concentrator Remote Server uses the status 12 internally to acknowledge the cancellation of a pending package.
psPendingAsk = PS_PENDING_ASK APM_STATUS_ASKING (0x40000004L)	13 Pending Ask	This status is specific to the Secure Access Policy Server and generated by the Pampered component of the Agent. This status indicates that the Agent is asking the Secure Access Policy Server for permission to run the package
psPermission-Denied = PS_PERMISSION_DENIED APM_STATUS_DENIED (0x40000001L)	14 Permission Denied	This status is also specific to the Secure Access Policy Server and generated by the Pampered component of the Agent. This status indicates that the policy prevents the package from being run (permission denied).
psFile_Inhibited = 15 KE_INHIBITED (2)	15 File Upload Inhibited	The SDK Custom Handler inhibited one or more files. If this behavior is expected, then you do not need to do anything. If not, then check the code in your custom handler and the file name. Make whatever changes are needed to correct the situation, update the custom handler on the device, and restart the Agent.
	16 Duplicate Script Name (Hidden)	The package has the same name as an invisible script. Change the name of the package and download it again.

As stated earlier in this section, when the status code for a package is psError, the Agents send the error codes (as attributes of the psError status code) in a PackageStatus POST to the Secure Access Concentrator Remote Server. The error codes that may be generated are listed in Table 10-2.

Table 10-2 Package Error Codes

Package Error Code	Explanation
peFAILED	0: The Agent failed to process the package.
peBAD_FORMAT	2: The Agent detected invalid XML formatting in the package.
peUNKNOWN_SOAP_METHOD	3: The Agent did not recognize the SOAP method. Check for a possible misspelling in the package content or a mismatch between the versions of the Agent and the Concentrator Remote Server.

Package Error Code	Explanation
peUNSUPPORTED_FUNCTION APM_STATUS_UNSUPPORTED (0x40000003L)	4: For example, the component was not found for a data item dependency.
peDI_NAME_NOT_FOUND KE_DI_NOT_FOUND (0xC0000400L)	5: The agent detected an unknown data item name in a dependency. The specified data item was not found.
peREGISTRY_NAME_NOT_FOUND KE_SCM_REGISTRY_ENTRY_NOT FOUND (0xC0001300L + 6)	6: The registry entry name was not found.
peREGISTRY_FILE_READ_ERROR KE_SCM_REGISTRY_FILE_ERROR (0xC0001300L + 7)	7: Failed in reading or parsing registry file; the dependency cannot be executed.
peINVALID_DEPENDENCY_EXPRESSION KE_SCM_DEPENDENCY_FAILED (0xC0001300L + 12)	8: The operator or expected value in the dependency is invalid.
peNO_FILES_FOUND KE_SCM_NO_UPLOAD_FILES (0xC0001300L + 2)	9: For an upload, no explicitly defined files were found,
peSOME_FILES_NOT_FOUND KE_SCM_PARTIAL_UPLOAD_FILES (0xC0001300L + 3)	10: For an upload, only some of the explicitly defined files were found and sent to the Server. Some were *not* found.
peDOWNLOAD_EXECUTION_FAILURE KE_SCM_DOWNLOAD_EXECUTION_FAILURE (0xC0001300L + 1)	11: The Agent failed to execute the first file in the download.
peARCHIVE_ERROR	12: One of the following operations on an archive file (tar.gzip) failed: creation, extraction, list, file name, and so on.
peREAD_ERROR	13: An attempt to read an archive being uploaded failed.
peHTTP_STATUS_ERROR KE_SCM_HTTP_STATUS_ERROR (0xC0001300L + 5)	14: An HTTP status error occurred.
peCHUNK_CHECKSUM_ERROR KE_SCM_MD5_CHUNK_ERROR (0xC0001300L + 8)	15: Even after *n* retries, a Chunk Checksum (MD5) error occurred (e.g., checksums did not match) during file download.
Web Client failures	
peCONNECTION_FAILURE	16: A Web Client connection error occurred. The Web Client could not connect to the Concentrator Remote Server.

Package Error Code	Explanation
peSOCKS_FAILURE	17: The SOCKS connection for the Web Client failed.
peHTTP_FAILURE	18: The HTTP connection for the Web Client failed.
peSSL_FAILURE	19:The SSL connection for the Web Client failed. The possible causes: the certificate could not be validated; the SSL port is not configured correctly; network problems made it impossible to make the connection.
peAGENT_SHUTDOWN	20: The Agent has been stopped.
peFILE_CHECKSUM_ERROR	21: Even after n retries, a FILE Checksum (MD5) error occurred during file download
peUPLOAD_FILE_MISSING_ERROR	22: A *partially* uploaded file is missing at the upload request.
peINVALID_DIRECTORY KE_SCM_INVALID_DIRECTORY (0xC0001300L + 12)	23: The requested directory cannot be created.
peRESTART_OF_GATEWAY_DEVICE KE_SCM_RESTART_OF_GATEWAY_DEVICE (0xC0001300L + 13)	24: The Agent cannot restart a device managed by the gateway device (only the Gateway Agent itself).
peCUSTOM_SOAP_FUNCTION_ERROR KE_SCM_CUSTOM_SOAP_FUNCTION_ERROR (0xC0001300L + 14)	25: General Purpose error that is used by custom SOAP functions that have an error.

Status codes for SOAP commands

The Agents return status codes in response to the SAL system SOAP commands. These codes are *not* errors. Rather, they indicate the status of the SOAP command, especially with regard to the interactions between the Agents and a Secure Access Policy Server.

Audit messages for file transfer activities during remote desktop sessions

For remote desktop sessions established through the Service application, all activities in the File Transfer window are audited. The Desktop Server sends audit messages to the Agent, which forwards the messages to the Concentrator Remote Server for display in the Device dashboard and the Administration application. When a remote desktop session is started from the Service application, the Agent connects to the Desktop Server, listening on port 8330. As file transfer activities occur, the Desktop Server writes audit messages to this port.

This method of auditing ensures that the Agent associates each remote desktop session with the correct session ID assigned by the Concentrator Remote Server.

The messages that you may see include completion and failure messages for uploads and downloads as well as messages that a folder or file was renamed, as follows:

- Folder renamed
- File renamed
- File upload complete
- File upload failed
- File download complete
- File download failed
- Folder upload complete
- Folder upload failed
- Folder download complete
- Folder download failed
- Folder deleted

Federated Communications support

A Concentrator Remote Server can be used as the sole server in a SAL system setup, or as part of a parent-child setup in which one or more SAL servers operate as parent servers to one or more SAL servers that operate as child servers to those parents. The latter setup is known as Federated Communications. In this type of communications, the child Concentrator Remote Server, or *site server*, is configured to forward remote session information and event and data item values to another Concentrator Remote Server.

Note:

The terms site server and child server are used interchangeably throughout this section.

Either server in this setup can operate as a parent server, and receive data from other child (or site) servers, or it can operate as a child server and forward its data to another (parent) server. A child server can have only one direct parent server, which means that it can forward its data to only one server. That parent server can forward to another server (and would therefore act as a grandparent server to this fist child server and as a parent to the second child server, in this example). For further explanation, see the following example.

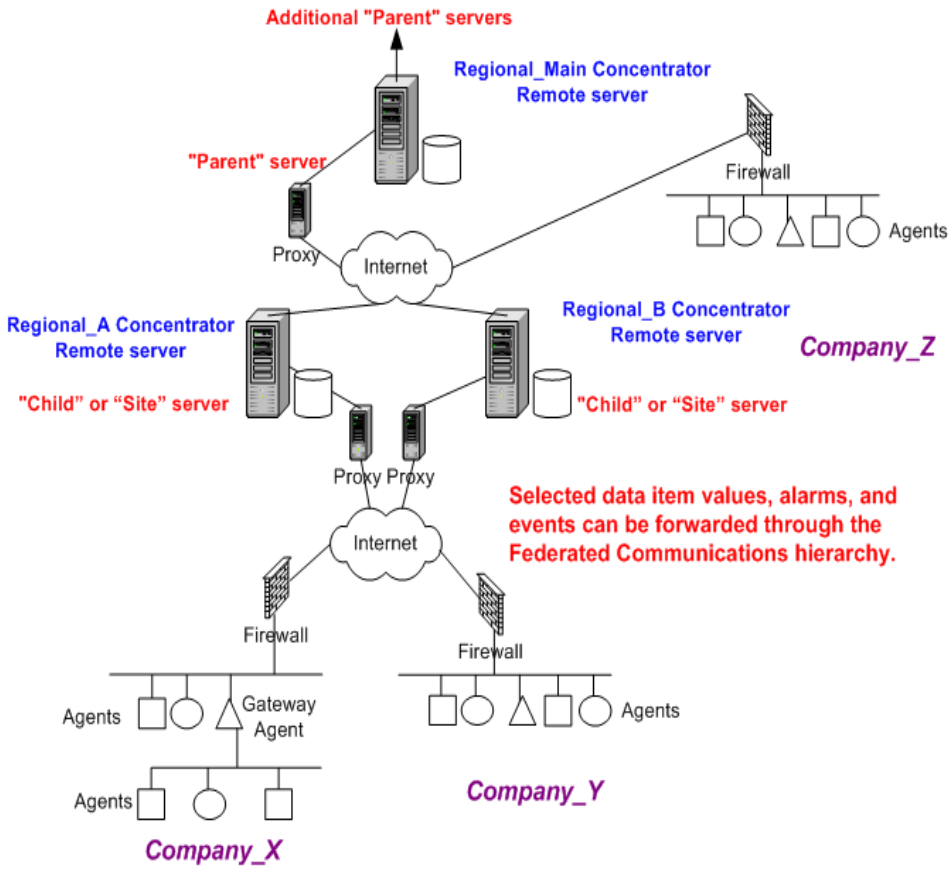


Figure 10-2: Example of Federated Communications setup

In Figure 10-2, data from devices at Company_X and Company_Y report to two site servers, Region_A and Region_B, respectively. Region_A and Region_B Concentrator Remote Servers forward remote session information, alarms, and events to another Concentrator Remote Server, Regional_Main. In addition, data for devices at Company_Z is reported directly to the Regional_Main Concentrator Remote Server.

Regional_Main could be configured to forward to another Concentrator Remote Server, as needed.

Server support for site server communications

By default, the server is set up to support Federated Communications. There are several server properties that control the communications between the site/child server and its parent. These properties are as follows:

com.axeda.drm.parent-server.post-rate=30

com.axeda.drm.parentserver.ssl.verifyhostnames= true

com.axeda.drm.parentserver.ssl.strictcertificate-verification =true

See Appendix C: Editing the DRMConfig.properties File for more information about these settings.

In addition, the Log4j properties files provide logging support for Federated Communications, known as parent-child configuration. By default, debugging for parent-child configuration is disabled. To enable the server to generate parent server debugging messages, you need to enable debugging in the Log4j.properties file. See Setting up logging in Appendix B: Concentrator Remote Server Files.

Configuring the Concentrator Remote Server as a site server

To use the Concentrator Remote Server as a child or site server in an Federated Communications setup, you need to do the following:

1. Open a Web browser session to this Concentrator Remote Server.
2. Navigate to the Administration Application, Administration home page.
3. Select the **Parent Server** menu. The Parent Server Configuration wizard appears.
4. Configure the information as prompted, including the host name and port of the parent server for this site server, the ping rate settings, SSL communications settings, and what information you want this site server to send to the parent server and how frequently.
5. Make sure the Certificate of Authority (CA) for this server is the same as the parent server's CA certificate. If the CA is different, you need to import the parent server's CA certificate. See the instructions in Chapter 3, "Using a Sun ONE LDAP Directory Server with SAL."

Support for multiple Concentrator Remote Servers

The Agents can communicate with more than one Secure Access Concentrator Remote Server. Communication with the following types of destination servers is supported:

- Primary Secure Access Concentrator Remote Server. Under normal conditions, the Agent uses this server for exchanging messages. This is a single Concentrator Remote Server if no others are defined.
- Backup Secure Access Concentrator Remote Server. The Agent switches to this server when it detects consistent failure in communication with the primary server.
- Additional Secure Access Concentrator Remote Server. When the Agent's Logger schema specifies that a non-primary server must be used for an *Enterprise stream* logging destination, the Agent uses this server for posting data and alarms.

Agents support dynamic redirection between servers through a command from the server. Dynamic redirection prevents any potential data loss while the Secure Access Concentrator Remote Server is unavailable, and provides for load balancing among Secure Access Concentrator Remote Server.

The Agent's project must be configured for communications with each type of server. The communications include the string alias name for the server, the hostname or IP address of the server, the port number for server communications. Proxy server parameters are not a part of a specific Secure Access Concentrator Remote Server definition. Rather, the Agents use global proxy server settings for requests to all Secure Access Concentrator Remote Servers.

Using different types of Concentrator Remote Servers

Each Agent keeps track of the locations of each Secure Access Concentrator Remote Server with which it communicates.

Communications failures that may occur include TCP/IP transport error, SSL error, HTTP error, and timeouts. If it detects a communications failure for three consecutive requests to the primary server, the Agent switches to its defined backup server. While communicating with the backup server, the Agent continuously attempts to re-register with the primary server. When registration with the primary server is successful, the Agent switches communications back to the primary server.

An Agent's Logger schema may explicitly specify a destination server for the logged data. In this case, messages should be sent to a current location for the specified additional server.

Dynamic redirection and maintenance mode

The SAL system supports dynamic server redirection, which means that an Agent can be instructed (by its project configuration) to use another Secure Access Concentrator Remote Server during run time. For example, if the Concentrator Remote Server is in the *maintenance mode* (and therefore temporarily incapable of processing device data, perhaps because the database or LDAP server is down), the server notifies the devices using a SOAP response status value. This response also contains a servlet location, which should be used by the device to send special ping messages. Devices will not post data after the Concentrator Remote Server has indicated to be in the maintenance mode. Two types of return status values may be sent in response to the ping messages:

- Continue to ping, withhold device data.
- Return to the normal mode using a server location specified in the response.

All Concentrator Remote Server commands in the described schema address individual devices. This means that all or some of the devices may be redirected to other Concentrator Remote Servers as a result of using the maintenance mode. This redirection mechanism applies to all types of Concentrator Remote Servers (Primary, Backup or Additional) because the Concentrator Remote Server is not configured to function for specific devices only.

To support different types of Concentrator Remote Server as well as dynamic server redirection, the Agents maintain the following set of run-time properties:

- Primary server descriptor
- Backup server descriptor
- A list of additional server descriptors
- Flag indicating whether primary or backup server is used

Each server descriptor includes the following properties:

- Reference to the default server attributes configured in the project.
- Current server location, specified by the URL provided by the Concentrator Remote Server during the redirection procedure. If empty, default server attributes are used.
- Flag indicating whether the device is registered with the server.
- Flag indicating whether the server is in the maintenance mode.

Prior to posting data to any type of Concentrator Remote Server, a device must be registered with that server. A dedicated registration thread performs device registration with all servers. This thread is activated each time any change in server disposition is detected. Its task is to register devices with primary and additional servers for which registration flags are not set. The registration thread also tries to register devices with the backup server, if they must use it and they are not registered with it.

A dedicated ping thread sends normal and maintenance ping messages for each device. This ping thread sends normal ping messages to the primary, backup, and additional servers as long as the device is registered with them. This thread also sends maintenance ping messages to the servers for which maintenance mode is indicated with the corresponding flag.

Device data elements are placed in the EnterpriseProxy queue, when submitted for delivery by other components. The EnterpriseProxy component of the Agent limits the queue size by the total size of items. Items in the queue may be deleted when the queue becomes full. That means that when a new data element is submitted and the queue is full, the less significant item (oldest, with lowest priority) is replaced.

A dedicated queue processing thread actually delivers the contents of the queue. This thread delivers device data to different servers according to the following rules:

- Queue items are selected for delivery based on the age and priority as well as on the *flush size*. Flush size is the maximum allowed formatted message size.
- For each data element of a device, the run-time properties of the associated device are used.
- The destination server for a device data element is determined by the destination server specification for the element (provided by its source).
- If a destination server is not explicitly specified by the data source, the destination server is determined by the value of the device's primary/backup server flag.
- Destination server parameters are taken from a corresponding device's server descriptor.
- If a registration flag is not set or a maintenance mode flag is set in the server descriptor, the data element is not delivered and remains in the queue.
- Data elements qualifying for delivery are grouped into messages by destination server. The resulting set of messages is submitted for delivery to the Web Client.
- The Web Client performs a set of simultaneous HTTP requests to deliver the data.

Communication scenarios

Consider the following scenarios involving different Concentrator Remote Server statuses.

Normal operation

Under normal circumstances, when the EnterpriseProxy component of the Agent starts, all servers for all managed devices are marked as not registered. The registration thread tries to register all devices with the primary server and additional servers using location attributes specified in project. This registration process runs until all of these servers are marked as registered for all devices. A server accepts data updates from a device only if that device is registered with it.

Communication failure with primary server

When the EnterpriseProxy component detects consistent communication errors with its primary server, it clears the registration flag for all primary server entries pointing to the same server. This action indicates that the registration thread should try to register all affected devices with their primary servers again. The action also indicates that the affected devices should use their current backup servers and clears the registration flag of their backup server descriptors. The registration thread then registers the devices with their backup servers. As soon as registration is successful, device data begins to flow to the backup servers.

Concentrator Remote Server indicates maintenance mode

When the EnterpriseProxy component receives a server's notification that the server is going into the maintenance mode, the server descriptor of the corresponding device is updated with new location attributes (if the server provided them). Additionally, the maintenance mode flag is set and the registration flag in the server's descriptor is cleared. The maintenance mode flag indicates that device data should not be sent. Also, this causes the ping thread to send maintenance ping messages to the specified location. If a response to such messages instructs a device to return to the normal mode, the maintenance mode flag is cleared and the current location is updated (if specified by the server) in the device's server descriptor. This allows the registration thread to begin registration of the device with the server. This handling applies to all types of Concentrator Remote Servers.

Error handling extensions

The SAL error handling mechanism operates as follows:

- When the server encounters some kind of inconsistency inside a received message (for example, the data type specified for a data item does not match the data representation), it silently skips the faulty part of the message. No error notifications are sent back to the Agent.
- When it receives indication of an error that requires a recovery action, the Agent performs this action first and then continues with its normal tasks.
- All result statuses indicating a failure address devices whose data elements caused an error condition during processing.
- A result status message may contain additional elements and attributes intended to facilitate a recovery action.

Possible error result statuses

Status: Device is not registered

If for some reason a result status indicates that a particular device is not registered with the Concentrator Remote Server, the registration flag in the corresponding device's server descriptor is cleared, causing the device to re-register with the server.

Status: Maintenance mode

When the Concentrator Remote Server returns a status indicating that it is in the maintenance mode, the Agent performs the actions described in the section, Concentrator Remote Server indicates maintenance mode.

Configuring Concentrator Remote Server to use a Syslog server

You can configure the Concentrator Remote Server to use a Syslog server as another means of capturing audit information. By default, the Concentrator Remote Server uses the JDBC Auditor for capturing this information; however, you can also add a Syslog server to this configuration as another destination for audit information.

To configure the Concentrator Remote Server to send audit log information to a Syslog server, do the following:

1. Configure the host, port, syslog facility ID, and message format template for the Syslog server in the log4j.properties file, *log4j.appender.SYSLOG* properties.
    - Modify the DRMConfig.properties file, *Audit Log Settings* properties, to (1) add the Syslog auditor type, and (2) specify the types of audit categories to dispatch (or send to the auditors). Note that if you leave the audit category property blank, *all* audit category types are dispatched to the Syslog server at the server location defined in the log4j.properties file.

See Setting up logging for information on configuring the log4j.properties file and DRMConfig.properties, and Audit Log Settings (Syslog Server settings) for information required to set up a Syslog server for your Concentrator Remote Server.

SOAP command status notification for Secure Access Policy Server

To support Secure Access Policy Server functionality, SOAP commands include attributes for user identification (userId) and command identification (cmdId). These attributes are processed by the Policy Server.

The eMessage element (SOAPStatus) is used to notify the Concentrator Remote Server about the status of a SOAP command's execution. As a response to a SOAP command, SOAPStatus also contains user and command identification attributes.

Database administration tools

The SAL system is a complex combination of technologies, and it is strongly recommended that you become familiar with the documentation of the Oracle Database System, the Web Application Server, and the LDAP directory server that you are using with the SAL system. This section provides an overview of the administration tools available to you.

Oracle database system management tools

The Oracle Enterprise Manager provides a Web-based interface for managing all the activities of your database. Depending on the size and organization of your company, you may perform all the management, maintenance, and performance tuning activities using this tool. In large organizations, different people may be using this tool for their specialty

tasks, such as routine backup and recovery and performance analysis, administrative tasks such as creating schema objects (tablespaces, tables, and indexes), managing user security, backing up and recovering your database, and importing and exporting data. You can also view performance and status information about your database instance.

As needed, you can also return to the Oracle configuration utilities to fine-tune the parameters of the database. For example, you can use the Oracle Database Configuration Assistant (DBCA) to delete a database, add options to a database, or to manage database templates.

Note:

A template is a definition of a database saved in an XML file format that can be used to create other databases.

Backing up and restoring applications

In addition to performing system-wide backups on a regular basis, the application information described in Table 10-3 should also be backed up on a regular basis. Database Administrators should visit http://www.oracle.com/technology/documentation/index.html for information about backup and restore practices for the SAL system.

Table 10-3 Backing up and restoring applications

Application	Backup	Restore
SAL Application	Periodically back up the SAL folder that was installed from the CD (typically located on a drive's root, such as `C:/server/SecureAccessLink/deploy`, `D:/server/SecureAccessLink/deploy`, `E:/server/SecureAccessLink/deploy`, and so on.)	Restore the SAL folder that you backed up to its original location.
LDAP Directory Server	You can export the contents of the directory server while it is running. This operation saves the data to a flat file, which you can import at a later time. To export the contents of the LDAP server: a. Sign onto the LDAP administration console, using the administration user name and password. b. Open the Directory Server. c. Locate the command that allows you to export databases. d. Type a file name for the exported content. e. As appropriate, choose the type of export. f. Click OK.	To restore directory server data, you can import the file you exported. Perform this operation while no applications are accessing the database. To import the data into the LDAP server: a. Sign onto the LDAP administration console, using the administration user name and password. b. Open the Directory Server. c. Locate the command that allows you to import databases. d. Select the exported file. e. As appropriate, choose the type of import. f. Choose whether to continue on error, and select a file for any rejected records. g. Click OK.

Using the JBoss JMX console

SAL and JBoss install several components, each of which may need your attention after your system is up and running.

Use the JMX Console to help troubleshoot any installation or configuration issues, such as the J2EE services running.

To access the JMX console, start the server and open a Web browser to the following URL: *http://localhost:8080/jmx-console/*. The JBoss Management Console appears, showing all of the services included in the currently running JBoss configuration and various details about each service.

The default user name and password for using the JMX Console with SAL is **admin** (user name) and **admin** (password).

Troubleshooting installation and configuration

If you have not installed and configured the SAL system and its various components correctly, starting or testing the system does not produce the expected results. In addition, if you are reinstalling any components, older files that have not been deleted can cause trouble. This section addresses some of the more common problems discovered during testing.

Troubleshooting a new installation

The most common problem that users encounter during a new installation of the Agents and the SAL system is lack of communication between the Concentrator Remote Server and the Agents, particularly, when the Agent is running as a service. To help Avaya Technical Support to service your call more quickly, use the following procedure to collect the information they request. Open an online file and record your observations and results of each step in the procedure. You can also jot down your observations on paper.

1. Check if the Agent is starting when configured to run as a service, If not, unregister the service (`ekernel -unregister` or `xgate -unregister`). Then run the agent from the command prompt and observe any messages that result. These messages are stored in the log file of the Agent.
2. Retrieve the log file of the Agent. The log file is stored in the root directory of the Agent, and the name of the file is `ekernel.log` or `xGate.log`. If your project is configured to create multiple log files, the number of the file is appended to the name.
3. Check the following infrastructure issues:
    - SSL. If you have configured the Agent and Concentrator Remote Server to use SSL to communicate, verify that the port number is correct (default is 443). Then, check that the SSL strength is configured correctly for both sides. Keep in mind that only a UNIX-based Web Server supports the 128-bit encryption level of SSL.

- Proxy setup. If you are using a proxy server between the Agent and the Concentrator Remote Server, verify that it is configured correctly (use the Deployment Utility).
- Browser setup. Check the setup for Internet Explorer:
    a. If possible, open Internet Explorer and attempt to access your secure HTTP (https) SAL server. You should be able to reach the point where you are prompted for the login screen for the SAL applications.
    b. If you see a prompt for SSL authentication, click **Yes** to continue to the login screen. If not, record that problem in your log for Avaya Technical Support.
    c. On the **Tools** menu, click **Internet Options.**
    d. When the Internet Options dialog box appears, click the **Connections** tab.
    e. On the **Connections** tab, click **LAN Settings**. The Local Area Network (LAN) Settings dialog box appears, as shown in Figure 10-3.

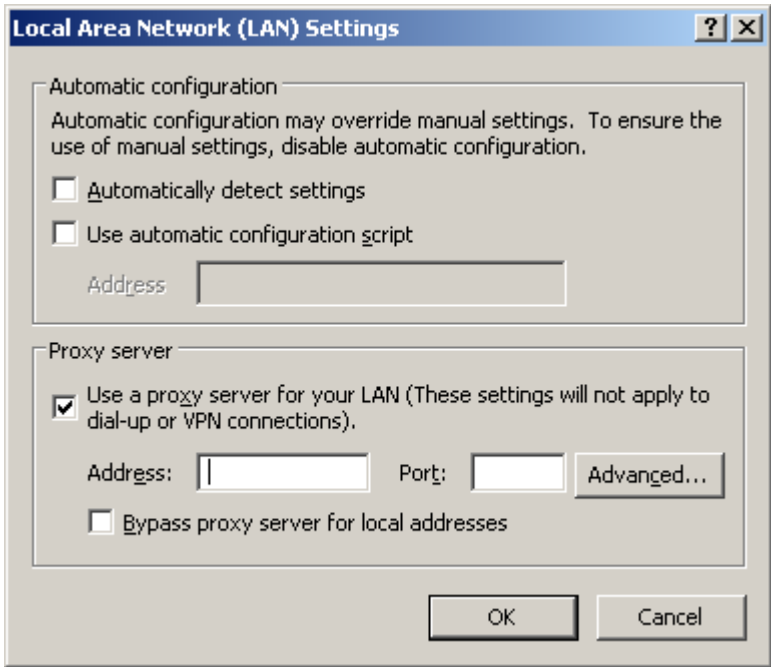


Figure 10-3: LAN Settings dialog box

    f. Verify that the proxy server settings are correct. In addition, either take a screenshot (press ALT+PrtScr) or copy down the proxy server settings shown here.
    g. If your proxy server setup also requires domain and user name information, verify that the information is correct and write it down.
    h. If you are using an automatically configured proxy server, a URL is usually required for the *.pac file. Make sure that you have the correct URL.
- Firewall. Check the firewall setup for the following:
    a. Check if there is a firewall that could block either posting data or receiving responses.

b. Check if the firewall blocks any MIME types. Print out the MIME Types check list. Then check all of the MIME types and write down Yes or No to indicate whether the MIME type is blocked by your firewall.

Checking for blocked URIs in the infrastructure

The following Uniform Resource Identifiers (URI) are required between the Agents, Access ARemote, and Web Browser to correctly communicate with the Concentrator Remote Server. If the Agent, Access ARemote, or Web Browser is not correctly communicating or suddenly stops communicating with the Concentrator Remote Server, check with your IT department to make sure that these URIs are not being blocked anywhere upstream in the network.

URI	Used by
/drm/*	User
/remote/*	jta20.jar, appbridge.jar and Agent
/eMessage	Agent
/MtMessage	Agent
/pserver	Access ARemote
/pviewer	Access AViewer
/pgetsession	Access ARemote
/paudit	appbridge.jar (for APB Access sessions)
/poptimize	Agent Access (ARemote & AViewer), jta20.jar, and appbridge.jar
/pconnectioninfo	For connection information tracking
/psessioninfo	Access (ARemote & AViewer)
/pfiletransfer	Access ARemote
/upload	Agent
/download	Agent
/images/*	
/istyles/*	
/index.html	

MIME Types check list

- For EMessage:
  - Agent -> Enterprise (POST)

    Content-Type: application/octet-stream

    Content-Length: 200

    Connection: Keep-Alive

    Expect: 100-continue

  - Enterprise -> Agent (reply)

    HTTP/1.1 100 Continue

    HTTP/1.1 200 OK

    Content-Type: application/octet

    Content-Length: 263

    Connection: close

    ...(data)
- Remote Session (GET)
  - Agent -> Enterprise

    Connection: Keep-Alive
  - Enterprise -> Agent (reply)

    Content-Length: 24

    Content-Type: application/octet-stream

    Connection: Keep-Alive

    Cache-Control: no-cache
- Remote Session (POST)
  - Agent -> Enterprise

    Content-Type application/octet-stream

    Content-Length: 24

    Connection: Keep-Alive
  - Enterprise -> Agent (reply)

    Content-Length: 4

    Connection: Keep-Alive
- File Upload (POST)
  - Agent -> Enterprise

    Content-Type: application/octet-stream

    Content-Length: 467

    Content-MD5: AxaxNGXeCARFwb5udFnQEQ==

    Connection: Keep-Alive

    Expect: 100-Continue
  - Enterprise -> Agent (reply)

    HTTP/1.1 100 Continue

    (data)

    HTTP/1.1 200 OK

    Content-Length: 0

Problems and actions

Problem: No connection to the database found.

Action: Look in the command shell window for entries identifying the starting of the connection pool.

For instance,

```
"Tue Mar 27 12:54:48 EST 2008: <I> <JDBC Pool> Connection for pool "ACMEPool"
created."
```

If this message does not appear, you may not have defined the connection pools correctly in the DRMConfig.properties file or database itself.

Problem: One or more services is not running.

Action: To determine if all the defined services started, refer to the command shell window for the messages identifying how many .jar files are loaded and how many Enterprise JavaBeans (EJBs) are deployed.

For instance,

```
"Tue Mar 27 12:54:56 EST 2001: <I> <EJB> 6 EJB jar files loaded, containing 12
EJBs."
```

```
"Tue Mar 27 12:54:56 EST 2001: <I> <EJB> 12 deployed, 0 failed to deploy."
```

If there is a discrepancy between the number of EJBs contained in the .jar files and the number of EJBs deployed, then there is a problem.

Make sure all the .jar files containing the services (Enterprise JavaBeans) to start are located correctly in the `/jboss-eap-4.3/jboss-as/lib` folder.

Problem: Cannot find sound files.

Action: Check that the sound files are on the Web Application Server in the SAL application subdirectory. Within the ServiceLink.ear application, the sound files are stores in `/jboss-eap-4.3/jboss-as/server/SecureAccessLink/deploy/servicelink.ear`, in the `/tones` subdirectory of your Web Application Server.

Preventive maintenance

This section is intended primarily for Concentrator Remote Server maintenance personnel, including server administrators and database administrators, who need to ensure that the Concentrator Remote Server system is functioning properly.

SAL best practices

To ensure your Concentrator Remote Server's optimized performance and to proactively prevent problems, certain server monitoring and maintenance tasks should be performed. Executing these tasks will help ensure that your server is running at peak performance, as well as identify any areas of potential problems or under-utilization. Results of the tasks may show that you need to swap or upgrade the hardware or software components of your system, modify your server's configuration, adjust networking setup, and so forth. These tasks should be considered basic to your server best practices.

Preventing problems

The list of server maintenance tasks includes those that should be performed frequently, such as each hour, as well as those that should be run only once each week or month. Some of the tasks should be performed by a DBA familiar with the SAL database, while others can be executed by a less-technical individual with access to and some knowledge of the Concentrator Remote Server.

Table 10-4 Maintenance Tasks Timeline

When	Component	Task	Description
As Needed	SAL Application Server	Monitor JBoss server queue and throughput	When the system slows down, monitor queue and throughput through the Care system or through a maintenance script. Make sure queues are not building up, and that throughput is increasing with incoming requests.
Daily	SAL applications and Concentrator Remote Serve	Monitor the *drm.log* file	Locate the drm.log file for the Concentrator Remote Server in the server directory. For example, `/JBOSS_home/server/<SecureAccessLink_server>/log` where `<SecureAccessLink_server>` is the name of the server created by the Concentrator Remote Server installer in the JBoss Server. For more information about what to look for in this file and how to set the logging levels, see Debugging Problems Using Server Logs.
	Database Server	Monitor Oracle Tablespaces for overall percentage use of the file, including possible data file extents.	If the tablespace is near the maximum percentage full and the data file does not extend further, then a new data file needs to be added. For example, if the tablespace is 100% full at just 10 MB in size but can extend to 2 GB, then the tablespace is not an issue. If the tablespace is 95% full at 2 GB and it extends to 2 GB, then a new data file is needed
Weekly	Secure Access Link Application Server	Monitor server disk space	Monitor disk space in the server and ensure that there is at least 1 GB free as a standard part of monitoring your operating system.
	Database Server	Monitor server disk space	Monitor the server disk space and verify there is at least 5 GB free. Follow these steps: a. If there is no space, you cannot add more data files or extend current ones. b. If the server is low on space, check for old database archive logs and other files that can be deleted and delete those files. c. If you find space is still low after deleting extraneous files, check the archive rules to determine if old data can be deleted. As a final option, if space is still too low you can add more disk space.
		Verify tablespaces extents and disk space requirements	Make sure that there is enough free disk space and tablespace to permit that server to log the next week's (or more) worth of data.

Troubleshooting problems using log files

If a problem occurs in the system, you need to determine the cause of the problem. Diagnosing the problem helps in determining the system areas that are affected and preventing future problems.

Avaya Support provides the following recommendations when troubleshooting your SAL system. The troubleshooting procedure you choose is determined by the actual problem and symptoms exhibited by your SAL system.

Troubleshooting problems using server logs

By far, the most important part in debugging any problems in the SAL system centers around the information provided in the log files. Typical problems identified in the logs would be errors in database connections or problems with devices posting data from the field. For the most part, you will be able to determine any errors and reasons for those errors.

The drm.log file

Created in the server entry directory, `/<JBOSS_home>/server/<SecureAccessLink_server>/log` where <SecureAccessLink_server> is the server entry, this file includes information from the SAL applications as well as the Concentrator Remote Server. When troubleshooting, check this file first.

All logging parameters (for example, level of information) for drm.log are set in the SAL log4j.properties file, which you can find in the SAL installation directory, `/avaya/SAL/CRS/config/`. Avaya recommends that you open this file and set it up for your environment so that the files do not become very large, very fast. For an example of this file, see Configuring error logging for drm.log.

Real world example of log:

```
Connection Pool "SecureAccessLink Pool" deployment failed with the
following error: 0:Could not create pool connection. The DBMS driver
exception was: IO exception: The Network Adapter could not establish
the connection
```

This error indicates that the server administrator needed to investigate the network link to the database and determine if the database instance was started and running. This problem resulted from the database instance being shutdown. Starting the database service fixed the problem.

Viewing log files

The best way to view the log files is to open them in Notepad or a similar purely text editor. WordPad will not work because the log files are locked.

Logging levels of the Concentrator Remote Server

Descriptions of the error logging levels, in order of increasing verbosity for the log file, are as follows:

1. NONE - No information will be logged. This level is not recommended.
2. FATAL - This level identifies that the server stopped running.

3. ERROR - This level identifies something unexpected that happened, which may have put the server in a bad state. The following situations that could create server errors include: database is down (SQL exceptions) and database exceptions.
4. WARN - This level identifies situations to which you need to pay attention and perhaps make changes. Typical warnings include resources (for example, database connection pools) are low.
5. INFO - This level identifies lower priority issues that are not yet issues but that may become issues if not addressed.
6. DEBUG or TRACE - These levels are used primarily for development purposes to help assess code execution.
7. ALL - This level provides the most information, as all activities are logged, from TRACE to FATAL. Do not use this level unless absolutely necessary for debugging. It causes the *drm.log* file to become very large, very quickly.

Configuring error logging for drm.log

1. Using a text editor, such as Notepad, open the `log4j.properties` file, which is located in `/avaya/SAL/CRS/config`, by default.
2. Set the levels you want for debugging your server. The levels are: NONE, FATAL, ERROR, WARN, INFO, DEBUG, TRACE, and ALL.

   The log4j.properties file contains instructions for configuring the settings, as shown in the following excerpt from this file (the lines shown in red are explained after this listing):

```
## ########################################################
## Define the base log level for all aspects not overridden with
## logger-specific settings below. Also, specify the appenders to
## use, which determine where log messages are delivered.
##
## The available log levels, from least verbose to most, are:
## NONE, FATAL, ERROR, WARN, INFO, DEBUG, TRACE, ALL

log4j.rootLogger=INFO, stdout, troubleshooterlog

## ########################################################
## Define an appender called "stdout" which writes log messages to the
## console.

log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%-5p %d [%c{1}]: %m%n

## ########################################################
## Define the base log level for all aspects not overridden with
## logger-specific settings below. Also, specify the appenders to
## use, which determine where log messages are delivered.
##
## The available log levels, from least verbose to most, are:
## NONE, FATAL, ERROR, WARN, INFO, DEBUG, TRACE, ALL

log4j.rootLogger=INFO, drmlog

## ########################################################
## Define an appender called "stdout" which writes log messages to the
## console.
```

```
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%-5p %d [%c{1}]: %m%n

## ############################################################
## Define an appender called "drmlog", which outputs log messages to a
## file, rolling over to a new file when it gets too big.
##
## To use this appender, either replace "stdout" in the first line of
## the file with "drmlog", or add ", drmlog" to the end of the line,
## like so:
## log4j.rootLogger=WARN, drmlog (only log to the file)
## OR
## log4j.rootLogger=WARN, stdout, drmlog (log to file and console)

log4j.appender.drmlog=org.apache.log4j.RollingFileAppender
log4j.appender.drmlog.layout=org.apache.log4j.PatternLayout
log4j.appender.drmlog.layout.ConversionPattern=%-5p %d [%c{1}]: %m%n
log4j.appender.drmlog.file=drm.log
log4j.appender.drmlog.maxFileSize=2MB
log4j.appender.drmlog.maxBackupIndex=10
```

In this excerpt from `log4j.properties`, the logging settings are as follows:

- The default logging is at the INFO level.
- The `drmlog` file is defined as a file called drm.log (then renamed to `nodeName.out`) with a maximum file size of 2 MB and a retention of 10 previous versions (total is last 20 MB of log messages).

The rest of this file is comprised of some predefined logging options which can be enabled and will be printed to the log file after the comments are removed. Additional entries can be made to this file, but entries should be made only when directed by an Avaya Support Engineer.

Important:

Setting drm.log to anything above INFO level can cause the file to become very big, very quickly, and with log rotation enabled, can mean you might miss the required error. It is recommended that you take these facts into consideration when deciding how to set the logging level.

3. Restart the server for the changes made in the `log4j.properties` file to take effect.

Unsolvable logging issues

If you find database or code issues that you cannot resolve on your own, contact Avaya Technical Support by creating a Footprints entry. Make sure to attach the <`nodeName`>`.out` file to the entry for review by Avaya Support personnel.

Web server logs

If your SAL system includes an installation of Apache as the Web server, you can review the Apache `error_log` file in the Apache `logs` directory. Apache sends all diagnostic information to this file, and uses it to record any errors that it encounters in processing requests. When viewing this file, ensure that the number of httpd processes has not reached the maximum allowed.

Resolving slow navigation issue

If it appears that navigation through the Applications has slowed down and the server performance has decreased, you should initiate a thread dump. To initiate a thread dump when the Concentrator Remote Server is running in a DOS window and not as a service, press <CTRL> <BREAK>.

Resolving slow performance issue

While a user is navigating through the Applications pages, database performance issues can occur which will result in slower performance. If this happens, it may be the result of an SQL statement running in the system.

The following SQL statement can be used to isolate the SQL query that is currently running and causing the slowdown. This statement must be run with DBA rights.

Finding the currently running SQL

```
select c.first_load_time "TIME", a.status "STATUS",
substr(a.osuser, 1, 9) "OSUSER",
substr(a.username, 1, 9) "USERNAME",
lpad(substr(to_char(a.sid), 1, 5), 5, ' ') "SID",
lpad(substr(to_char(a.serial#), 1, 5), 5, ' ') "SERIAL",
lpad(substr(to_char(b.piece), 1, 2), 2, ' '), b.sql_text
from v$session a, v$sqltext b, v$sqlarea c
where a.sql_address = b.address and
a.sql_hash_value = b.hash_value and
a.username <> 'SYS' and
c.address = a.sql_address and
b.piece < 100
order by 1 asc, 3 asc, 4 asc, 5 asc, 6 asc, 7 asc;
```

Using diagnostic scripts to troubleshoot

The following scripts are provided for use by the DBA as another means of troubleshooting server and database problems.

```
prompt '*** Actively running SQL ***'
break on sid skip 1 on username
column sid format 999
column username format a10
SELECT c.first_load_time "LOAD TIME", a.sid, a.serial#,
a.username, b.sql_text
   FROM v$session a,v$sqltext b, v$sqlarea c
   WHERE a.username is not null
   AND c.address = a.sql_address
   AND a.username != 'SYSTEM'
   AND a.username != 'SYS'
   AND a.osuser != ' '
   AND a.osuser != 'slux002'
   AND a.status = 'ACTIVE'
   AND a.sql_address = b.address
   ORDER BY 1, 2, b.piece;

prompt '*** Long running SQL ***'

SELECT a.time_remaining, a.elapsed_seconds, b.sql_text, b.piece
   FROM v$session_longops a, v$sqltext b
   WHERE a.time_remaining > 0
```

```
   AND a.sql_hash_value = b.hash_value
   ORDER BY b.hash_value, b.piece ASC;

prompt '*** Top 10 most frequently reparsed SQL statements ***'

column sql_text format a40 word_wrapped
column parse_calls format 999,999,999
column executions format 999,999,999
SELECT *
   FROM (SELECT sql_text, parse_calls, executions, address, hash_value
   FROM v$sqlarea
   ORDER BY parse_calls desc)
   WHERE rownum < 10
   AND parse_calls > 0
   AND (executions / parse_calls) > .5
   AND sql_text not like '%$%';

prompt '*** Determine if the sort area size is appropriate ***'
SELECT (s1.value + s2.value) "Total Sorts",
s1.value "Memory Sorts",
s2.value "Disk Sorts",
s1.value / (s1.value + s2.value) "Memory to Disk Sort
Ratio",
(case when (s1.value / (s1.value + s2.value)) > .8
then 'SORT_AREA_SIZE OK'
else 'Increase SORT_AREA_SIZE' end) as "Message"
FROM v$sysstat s1, v$sysstat s2
WHERE s1.name = 'sorts (memory)'
AND s2.name = 'sorts (disk)';

prompt '*** Open Cursors ***'

SELECT max(a.value) as highest_open_cur, p.value as max_open_cur
   FROM v$sesstat a, v$statname b, v$parameter p
   WHERE a.statistic# = b.statistic#
   AND b.name = 'opened cursors current'
   AND p.name= 'open_cursors'
   GROUP BY p.value;

prompt '*** Used pool ***'

select sum(bytes) "Used Pool" from sys.v_$sgastat where
POOL = 'd pool' and name != 'free memory';

prompt '*** Free memory ***'
select pool, name, bytes from sys.v_$sgastat where name = 'free
memory';
```

Notifying server problems

The Concentrator Remote Server provides the ability to send notification e-mails should an error occur in the system. You can configure support for notifications in the server's properties.

To configure support for server notifications

1. Locate the `DRMConfig.properties` file located in the config subdirectory of your SAL installation (`..avaya/SAL/CRS/config`).
2. Search the file for the following entries and provide values as required:
   - `.. com.axeda.drm.administrator.email=`*`user@server.com`*

This property identifies the e-mail address to which notifications will be sent. Replace `user@server.com` with the e-mail address of your server's administrator. The e-mail address will be used in the To and From fields in the e-mail message.

- `.. com.axeda.drm.server.name=`*`SAL Server`*

  This property identifies the name of this Concentrator Remote Server. This name will be sent in the e-mail. This name is useful, especially if should there is more than one server being administered. Replace `SAL Server` with the server name.

- `.. com.axeda.drm.email.server=`*`mailserver.server.com`*

  This property identifies the mail server which can relay from the Concentrator Remote Server. This value is useful also when sending device notifications to people monitoring devices in the application. Replace `mailserver.server.com` with the address of your the e-mail server that your Concentrator Remote Server needs to use for sending e-mail messages.

3. Save the file.

For details about configuring support for notifications in the `DRMConfig.properties` file, see Appendix C: Editing the DRMConfig.properties File.

Important:

The default settings for two properties in the software-resources.properties file, `email.error.from` and `email.finished.from`, need to be modified if your users want to send e-mail notifications about software package deployments to *anonymous* e-mail addresses (that is, those addresses not defined in the Concentrator Remote Server directory service). By default, these two properties are set as `AxedaServiceLink`. You should change these to valid e-mail addresses.

Making properties visible by editing DRMConfigInfo.properties

The DRMConfigInfo.properties file contains configuration information from multiple sources, including the DRMConfig.properties file.In addition, it specifies whether the configuration information is visible from the Administration application.

If a parameter from the DRMConfig.properties file that you want to be able to see quickly is not visible in the Administration application, you can make it visible by copying the syntax of an existing parameter in this file and then changing the parameter name and entering its current setting in place of the information you copied.

See the online help for the application for an explanation of the parameters as they appear in the table. See Appendix C: Editing the DRMConfig.properties File for details about the DRMConfig.properties file.

Troubleshooting after reinstalling SAL system components

Problems with database searches

Problem 1: Search by device group name takes longer than by product family

If you have a device group with 10,000 devices in it from the same product family, and you run a search for all the devices by the product family name, the search returns results within 15 seconds. However, if you search for all the devices by the device group name, the search takes over 2 minutes to load the results.

Actions: Set the maximum results size to a smaller number (for example, 250 instead of 10,000). On a regular basis, analyze the tables in the database.

Problem 2: Search by admin user faster than by nonadmin user

Create a product family with 10,000 devices. Log in as the administrator and search for that product family from the Service application. The results return in 15 to 20 seconds. However, if you log in as a nonadministrative user and run the same search, the results take 3 minutes to return.

Actions: Make sure that the nonadministrative user has permission to see the product family. On a regular basis, analyze the tables in the database.

Customizing applications

You may want to customize the Web-based SAL applications by creating your own JSPs or translating the *.properties files. The applications are shipped as WAR files and then extracted during the installation process. You do not need to expand any WAR files before customizing the applications.

To customize the applications:

1. Add your customized files to the appropriate directories:

   1a. Add custom JSPs

   1b. Add translated *.properties files for JSPs

2. Restart the Secure Access Concentrator Remote Server

The Concentrator Remote Server automatically makes the necessary changes to the SAVED_DISPLAY table in the Concentrator Remote Server database. Should your Database Administrator need to check or edit the table, see the *System Database Reference Guide* or the installation guide for your version of the Oracle software.

The rest of this section describes each of these steps in detail.

1a. Add custom JSPs

Store your custom JSPs in the appropriate folder for the application to which you want to add them. If you used *.properties files to support the JSPs (for all text strings in your JSP), you also need to add them to the appropriate directory. Step 1c explains the location of the *.properties files in the Application directories.

1b. Add translated *.properties files for JSPs

If you have translated the help files for the application, you can create a folder for the translated files (language) and add the help files to the help.war in the servicelink.ear, installed to the following location: `<JBoss_Home>/server/<Secure_Access Link_server>/deploy/servicelink.ear`. The en subdirectory under help contains the English version of the help. Use the lettered ISO code for the language as the folder name. For example, for French (France), you would use fr, and for Canadian French, you would use frca.

1. Locate the subdirectories and English versions of the *.properties files, and copy the translated *.properties files to those locations. The files in the following table are all located in subdirectories of the Applications under your Web Application Server installation directory: `<JBoss_Home>/server/<SecureAccessLink_server>/deploy/servicelink.ear/drm.war`.

   Note:

   For brevity in the following table, the extension .properties has been omitted.

Table 10-5 Locations of *.properties files

In Subdirectory	Copy translated versions of
In the drm.war of servicelink.ear (*<JBoss_Home>/server/<SecureAccessLink_server>/deploy/servicelink.ear/drm.war)*	
.../aagweb/classes	aag
.../WEB-INF/classes/com/axeda/drm/resources/data	date_ranges encodings gateway product family modules mru_key parameter_type privileges report_names resource_types scm_intervals script_results tasks time_units
.../WEB-INF/classes/com/axeda/drm/resources/images	chart data_item display
.../WEB-INF/classes/com/axeda/drm/rules	messages

In Subdirectory	Copy translated versions of
.../WEB-INF/classes/com/axeda/drm/services/usage	DateIntervalResources GroupByResources ThresholdTypes UsageColumnResourcess
.../WEB-INF/classes/com/axeda/drm/soap	messages
In the following subdirectories of *<JBoss_Home>/server/<SecureAccessLink_server>/deploy/servicelink.ear/drm.war/WEB-INF/classes/com/axeda/drm/webapp*	
../access	JspResources
../admin	JspResources
../common	JspResources
../common/modules	JspResources
../contact	JspResources
../dashboard	JspResources
../dataexport	JspResources
../device	JspResources
../error	JspResources
../home	JspResources
../includes	JspResources
./report	JspResources
./resources	application errors waag
../rule	JspResources
../scm	JspResources
../scripts	JspResources
.../service	JspResources
../service/device/details	ShowRemoteSessionResources
../service/device/details/remot	RemoteDescriptionFormResources
../snapshot	JspResources
../snapshot/viewer	SetFilterFormResources

In Subdirectory	Copy translated versions of
../templates	JspResources
../text/logging	JspResources
../ui	JspResources
../usage	JspResources

2. In the `(<JBoss_Home>/server/<SecureAccessLink_server>/deploy/servicelink.ear/ drm.war/WEB-INF/classes/com/axeda/drm/servlet/remote)` copy in the translated version of JspResources.properties.

Restart the Secure Access Concentrator Remote Server

1. If the server is still running, go to the system console window where you started the server, and stop the server.

   If the server is not running, open a command shell.

2. If necessary, change to the `<JBoss_Home>/bin` subdirectory of your Web Application Server directory.
3. Type `secureaccesslinkrun.sh` to start the Secure Access Concentrator Remote Server. (Start the JBoss server separately.)

If you are adding custom JSPs or translated *.properties (and help) files, you are done.

Behaviors to watch out for

Using the Back button of your browser can cause problems when you are using the Applications. For best results, do *not* use the standard browser buttons to navigate the Applications. Use the navigation tools provided in the applications themselves.

Appendix A: Preinstallation checklist

This checklist summarizes the information you require before you start the installation process. Fill in the values where blank, especially the Policy Server items that cannot be configured after installation.

Table 1: Preinstallation information checklist

Concentrator Remote Server item	Value (examples)	Installer default value	Configurable after installation	Value
Java Path	/home/weblogic/bea/jdk150_10/bin/java	<Value of JAVA_HOME environment variable>	NO	
Install Location	/home/weblogic/servicelink	/opt/Avaya/SAL/CRS	NO	
Cognos report server URL	http://***dtxaxe01*** (change for correct short hostname)	http://localhost	YES	
Cognos configuration				
Cognos Report Server URL				
Cognos Web server listening port	443	80	YES	
Default Cognos Web application port	9300	9300	YES	
JBoss configuration				
JBoss Home Directory	/home/weblogic/bea	/usr/local/bea	NO	
Avaya Secure Access Remote Server server name		SecureAccessLink	NO	
JBoss Server IP Address			YES	
JBoss Server Listening Port			NO	
Keystore Configuration				
Identity Keystore file location			YES	
Identity Keystore Passphrase			YES	
Keystore Private Key Passphrase			YES	
Alias of Keystore Private Key			YES	

Concentrator Remote Server item	Value (examples)	Installer default value	Configurable after installation	Value
Identity Keystore Private Key Passphrase			YES	
Trust Keystore File Location				
Trust Keystore Passphrase				
Listening Port used for SSL connections	***7443***		YES	
CRL/OCSP Setup				
CRL File Location			YES	
OCSP URL			YES	
OCSP Certificate file location			YES	
OCSP Certificate Authority file location			YES	
OCSP Truststore file location			YES	
OCSP Truststore Passphrase			YES	
Check CRL or OCSP first	***OCSP***		YES	
Database configuration				
Database Host Name	***dtxdb02*** (change for correct short hostname)	server.avaya.com	YES	
Database SID	***D4AXE01*** (change for correct SID)		YES	
Database User Name	slink		YES	
Database User Password	*<DB Schema Password>*		YES	
Stage schema name			YES	
SAL configuration				
SMTP Server Address	mailhost		YES	
Admin e-mail	*<leave blank>*		YES	
Software Management server hostname	***dtxaxe01.dal.avaya.com*** (change for correct long FQDN)	server.avaya.com	YES	
Software Management Listening Port	80	7002	YES	

Concentrator Remote Server item	Value (examples)	Installer default value	Configurable after installation	Value
URL exclude list	***.avaya.com, *.domain.com**	*.avaya.com	YES	
Directory server configuration				
Host name for the Directory Server	dvasun12.dev.esp.avaya.com	server.avaya.com	YES	
Listening Port for the Directory Server	389	389	YES	
Directory Server Principal DN	Cn=DRMProxy,ou=special users,dc=Avaya,dc=com	Uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot	YES	
Principal Password	<LDAP Password>		YES	
User Base DN	ou=People,dc=Avaya,dc=com	ou=People,dc=avaya,dc=com	YES	
Group Base DN	ou=axeda,ou=Groups,dc=avaya,dc=com	ou=Groups,dc=avaya,dc=com	YES	
Username Attribute	uid	uid	YES	
Static Group Name Attribute	cn	cn	YES	
User from Name Filter	(&amp ;(uid=%g)(objectclass=groupofUniqueNames))(&amp ;(cn=%g)(objectclass=groupOfURLs)))	(|(&amp ;(cn=%g)(objectclass=groupofUniqueNames))(&amp ;(cn=%g)(objectclass=groupOfURLs)))	YES	
Username for LDAP Admin			YES	
LDAP Admin Password			YES	
Radius configuration (optional)				
RADIUS Host Name			YES	
RADIUS Authentication Port			YES	
RADIUS Accounting Port			YES	
RADIUS Shared Secret			YES	
Socket Timeout (milliseconds)			YES	
Maximum Number of Retries			YES	
LDAP Usergroup for RADIUS Users			YES	

Appendix B: Concentrator Remote Server files

This appendix provides details about the directories and files that make up the Concentrator Remote Server installation in the following sections:

Directory structure

The bin directory

The config directory

The ddl directory

The lib directory

The scm directory

WEB-INF in /servicelink.ear/drm.war/

The Uninstall Concentrator Remote Server directory

Files in the JBoss installation directory

Setting up logging

Directory structure

The installation directory for the SAL system software (called `avaya/SAL/CRS`, by default) should contain the following main subdirectories: `bin`, `config`, `ddl`, `lib`, `scm`, `sessionlogs`, and `Uninstall Avaya Secure Access Site Server`. Most of these main subdirectories contains one or more subdirectories.

The bin directory

Provides the command line script, `serverVersion`, that you can run to obtain the Concentrator Remote Server version. For instructions on using this script, see Determining the Concentrator Remote Server version.

The config directory

The config directory contains subdirectories whose contents support the Applications. Be very careful while editing any of these files. If you do not edit them in a pure text editor and save as a pure text file, your system may not run. This directory also contains the following XML configuration files and properties files for the Secure Access Concentrator Remote Server:

- **agent_codes.properties** - This file contains properties used to generate SOAP messages sent by the Concentrator Remote Server. These properties are separated into this file for purposes of translation. Some of these messages are explained in Agent-generated Package Status Codes.
- **axle-config.xml** - A configuration file for the rules interpreter of the Usage application (called XLE). This file is used to define new functions in AXLE that are needed to manipulate usage data.
- **custom-actions.xml**, **custom-rules.xml**, and **custom-startup.xml** - These files are for developers to define for the system any custom actions, rules, or startup tasks that they have implemented using the SAL SDK. The content of these files explain what to do.
- **CustomConfig.properties** - Contains any custom build information for the Secure Access Concentrator Remote Server. The information displayed in this file is viewable, by default, through the System Configuration page of the Administration application.
- **CustomConfigInfo.properties** - A copy of CustomConfig.properties that the Administration application uses to determine whether or not the properties are visible on the System Configuration page. To edit the properties, you must use a text editor to open and modify the CustomConfigInfo.properties file.
- **DRMConfig.properties** - The main configuration file for the Secure Access Concentrator Remote Server. For details on DRMConfig.properties, see Appendix C: Editing the DRMConfig.properties File.

- **DRMConfigInfo.properties** - A copy of DRMConfig.properties that the Administration application uses to determine whether or not the properties are visible on the System Configuration page. To edit the properties, you must use a text editor to open and modify the *DRMConfigInfo.properties* file.
- **kagi.properties** - This cryptic-looking file contains the information needed by the Blowfish algorithm for encrypting messages (data updates, e-mail messages, alarms, and other events) between the Secure Access Concentrator Remote Server and the agents sending data (Connector, Gateway). If you are using SSL encryption, you do not need this file.
- **log4j.properties** - A file for setting up the logging for the Concentrator Remote Server and the Applications. For more information and a listing of this file, see Setting up logging.
- **multi-mapper.xml** - A mapping file for setting up multiple schedule rules.
- **service-hierarchy-choices.xml** - An XML configuration file that specifies the hierarchy for browsing product family and device information in the dashboard of the Service application. This file allows you to customize the dashboard.
- **software-resources.properties** - This file contains properties used to generate e-mail messages sent by the SAL System. These properties are separated into this file for purposes of translation.

  Important:

  The default settings for two properties in the software-resources.properties file, *email.error.from* and *email.finished.from*, need to be modified if your users want to send e-mail notifications about software package deployments to *anonymous* e-mail addresses (that is, those addresses not defined in the Concentrator Remote Server directory service).
- **startup.xml** - A configuration file for the Scheduler.

To make the standard reports available, your server administrator needs to load the SAL Report Pack into the server. see Chapter 6: Installing and Configuring the Reporting Software for complete information.

Listing for startup.xml

Located in the *config* subdirectory of your SAL installation (`/avaya/SAL/CRS/config/`), this file sets parameters for the Scheduler, including how often to synchronize user group information with the directory server, how often to check for missing devices, and how long to retain files. This listing is provided in case you are directed to make changes by Hot Fix release notes or Avaya Technical Support.

startup.xml listing

```
<startup>
  <instance class-name="com.axeda.drm.services.users.SynchronizeUsersTask">
     <synchronize-users-task>
        <name>Synchronize Users with User Store</name>
        <schedule>period 15 minute</schedule>
        <pooled>true</pooled>
     </synchronize-users-task>
  </instance>
<instance class-name="com.axeda.drm.services.maintenance.MaintenanceHistoryDataTask">
  <maintenance-history-task>
     <name>Copy Current Maintenance data to Maintenance history tables</name>
     <schedule>period 12 hour</schedule>
```

startup.xml listing (continued)

```
      <pooled>true</pooled>
      <separate-thread>true</separate-thread>
  </maintenance-history-task>
</instance>
<instance class-name="com.axeda.drm.services.usergroups.SynchronizeUserGroupsTask">
  <synchronize-user-groups-task>
      <name>Synchronize User Groups with User Store</name>
      <schedule>period 15 minute</schedule>
      <pooled>true</pooled>
  </synchronize-user-groups-task>
</instance>
<instance class-name="com.axeda.drm.services.trigger.MissingDevicesTask">
  <missing-devices-task>
      <name>Find missing devices</name>
      <schedule>period 5 minute</schedule>
      <pooled>true</pooled>
      <separate-thread>true</separate-thread>
      <delay-period>0</delay-period>
  </missing-devices-task>
</instance>
<instance class-name="com.axeda.drm.services.agent.status.StatusManagerTask">
  <status-manager-task>
      <name>Handle background status updates</name>
      <schedule>period 5 minute</schedule>
      <pooled>true</pooled>
  </status-manager-task>
</instance>
<instance class-name="com.axeda.drm.services.archive.ArchiveTask">
  <archive-task>
      <name>Archive</name>
      <schedule>start 2004-01-01-00:00:00 period 1 day</schedule>
      <pooled>true</pooled>
      <separate-thread>true</separate-thread>
  </archive-task>
</instance>
<instance class-name="com.axeda.drm.services.notification.EscalateNotificationsTask">
  <escalate-notifications-task>
      <name>Escalate unacknowledged notifications</name>
      <schedule>period 5 minute</schedule>
      <pooled>true</pooled>
  </escalate-notifications-task>
</instance>
<instance class-name="com.axeda.drm.datamart.DatamartRefreshTask">
  <datamart-refresh-task>
      <name>DataMart refresh</name>
      <schedule>period 30 minute</schedule>
      <pooled>true</pooled>
      <separate-thread>true</separate-thread>
  </datamart-refresh-task>
</instance>
<instance class-name="com.axeda.drm.services.vendor.SessionMonitorTask">
  <vendor-access-session-monitor-task>
      <name>Monitor Partner Access Session Expiration State</name>
      <schedule>period 1 minute</schedule>
      <pooled>true</pooled>
  </vendor-access-session-monitor-task>
</instance>
<!-- This task allows periodic cleanup of files and directories. It is a
    sub-class of PeriodicCleanupTask.
    KEEP-INTERVAL: The number of seconds to keep files around before deleting
       them. This value is subtracted from the current time to
       determine the date/time from which to keep files. Common values are:

       1 minute: 60
       1 hour: 3600
       1 day: 86400
       1 week: 604800
       1 month: 18144000
```

startup.xml listing (continued)

```
       1 year: 31536000

       Recommended value is 1 day.

    INCLUDE-FILESET: A semi-colon delimited list of directories or files that
        should be checked for files to be cleaned up. For example:
        D:/drm/scm/downloads/temp;D:/some-other/directory/path
    RECURSE: Whether or not to recurse subdirectories of directories
        pecified by INCLUDE-FILESET. true/false.
-->
<!--
  <instance class-name="com.axeda.drm.services.trigger.CleanupFilesTask">
     <cleanupfilestask>
         <name>Cleanup Files Task</name>
         <schedule>start 2004-03-27-00:00:00 period 1 day</schedule>
         <pooled>true</pooled>
         <separate-thread>true</separate-thread>
         <keep-interval>86400</keep-interval>
         <include-
fileset>C:/dev/drm38/drm/install/scm/downloads/temp2;C:/dev/drm38/drm/
install/scm/downloads/temp;</include-fileset>
         <recurse>true</recurse>
     </cleanupfilestask>
  </instance>-->
</startup>
```

The config/audit subdirectory

This subdirectory contains the *messages.properties* files, English version and those translated to other supported languages. The messages.properties file contains the display strings for audit messages in the SAL system. The file is located here to facilitate reporting.

The config/rules subdirectory

This subdirectory contains the templates for rules that you can configure in the Usage application. The templates are XML-based files that the application reads to present the conditions in the wizard for setting up Calculation Rules.

The ddl directory

This directory contains SQL scripts for use in setting up the table structure for the database and a new database user to work with the Oracle database for Concentrator Remote Server.

The `ddl` directory contains a subdirectory, `tablespaces`, which contains the following sample scripts for creating tablespaces:

- **create_tablespaces_production.sql** - To create tablespaces for a production environment.
- **create_tablespaces_development.sql** - To create tablespaces for a development environment.

  For details about editing these scripts and running them, see "Creating Tablespaces" in Chapter 6, "Configuring the Oracle Database."

The `ddl` directory also contains a subdirectory, `common`, which contains scripts that are used by the database migration scripts that are part of Service Pack releases and upgrade releases.

In addition, the `ddl` directory contains basic scripts and scripts that call the basic scripts. The following files contain the scripts that set up and initialize the database for the Concentrator Remote Server:

- **create_oracle_user.sql** - Sets up a new database user. This script must be run once to create the database user so that you can log in as that user and run the remaining scripts. For details about using this script, see "Creating the Database User" in Chapter 6, "Configuring the Oracle Database."
- **create_all_tables.sql** - Creates and initializes the table structure for the database. The script accomplishes this by running all of the following SQL scripts stored in the `ddl` directory:
    - **create_online_tables.sql** - Creates the table structure for the device data in the database. This script calls many 'create' and 'initialize' scripts to first set up the tables (create) and then populate the tables with any required data (initialize).
    - **create_reporting_tables.sql** - Creates the table structure for case activity and devicestate reporting in the database. This script calls the following scripts: `create_dimension_tables.sql` (creates dimension or fact tables and views to be used for reporting), `create_fact_tables.sql` (device states), and `initialize_reporting_tables.sql` (case activity).
    - **create_etl_tables.sql** - Creates the structure for the ETL (staging) tables in the database. This script creates tables (and indexes to the tables) and ETL procedures. The tables created by this script include device information, device state duration, device state transitions, and case activity.

In addition to the scripts used for creating and initializing table structures, the ddl directory also contains scripts that clean up the database. You can use the `drop_all_tables.sql` script that cleans up all existing table structures by calling a number of 'drop' scripts.

The lib directory

This directory contains all the base JAR files for the Applications.

The scm directory

This directory identifies directory locations for files uploaded to and from the server as a result of software management packages or Transport operations. Following types of files are stored in this directory:

- *downloads* subdirectory package files to be included as part of a package should be stored in this directory. The DRMConfig.properties file *(com.axeda.drm.scm* properties) needs to be updated with this directory location if it is changed after installation.

- *export* subdirectory files to be exported to devices via Transport - Export sessions are stored in this directory. The DRMConfig.properties file *(com.axeda.drm.transportservicelink.export* property) needs to be updated with this directory location if it is changed after installation.
- *import* subdirectory files imported from devices via Transport - Import sessions are stored in this directory. The DRMConfig.properties file *(com.axeda.drm.transportservicelink.import* property) needs to be updated with this directory location if it is changed after installation.
- *uploads* subdirectory files uploaded from devices as part of package operations are stored in this directory. The DRMConfig.properties file *(com.axeda.drm.scm* properties) needs to be updated with this directory location if it is changed after installation.

WEB-INF in /servicelink.ear/drm.war/

The *WEB-INF* directory contains important configuration files for running the Applications through the JBoss Server. These files include *web.xml,* and other XML configuration files for the applications.

The The web.xml configuration file contains the parameter that controls the length of time that the system allows an inactive session to remain open before it ends the session. This parameter is `<sessiontimeout>`. Its default setting is 20 minutes. The listing of this file in this section shows this parameter `in this font`.

The web.xml configuration file

web.xml listing

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<web-app id="WebApp" version="2.4" xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/webapp_
2_4.xsd">

  <!-- Filters -->
  <filter>
     <filter-name>InitializationFilter</filter-name>
     <filter-class>com.axeda.drm.servlet.InitializationFilter</filter-class>
  </filter>

  <filter>
     <filter-name>CheckUriAccessFilter</filter-name>
     <filter-class>com.axeda.drm.servlet.CheckUriAccessFilter</filter-class>
  </filter>

  <filter>
     <filter-name>UsageFilter</filter-name>
     <filter-class>com.axeda.drm.webapp.usage.UsageFilter</filter-class>
  </filter>

  <filter>
     <filter-name>compressionFilter</filter-name>
     <filter-class>com.axeda.drm.servlet.CompressionFilter</filter-class>
  </filter>
```

web.xml listing (continued)

```
  <filter>
       <filter-name>StaticFileCacheControlFilter</filter-name>
       <filter-class>com.axeda.drm.servlet.StaticFileCacheControlFilter</filter-class>
  </filter>

  <filter-mapping>
       <filter-name>StaticFileCacheControlFilter</filter-name>
       <url-pattern>*.js</url-pattern>
  </filter-mapping>

  <!-- The InitializationFilter mappings need to be first to ensure -->
  <!-- that the Context is in place before other filters execute -->
  <filter-mapping>
       <filter-name>InitializationFilter</filter-name>
       <url-pattern>/actions/*</url-pattern>
  </filter-mapping>

  <filter-mapping>
       <filter-name>InitializationFilter</filter-name>
       <url-pattern>/scripts/*</url-pattern>
  </filter-mapping>

  <filter-mapping>
       <filter-name>InitializationFilter</filter-name>
       <url-pattern>/waagServlet/*</url-pattern>
  </filter-mapping>

  <filter-mapping>
       <filter-name>InitializationFilter</filter-name>
       <url-pattern>//waagServlet/*</url-pattern>
  </filter-mapping>

  <filter-mapping>
       <filter-name>CheckUriAccessFilter</filter-name>
       <url-pattern>/actions/*</url-pattern>
  </filter-mapping>

  <filter-mapping>
       <filter-name>UsageFilter</filter-name>
       <url-pattern>/actions/usage/*</url-pattern>
  </filter-mapping>

  <filter-mapping>
       <filter-name>compressionFilter</filter-name>
       <url-pattern>*.jsp</url-pattern>
  </filter-mapping>

  <!-- SCM File Viewer servlet -->
  <servlet id="Servlet_fileviewer">
       <servlet-name>fileviewer</servlet-name>
       <servlet-
class>com.axeda.drm.services.scm.fileviewer.FileViewerServlet</servlet-class>
  </servlet>
```

web.xml listing (continued)

```
  <!-- The WAAG servlet -->
  <servlet id="Servlet_waagServlet">
       <servlet-name>waagServlet</servlet-name>
       <servlet-class>com.axeda.drm.waag.servlets.waagServlet</servlet-class>
  </servlet>

  <!-- The ShowRemoteSession servlet -->
  <servlet id="Servlet_ShowRemoteSession">
       <servlet-name>ShowRemoteSession</servlet-name>
       <servlet-
class>com.axeda.drm.webapp.service.device.details.ShowRemoteSession</servletclass>
  </servlet>

  <!-- The RunReportServlet servlet -->
  <servlet id="Servlet_RunReport">
       <servlet-name>RunReportServlet</servlet-name>
       <servlet-class>com.axeda.drm.servlet.RunReportServlet</servlet-class>
  </servlet>

  <!-- The RunCognosReportServlet servlet -->
  <servlet id="Servlet_RunCognosReport">
       <servlet-name>RunCognosReportServlet</servlet-name>
       <servlet-class>com.axeda.drm.servlet.RunCognosReportServlet</servlet-class>
  </servlet>

  <!-- The RunCognosChartServlet servlet -->
  <servlet id="Servlet_RunCognosUsage">
       <servlet-name>RunCognosChartServlet</servlet-name>
       <servlet-class>com.axeda.drm.servlet.RunCognosChartServlet</servlet-class>
  </servlet>

  <!-- The RefreshAlertsServlet servlet -->
  <servlet id="Servlet_RefreshAlerts">
       <servlet-name>RefreshAlertsServlet</servlet-name>
       <servlet-class>com.axeda.drm.servlet.RefreshAlertsServlet</servlet-class>
  </servlet>

  <!-- The GetRandomPasswords servlet -->
  <servlet id="Servlet_RandomTokens">
       <servlet-name>GenerateRandomTokens</servlet-name>
       <servlet-class>com.axeda.drm.servlet.GenerateRandomTokens</servlet-class>
  </servlet>

  <!-- The File upload servlet -->
  <servlet id="Servlet_FileUpload">
       <servlet-name>fileUpload</servlet-name>
       <servlet-class>com.axeda.drm.servlet.FileUploadServlet</servlet-class>
  </servlet>
```

web.xml listing (continued)

```
  <!-- The Struts servlet -->
  <servlet id="Servlet_action">
       <servlet-name>action</servlet-name>
       <servlet-class>org.apache.struts.action.ActionServlet</servlet-class>
       <init-param>
          <param-name>config</param-name>
          <param-value>/WEB-INF/struts-config.xml</param-value>
       </init-param>
       <init-param>
          <param-name>debug</param-name>
          <param-value>0</param-value>
       </init-param>
       <init-param>
          <param-name>detail</param-name>
          <param-value>0</param-value>
       </init-param>
       <init-param>
          <param-name>validate</param-name>
          <param-value>true</param-value>
       </init-param>
       <load-on-startup>2</load-on-startup>
  </servlet>

  <servlet id="Servlet_startup">
       <servlet-name>startup</servlet-name>
       <servlet-class>com.axeda.drm.startup.StartupServlet</servlet-class>
       <load-on-startup>3</load-on-startup>
  </servlet>

  <!-- beginning for Site Preparation Utility servlets -->
  <servlet>
       <servlet-name>appInit</servlet-name>
       <servlet-class>com.axeda.servlets.AppInitServlet</servlet-class>
       <load-on-startup>1</load-on-startup>
  </servlet>

  <!-- The File upload servlet -->
  <servlet id="Servlet_checkdatabase">
       <servlet-name>checkDataBase</servlet-name>
       <servlet-class>com.axeda.servlets.CheckDataBaseServlet</servlet-class>
  </servlet>

  <servlet>
       <servlet-name>getSupportedMimeTypesList</servlet-name>
       <servlet-class>com.axeda.servlets.SupportedMimeTypesListServlet</servlet-class>
  </servlet>

<servlet>
       <servlet-name>getMimeType</servlet-name>
       <servlet-class>com.axeda.servlets.SendMimeTypesServlet</servlet-class>
</servlet>
```

web.xml listing (continued)

```
<servlet>
     <servlet-name>enterpriseServerListServlet</servlet-name>
     <servlet-class>com.axeda.servlets.EnterpriseServerListServlet</servlet-class>
</servlet>

<servlet-mapping>
     <servlet-name>getSupportedMimeTypesList</servlet-name>
     <url-pattern>/getSupportedMimeTypesList</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>getMimeType</servlet-name>
     <url-pattern>/getMimeType</url-pattern>
</servlet-mapping>
<servlet-mapping>
     <servlet-name>enterpriseServerListServlet</servlet-name>
     <url-pattern>/enterpriseServerListServlet</url-pattern>
</servlet-mapping>

<servlet>
     <servlet-name>SitePrepForwardServlet</servlet-name>
     <jsp-file>/sitepreputility/siteprepappletlaunch.jsp</jsp-file>
</servlet>
<servlet-mapping>
     <servlet-name>SitePrepForwardServlet</servlet-name>
     <url-pattern>/sitepreparationutility</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>checkDataBase</servlet-name>
     <url-pattern>/checkDataBase</url-pattern>
</servlet-mapping>

<!-- end of Site Preparation Utility servlets -->

<servlet-mapping>
     <servlet-name>RunReportServlet</servlet-name>
     <url-pattern>/run-report/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>RunCognosReportServlet</servlet-name>
     <url-pattern>/run-reports/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>RunCognosChartServlet</servlet-name>
     <url-pattern>/run-charts/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>RefreshAlertsServlet</servlet-name>
     <url-pattern>/refresh-alerts/*</url-pattern>
</servlet-mapping>
```

web.xml listing (continued)

```
<servlet-mapping>
     <servlet-name>GenerateRandomTokens</servlet-name>
     <url-pattern>/random-tokens/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>fileviewer</servlet-name>
     <url-pattern>/file-viewer/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>waagServlet</servlet-name>
     <url-pattern>/waagServlet</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>waagServlet</servlet-name>
     <url-pattern>//waagServlet</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>waagServlet</servlet-name>
     <url-pattern>/cgi-bin/aagweb.exe</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>ShowRemoteSession</servlet-name>
     <url-pattern>/service/device/details/showRemoteSession</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>fileUpload</servlet-name>
     <url-pattern>/applets/fileUpload/</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>startup</servlet-name>
     <url-pattern>/startup</url-pattern>
</servlet-mapping>

<servlet-mapping>
     <servlet-name>action</servlet-name>
     <url-pattern>/actions/*</url-pattern>
</servlet-mapping>

<session-config>
     <session-timeout>20</session-timeout>
</session-config>

<welcome-file-list>
     <welcome-file>index.html</welcome-file>
</welcome-file-list>
```

web.xml listing (continued)

```
  <error-page>
       <exception-type>com.axeda.drm.security.AccessDeniedException</exception-type>
       <location>/home/page_access_denied.jsp</location>
  </error-page>

  <error-page>

  <exception-type>java.lang.Throwable</exception-type>
       <location>/error/generic_error.jsp</location>
       </error-page>
  <error-page>

  <error-code>410</error-code>
       <location>/error/generic_error.jsp</location>
  </error-page>

  <error-page>
       <error-code>404</error-code>
       <location>/error/generic_error.jsp</location>
  </error-page>

  <error-page>
       <error-code>400</error-code>
       <location>/error/generic_error.jsp</location>
  </error-page>

  <jsp-config>
       <jsp-property-group>
          <url-pattern>*.jsp</url-pattern>
          <page-encoding>UTF-8</page-encoding>
       </jsp-property-group>
  </jsp-config>

  <resource-ref id="ResourceRef_DRMPool">
       <res-ref-name>ServiceLink Pool Reference</res-ref-name>
<!-- <res-type>javax.sql.DataSource</res-type> -->
       <res-type>java.lang.Object</res-type>
       <res-auth>Container</res-auth>
       <res-sharing-scope>Unshareable</res-sharing-scope>
  </resource-ref>

  <resource-ref id="ResourceRef_QueueFactory">
       <res-ref-name>ServiceLink QueueFactory Reference</res-ref-name>
       <res-type>java.lang.Object</res-type>
<!-- <res-auth>Container</res-auth> -->
       <res-auth>Application</res-auth>
       <res-sharing-scope>Unshareable</res-sharing-scope>
  </resource-ref>

  <resource-ref id="ResourceRef_TopicFactory">
       <res-ref-name>ServiceLink TopicFactory Reference</res-ref-name>
       <res-type>java.lang.Object</res-type>
       <res-auth>Application</res-auth>
       <res-sharing-scope>Unshareable</res-sharing-scope>
  </resource-ref>
```

web.xml listing (continued)

```
  <security-constraint>
       <display-name></display-name>
       <web-resource-collection>
          <web-resource-name>anything</web-resource-name>
          <url-pattern>/*</url-pattern>
          <http-method>GET</http-method>
          <http-method>PUT</http-method>
          <http-method>HEAD</http-method>
          <http-method>POST</http-method>
       </web-resource-collection>
       <auth-constraint>
          <role-name>ServiceLinkUsers</role-name>
       </auth-constraint>
  </security-constraint>

  <login-config>
       <auth-method>FORM</auth-method>
       <realm-name>Caching Realm for ServiceLink</realm-name>
       <form-login-config>
          <form-login-page>/home/login.jsp</form-login-page>
          <form-error-page>/home/login_error.jsp</form-error-page>
       </form-login-config>
  </login-config>

  <security-role>
       <description>ServiceLinkUsers</description>
       <role-name>ServiceLinkUsers</role-name>
  </security-role>
</web-app>
```

The Uninstall Concentrator Remote Server directory

Provides the program file for uninstalling the Concentrator Remote Server software.

Files in the JBoss installation directory

When you install the Concentrator Remote Server, a new server entry is created in the JBoss Home directory. The default name for the new SAL server entry is `SecureAccessLink`. Additional servers (that is, `all`, `default`, and `minimal`) are created as well. Although the `all` and `minimal` servers are not used, the `default` server IS used by the SAL installer. You can delete the `all` and `minimal` directories, but you need to keep the `default` directory.

The contents of the /bin directory are noteworthy to SAL administrators. See your JBoss Enterprise Application Platform documentation for complete information on the other JBoss directories.

The /bin directory

Provides the startup and shutdown scripts for the SAL server. The ***secureaccesslinkrun*** script starts the Enterprise and JBoss servers, and ***secureaccesslinkshutdown*** stops the servers.

When you install the Concentrator Remote Server, a new server entry is created in the JBoss Home directory. The default installation name is *SecureAccessLink*. Though three

additional servers, All, Default, and Minimal, are also created, SAL does not use these and you can delete them.

The /conf directory

Provides SAL configuration for JBoss, including login-config.xml (with LDAP settings), and jboss-log4j.xml (provides additional logging settings above the server), Log4j.properties file, and jndi properties for this server.

The /deploy directory

Contains the *servicelink.ear* (exploded or unexploded, depending on your server environment), in addition to many JBoss server files including the jmx-console. The Applications are deployed through the servicelink.ear. Any WARs to be deployed (for example, webservices.war) go in the servicelink.ear. Contains the SAL server deployments: drm, help, public, remote, rpc, and webservices.

server.xml

One important file to note in this directory is the server.xml.

This file includes information about what Web features to turn on when the server starts up, including the SSL configuration settings for JBoss. You are prompted to set up SSL communications during server installation, but if you need to modify SSL settings after installation, you can do so using this file. SSL settings for SAL will appear in the section "SSL/TLS Connector configuration using the admin devl guide keystore" (or similar name).

drm.war

The drm.war subdirectory contains the Applications for this server. Any changes to Applications, to Desktop or Access viewers, project displays, language translations, and so forth need to be made to the drm.war subdirectory in the servicelink.ear. All web.xml files for SAL are provided in this EAR.

The example below shows the contents of drm.war in servicelink.ear:

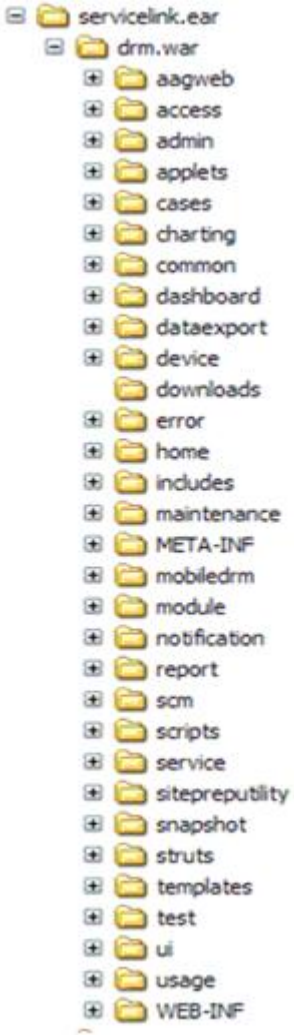


Figure B-5: Contents of drm.war in servicelink.ear

Setting up logging

To set up the logging to be done in the drm.log file, edit the `log4j.properties` file, which is located in the `config` subdirectory of your main Concentrator Remote Server installation directory. For example, by default, the file is located in `/avaya/SAL/CRS/config/`. The `log4j.properties` file contains instructions for configuring the settings, as shown in the following example of this file (the lines `in this font` are explained after this listing).

log4j.properties listing

```
## ############################################################
## Define the base log level for all aspects not overridden with
## logger-specific settings below. Also, specify the appenders to
## use, which determine where log messages are delivered.
##
## The available log levels, from least verbose to most, are:
## NONE, FATAL, ERROR, WARN, INFO, DEBUG, TRACE, ALL

log4j.rootLogger=INFO, stdout, troubleshooterlog

## ############################################################
## Define an appender called "stdout" which writes log messages to the
## console.

log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%-5p %d [%c{1}]: %m%n

## ############################################################
## Define the base log level for all aspects not overridden with
## logger-specific settings below. Also, specify the appenders to
## use, which determine where log messages are delivered.
##
## The available log levels, from least verbose to most, are:
## NONE, FATAL, ERROR, WARN, INFO, DEBUG, TRACE, ALL
log4j.rootLogger=INFO, drmlog

## ############################################################
## Define an appender called "stdout" which writes log messages to the
## console.

log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%-5p %d [%c{1}]: %m%n
```

***log4j.properties* listing (continued)**

```
## ############################################################
## Define an appender called "drmlog", which outputs log messages to a
## file, rolling over to a new file when it gets too big.
##
## To use this appender, either replace "stdout" in the first line of
## the file with "drmlog", or add ", drmlog" to the end of the line,
## like so:
## log4j.rootLogger=WARN, drmlog (only log to the file)
## OR
## log4j.rootLogger=WARN, stdout, drmlog (log to file and console)

log4j.appender.drmlog=org.apache.log4j.RollingFileAppender
log4j.appender.drmlog.layout=org.apache.log4j.PatternLayout
log4j.appender.drmlog.layout.ConversionPattern=%-5p %d [%c{1}]: %m%n
log4j.appender.drmlog.file=drm.log
log4j.appender.drmlog.maxFileSize=2MB
log4j.appender.drmlog.maxBackupIndex=10

## ############################################################
## Define an appender called "SYSLOG", which outputs log messages to a
## Unix-style Syslog server.
##
## log4j.appender.SYSLOG.SyslogHost=hostname_or_IP_address[:port_number_if_not_514]
#### Uncomment settings below to activate capability for logging audit messages to a
Syslog Server.

# log4j.appender.SYSLOG=org.apache.log4j.net.SyslogAppender
# log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
# log4j.appender.SYSLOG.layout.ConversionPattern=%d{ISO8601}: %m%n
# log4j.appender.SYSLOG.SyslogHost=localhost
# log4j.appender.SYSLOG.Facility=LOCAL0
# log4j.appender.SYSLOG.FacilityPrinting=false

## ############################################################
## Special Syslog Server logger
## log4j.logger.com.axeda.drm.SYSLOG=<severity_levels (e.g. INFO)>, <appender_names
(i.e. SYSLOG)>
##
## The following setting enables/disables the Syslog Server logger from sharing its
ancestor's
appenders.
##
## log4j.additivity.com.axeda.drm.SYSLOG=<true_or_false>
## NOTE: In production mode, the value of this property should always be set to false.
##
## Uncomment settings below to activate capability for logging audit messages to a
Syslog Server.

# log4j.logger.com.axeda.drm.SYSLOG=INFO, SYSLOG
# log4j.additivity.com.axeda.drm.SYSLOG=false

## ############################################################
```

***log4j.properties* listing (continued)**

```
## The Jakarta components used in ServiceLink have an unfortunate tendency ## to log
more verbosely than necessary. Here, we set their log level to
## ERROR regardless of what the rootLogger is configured as.

log4j.logger.org.apache.commons=ERROR
log4j.logger.org.apache.struts=ERROR

## Same goes for the shiftone classes used in testing.
log4j.logger.org.shiftone=ERROR

## The beehive log level set into Error Level regardless of what the
## rootLogger is configured as. (SCR:14192)
log4j.logger.org.apache.beehive=ERROR

## ################################################################
## From this point in the file, we list a number of useful log
## settings that can be used to investigate particular kinds of
## problems.
## Note that you can modify the log levels of the different categories
## on-the-fly (while the server is running) by using the URL
## http://YOURSERVER/drm/actions/test/logging/show (as an
## administrator). Changes you make using the web UI will NOT be
## persisted to this file.

## ################################################################
## Debugging database connection leaks/problems? Uncomment the
## following line.

# log4j.logger.com.axeda.common.jdbc.LimitedConnection=DEBUG

## ################################################################

## Debugging notifications? Uncomment the following lines.

# log4j.logger.com.axeda.drm.entity.action.NotificationAction=DEBUG
# log4j.logger.com.axeda.drm.services.notification=DEBUG
# log4j.logger.com.axeda.drm.util.Emailer=DEBUG
# log4j.logger.com.axeda.drm.common.formatting=DEBUG

## ################################################################
## Debugging rule execution? Uncomment the following lines.

# log4j.logger.com.axeda.drm.services.rules=DEBUG
# log4j.logger.com.axeda.drm.services.action=DEBUG
# log4j.logger.com.axeda.drm.entity.action=DEBUG
```

***log4j.properties* listing (continued)**

```
## ############################################################
## Debugging expression conditions? Uncomment the following lines.

# log4j.logger.com.axeda.common.expression=DEBUG
# log4j.logger.com.axeda.common.expression.Reader=WARN
# log4j.logger.com.axeda.common.expression.Environment=WARN
# log4j.logger.com.axeda.drm.usage.rules=DEBUG

## ############################################################
## Debugging usage? Uncomment the following lines.

# log4j.logger.com.axeda.drm.services.usage=DEBUG
# log4j.logger.com.axeda.drm.webapp.usage.configuration=DEBUG

## ############################################################
## Debugging action configuration? Uncomment the following lines.

# log4j.logger.com.axeda.drm.services.action=DEBUG
# log4j.logger.com.axeda.drm.entity.action=DEBUG
# log4j.logger.com.axeda.drm.taglib.action=DEBUG

## ############################################################
## Debugging security? Uncomment the following lines.

# log4j.logger.com.axeda.drm.security=DEBUG
# log4j.logger.com.axeda.drm.webapp.security.page=DEBUG
# log4j.logger.com.axeda.drm.servlet.CheckUriAccessFilter=DEBUG

## ############################################################
## Debugging scripts? Uncomment the following lines.

# log4j.logger.com.axeda.drm.services.script=DEBUG
# log4j.logger.com.axeda.drm.entity.script=DEBUG

## ############################################################
## Debugging charting? Uncomment the following lines.
# log4j.logger.com.axeda.drm.webapp.charting=DEBUG

## ############################################################
## Debugging eMessage? Uncomment the following lines.
# log4j.logger.com.axeda.drm.devcon.emessage.handlers=DEBUG
# log4j.logger.com.axeda.drm.services.agent.SchemaStatusMessageHandler=DEBUG
# log4j.logger.com.axeda.drm.services.agent.SchemasMessageHandler=DEBUG
# log4j.logger.com.axeda.drm.services.agent.TimerStatusMessageHandler=DEBUG

## ############################################################
## Debugging software? Uncomment the following lines.

# log4j.logger.com.axeda.drm.services.scm=DEBUG
# log4j.logger.com.axeda.drm.entity.scm=DEBUG
```

***log4j.properties* listing (continued)**

```
## ############################################################
## Debugging MaintenancePing? Uncomment the following lines.

# log4j.logger.com.axeda.drm.devcon.maintenanceping=DEBUG

## ############################################################
## Debugging DevconNotification? Uncomment the following lines.

# log4j.logger.com.axeda.drm.devcon.notification=DEBUG

## ############################################################
## Debugging parent server configuration?
## Uncomment the following lines.

# log4j.logger.com.axeda.drm.server.communication=DEBUG

## ############################################################
## Debugging missing/returned devices logic? Uncomment below.

# log4j.logger.com.axeda.drm.services.device.MissingStrategy=DEBUG
# log4j.logger.com.axeda.drm.services.trigger.MissingDevicesTask=DEBUG
##############################################################
```

In this example, the logging settings shown in red set the following parameters:

- The default logging is set at the INFO level
- The *drmlog* file is defined as a file called drm.log (then renamed to ***nodeName.out***) with a maximum file size of 2 MB and a retention of 10 previous versions (total is last 20 MB of log messages).

The rest of this file contains predefined logging options that can be enabled and will be printed to the log file after you remove the comments, save the file and restart the server. Additional entries can be made to this file, but those should be done only as directed by an Avaya Support Engineer.

Important:

Setting drm.log to anything above INFO level can cause the file to become very big, very quickly, and with log rotation enabled, this can mean you might miss the required error. Avaya recommends that you take these facts into consideration when deciding how to set the logging level.

For the changes to take effect, you must restart the server.

Syslog server settings

If you are using a Syslog server as another means of capturing audit information (that is, in addition to the JDBC Auditor), you need to define an appender called "SYSLOG," which outputs log messages to a Unix-style Syslog server. Also, you need to specify which information to dispatch to the Syslog server. By default, syslog support is commented out in the log4j.properties file. You will need to remove the comments from the applicable syslog properties and then configure them as needed for your use.

Additionally, in the *DRMConfig.properties* file, you need to define the Syslog auditor type for the server, and then specify the types of audit categories to dispatch (or send) to the auditors.

Adding the appender

In the log4j example shown, you see the following section:

```
## Define an appender called "SYSLOG", which outputs log messages to a
## Unix-style Syslog server.
##
## log4j.appender.SYSLOG.SyslogHost=hostname_or_IP_address[:port_number_if_not_514]
##
## Uncomment settings below to activate capability for logging audit messages to a
Syslog Server.

# log4j.appender.SYSLOG=org.apache.log4j.net.SyslogAppender
# log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
# log4j.appender.SYSLOG.layout.ConversionPattern=%d{ISO8601}: %m%n
# log4j.appender.SYSLOG.SyslogHost=localhost
# log4j.appender.SYSLOG.Facility=LOCAL0
# log4j.appender.SYSLOG.FacilityPrinting=false
```

You can leave these settings as shown or modify for the settings needed for your Syslog server setup. Ensure that the values of the settings `log4j.appender.SYSLOG.SyslogHost`, and `log4j.appender.SYSLOG.Facility` are set to the appropriate values for the running syslog server daemon.

If the UDP port for the running syslog server is 514 (the default UDP port number for Syslog servers), then ":514" may be left off of the value of the `log4j.appender.SYSLOG.SyslogHost` property.

Adding the Syslog auditor type

In the log4j example shown, you see the following section:

```
## Special Syslog Server logger
## log4j.logger.com.axeda.drm.SYSLOG=<severity_levels (e.g. INFO)>, <appender_names
## (i.e. SYSLOG)>
##
## The following setting enables/disables the Syslog Server logger from sharing its
## ancestor's appenders.
##
## log4j.additivity.com.axeda.drm.SYSLOG=<true_or_false>
## NOTE: In production mode, the value of this property should always be set to false.
```

```
##
## Uncomment settings below to activate capability for logging audit messages to a
## Syslog server.

# log4j.logger.com.axeda.drm.SYSLOG=INFO, SYSLOG
# log4j.additivity.com.axeda.drm.SYSLOG=false
```

This property registers the audit category types the Concentrator Remote Server will dispatch (or send) to the configured auditors. This property is defined by a comma-separated pair of values: severity level, appender name. The Severity level specifies the type of audit category to dispatch. The appender name identifies the auditor destination for the audit message types.

The value of the `log4j.logger.com.axeda.drm.SYSLOG` setting should generally be "INFO, SYSLOG." Note that SAL always dispatches the audit log messages with a priority of INFO.

The `log4j.additivity.com.axeda.drm.SYSLOG` property controls whether or not audit messages intended for the syslog server auditor are sent also to the drm.log file (which is the defined root logger for Log4j). By default, this property is set to false and generally should not be changed. If this property is changed to `true`, audit messages destined for the syslog will also appear in the drm.log file.

Appendix C: Editing the DRMConfig.properties file

This appendix provides a complete listing of the contents of the DRMConfig.properties file as well as definitions of the properties and the names shown on the System Configuration page of the Administration application for the properties.

Note:

The System Configuration page shows one property that is not defined in DRMConfig.properties. The CustomConfig.properties file provides a property to specify any custom build information for the Concentrator Remote Server, if applicable. This custom built information, defined in the **com.axeda.drm.custom.build-info** property, is displayed on the System Configuration page.

Overview of the DRMConfig.properties file

The `DRMConfig.properties` file is the configuration file for your Secure Access Concentrator Remote Server and the applications of the SAL system. By default, this file is located in the `avaya/SAL/CRS/config` directory.

When you install the Concentrator Remote Server software using the Installer, the settings you choose are saved in the `DRMConfig.properties` file. Although the file contains default settings for some properties that are appropriate for most installations, you may need to modify some information in this file to customize the use of each Secure Access Concentrator Remote Server. For example, you may want to add the name of the secondary directory server. By default, the Installer uses the information for the main directory server entered in the Installer. This section provides a table of all the properties, as they are organized in this file. The table also shows the names of the properties as they appear on the System Configuration pages of the Administration application.

Important:

If you are planning to use Desktop Viewer and Desktop Server, make sure that you configure the related properties as explained in Table B-1, under Global Access Server (GAS)/Remote Session Settings.

Complete list of properties

Table B-1 lists and describes the properties in the `DRMConfig.properties` file in the order in which they appear in the file. After your Secure Access Concentrator Remote Server is up and running, you can view settings for all of these properties by accessing the System Configuration pages of the Administration application. By default, these pages show the properties in groups of 25, across several pages, organized by functionality and then alphabetically within the functional group. However, you can filter the property list and display only the properties you want to see. For example, if you want to see all properties related to the Global Access Server, type `Global Access Server` in the text box at the top of the list, and click **Filter**. The page displays all properties whose name contains "Global Access Server." The column in the middle of Table B-1 provides the version of the property names as shown on the System Configuration pages.

Note:

Some properties are not displayed at all (those related to user name and password, in particular). Other properties are disabled (commented out) by default and also do not appear on the System Configuration pages. If you enable these properties, make sure that you copy them to the DRMConfigInfo.properties file. The Administration application derives its list from the DRMConfigInfo.properties file, not from the actual DRMConfig.properties file.

When editing the DRMConfig.properties or DRMConfigInfo.properties files, be sure to use forward slashes for all paths, no matter which operating system is running your Secure Access Concentrator Remote Server. All DRMConfig properties (name-value pairs) need to be on the same line. If you are copying the DRMConfig name-value pairs directly from this documentation, make sure you remove any carriage returns.

Table B-1 DRMConfig.properties File

This line	Sets the property called	Specify
Build information		
`com.axeda.drm.build-info= x.x build # (yyyy/mm/dd hh:mm EST)`	Build number	The software version, and number, date and time of this build, which is set during the installation. You do not need to modify this setting. You will need it when contacting Technical Support to help identify the version of software you are running.
SAL administrator		
`com.axeda.drm. administrator.email= your_servicelink_admin_email _address`	Administrator e-mail	The e-mail address of a user defined as a SAL administrator for this Concentrator Remote Server. This value is entered during the server installation process.
SAL user's password length		
`com.axeda.drm. user.password.length=6`	Minimum User's password length	The default length of a user's password
Password expiration control		
`com.axeda.drm. user.password.expired=30`	User's passwords are expiring in (days)	By default, the user's password expires in 30 days. If you set this property to -1, the password expiration attribute will not be set.
`com.axeda.drm. user.password.expiration_warning=5`	User's password expiration warning will be shown in (days)	By default, the SAL system warns users 5 days before their passwords are due to expire. If this property is set to -1, Secure Access Link does not check passwords for expiration.
SAL support		
`com.axeda.drm. support.email= tsupport@avaya.com`	Support e-mail	The e-mail address of Avaya's Technical Support group.
SAL server name		
`com.axeda.drm.server.name=`	Concentrator Remote Server host name	The name of this Concentrator Remote Server. This is the name entered during the server installation process. Note that this name does *not* need to correspond to a computer name. Note that the pound sign (#) is a reserved character and should not be used in the name. **Important:** The server sets this value automatically, using the name provided during installation. If this value is not set, the server will not start.

This line	Sets the property called	Specify
Auto refresh rate		
com.axeda.drm.table. auto_refresh_rate=60	Auto Refresh Rate	The default rate of refreshing tables is every 60 seconds. Leave this rate at installation. Your environment may require a change after the system has been running for a while.
com.axeda.drm. notification-refresh- interval= 1200000	User alerts refresh rate	The default number of milliseconds between automatic refreshing of user alerts.
User store settings		
#com.axeda.drm.userStore. factory= com.axeda.drm.user. ActiveDirectoryUserStoreFact ory com.axeda.drm.userStore. factory= com.axeda.drm. user.LdapUserStoreFactory	User store class name	The location of user information for SAL. Change this setting ONLY if you are storing user information somewhere other than a Sun ONE LDAP directory server and have implemented your own UserStore and UserStoreFactory. For example, if you are using Microsoft Active Directory, and you have implemented a UserStore and UserStoreFactory, change the setting accordingly. By default, the line for Active Directory is commented out. The enabled line is for Sun ONE LDAP directory server.
com.axeda.drm.userStore. authenticator.types = IPlanetAuthenticatorMBean, LDAPAuthenticatorMBean	Authenticator types assigned to the user store (commaseparated)	Supported Authenticator types: - ActiveDirectoryAuthenticatorMBean - IPlanetAuthenticatorMBean - LDAPAuthenticatorMBean - NovellAuthenticatorMBean - OpenLDAPAuthenticatorMBean If using ActiveDirectory, set this to: com.axeda.drm.userStore.authenticator. types = ActiveDirectoryAuthenticatorMBean If using Sun ONE, set this to: com.axeda.drm.userStore.authenticator. types = IPlanetAuthenticatorMBean,LDAPAuthenti catorMBean
com.axeda.drm.userStore. group.users= ServiceLinkUsers	User store user group name	The groups you have created within LDAP (or your custom user store) for the SAL system. For the system to recognize users as administrators, they must belong directly to the group specified by the userStore.group.administrators setting. For the system to allow access to users, those
com.axeda.drm.userStore. group.administrators= ServiceLinkAdmins	User store administrator group name	
com.axeda.drm.userStore.	LDAP Admin	

This line	Sets the property called	Specify
group.ldap.administrators= ServiceLdapAdmins	group name	users must belong to a group that belongs to the groups specified by the userStore.group.users setting. Note that since groups may contain sub-groups, the users must belong to a group that has ServiceLinkUsers (to use the default user group name) as an ancestor. All users defined in the group.ldap.administrators group can edit LDAP settings (for Sun ONE servers only). Membership in this group does *not* provide login access to the Applications.
com.axeda.drm.directory-server. on=true.	User store administration enabled	Leave this setting at true to ensure the use of your directory server for control of access to SAL.
Login settings for JBoss server		
com.axeda.drm.jboss. application.policy_name= servicelinkpolicy	Not displayed in the Administration application	Identifies the name of the application policy used by the JBoss server. Avaya recommends that you do not change the default property value, servicelinkpolicy. If you do change the value in this file, you will need to make the same change to the login-config.xml file in the JBoss Server.
com.axeda.drm.jboss. directory.server.loginmodule = org.jboss.security. auth.spi.LdapExtLoginModule	(Not displayed in the Administration application)	Identifies the login module (a class) used by the Concentrator Remote Server for JBoss. Avaya recommends that you do not change the default property value, org.jboss.security.auth.spi. LdapExtLoginModule. If you do change the value in this file, you will need to make the same change to the login-config.xml file in the JBoss Server.
Primary LDAP authenticator		
com.axeda.drm. directory-server. primary_authenticator= $DS_PRIMARY_AUTH_1$	(Not displayed in the Administration application)	The primary authenticator for LDAP, which is used to locate the authenticator where users and groups are created. This entry should match the name of the security realm defined for the Primary Userstore; for example, *IPlanet*. This value is set during the server installation process, based on selection of directory service. For LDAP, the default is *IPlanet*; for Active Directory, the default is *ActiveDirectory*. If you set up security realms separately, make sure you modify this property to specify the name of the security realm specified in the JBoss server.

This line	Sets the property called	Specify
Partner store settings (LDAP)		
`com.axeda.drm.partner.store.factory=com.axeda.drm.user.VendorLdapUserStoreFactory`	Partner store class name	The kind of LDAP used as a partner login store. By default, the partner login store is set to the Directory Server chosen for partner login during installation (set by the property `com.axeda.drm.userVendor.LdapUserStoreFactory`).
`com.axeda.drm.partner.store.authenticator.types = IPlanetAuthenticatorMBean,LDAPAuthenticatorMBean`	Authenticator types assigned to the partner user store (comma-separated)	Supported Authenticator types for the Partner Login user store (if applicable to this server): - ActiveDirectoryAuthenticatorMBean - IPlanetAuthenticatorMBean - LDAPAuthenticatorMBean - NovellAuthenticatorMBean - OpenLDAPAuthenticatorMBean If using ActiveDirectory, set this to: `com.axeda.drm.partner.store.authenticator.types = ActiveDirectoryAuthenticatorMBean` If using Sun ONE, set this to: `com.axeda.drm.partner.store.authenticator.types = IPlanetAuthenticatorMBean,LDAPAuthenticatorMBean`.
`com.axeda.drm.partner.store.authenticator=[replace with the real name]`	Name of the authenticator for partner logins	The name of the JBoss Authenticator configured for the partner login store. For example, *IPlanetLDAPAuthenticator.* This is the name of the security realm set up in JBoss. The default value is defined by the installer when partner login is configured.
`com.axeda.drm.partner.login.default.session.duration = 2880`	Default partner login session duration in minutes	The duration for this session, which is the number of minutes from when the session is created until it expires. During this period, no one else may log in to the server using the code created for this session. The default is 2880 minutes, or 48 hours (2 days).
`com.axeda.drm.partner.login.notify.support = true`	Notify administrator about partner login requests	True (default value) for the server to send e-mail messages requesting a session to the Concentrator Remote Server administrator e-mail address. False for the Concentrator Remote Server administrator to not receive these e-mail messages.

This line	Sets the property called	Specify
com.axeda.drm.partner. support.url = http:// [Support address]: [port number]	The partner login support URL	The SAL support URL used by the partner login sessions. This value is defined during the server installation process. Specify the complete SAL server address; for example, http://support.acme.com:1001. This value is entered during server installation. **Note:** Partners will need to access this URL; therefore, this address must be accessible outside the corporate firewall.
com.axeda.drm.partner. allow-remove=true	Allow users to remove partner accounts	True (default) to enable users to remove partners defined in the server from the server. False to prevent Applications users from deleting partners. Users also need the privilege, *Partner Login Session - Remove Partner Account,* to be able to remove partner login accounts. Additional notes: – Only disabled partners can be removed from the application. – When the partner is disabled, all active sessions for that partner will be closed. – Contacts of removed partners cannot log in to the Applications. – If a partner is removed from the server after he or she is assigned to a case, the case will show no partner assignment.
com.axeda.drm.partner. store.use.primary. authenticator=true	Use primary authenticator for partner store. **Note:** This property is not recommended for production.	True for the primary authenticator for the Concentrator Remote Server to be used also for the partner store. Set this to true only when testing partner authentication in a development/staging environment. You MUST set this value to false for a production server.
Partner Login notification messages - When a new case is created, this e-mail message is sent to the designated case partner.		
com.axeda.drm.partner. subject	Partner Login notification subject	Identifies the subject line for the e-mail message to send to the partner for a new case. Default is *Partner Login Support Information*.

This line	Sets the property called	Specify
com.axeda.drm.partner.message	Partner Login notification message	Identifies the message body for the e-mail message to send to the partner for a new case. Default is "Please visit: {0} and use the login code: {1} to access case number: {2}." In this example, {0} is replaced with the URL of the Concentrator Remote Server for the case, {1} is replaced with the partner login code the server created for this case, and {2} is replaced with the Case ID.
com.axeda.drm.partner.supportMessage	Partner Login support message	Identifies the message body for the e-mail message to send to the designated support personnel for a new case. Default is *Partner Login information with login code {0}, was sent to {1} partner {2} for case number {3}.* In this example, {0} is replaced with the partner login code the server created for the case, {1} is replaced with the name of the partner assigned to this case, {2} is replaced with the e-mail address of the partner assigned to this case, and {3} is replaced with the Case Number for the case.
com.axeda.drm.partner.fromAddress	Partner Login return address	Identifies the e-mail address of the sender for the e-mail message to send to the designated support personnel for a new case. The default address is *support@avaya.com.*
com.axeda.drm.partner.caseNotSpecified	Not displayed in the Administration application	Identifies the case number for this e-mail, if one is specified.
com.axeda.drm.partner.accessCodeNotSpecified = 'nonspecified'	Not displayed in the Administration application	Identifies the login code for the session for this e-mail, if one is specified.
Directory server (LDAP) settings		
com.axeda.drm.directory-server.port=DS_PORT_1	Not displayed in the Administration application	The number of the port on the primary server to use for directory-server communications. The standard port for LDAP directory servers is 389. This value is entered during the server installation process. If you add this property, it appears on the System Configuration page as *Primary directory server port*. **Note:** If you want to use SSL with your LDAP Sun ONE

This line	Sets the property called	Specify
		Directory Server, see Enabling SSL Encryption for Sun ONE/iPlanet Servers.
com.axeda.drm.directory-server.name=DS_HOST_1	Not displayed in the Administration application	The IP address or hostname of the server running your primary directory server. This value is entered during the installation process. Example: ldapserver_1.avaya.com. If you add this property, it appears on the System Configuration page as *Primary directory server*.
com.axeda.drm.directory-server.peoplesearch=$USER_DN_1$	Not displayed in the Administration application	Search information for locating users in the primary directory server database. This value is entered during the installation process. If you add this property, it appears on the System Configuration page as *Primary directory server people search*.
com.axeda.drm.directory-server.groupsearch=$GROUP_DN_1$	Not displayed in the Administration application	Search information for locating groups in the database of the primary directory server. This value is entered during the installation process. If you add this property, it appears on the System Configuration page as *Primary directory server group search*.
com.axeda.drm.directory-server.adminsearch=uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot	Not displayed in the Administration application	Search information for locating administrators in the database of the primary directory server. If you add this property, it appears on the System Configuration page as *Primary directory server admin search*.
com.axeda.drm.directory-server.ssl=false	SLDAP SSL Enabled	False (default) to disable the SLDAP SSL support for the Concentrator Remote Server. Change this to *true* if the Concentrator Remote Server needs to support SLDAP SSL.
Secondary directory server (LDAP) settings		
com.axeda.drm.secondary.directory-server.port=DS_PORT_1	Not displayed in the Administration application	The number of the port on the secondary server to use for directory-server communications. The standard port for LDAP directory servers is 389. This value is entered during installation. If you add this property, it appears on the System Configuration page as *Secondary directory server port*.

This line	Sets the property called	Specify
com.axeda.drm.secondary.directory-server.name=DS_HOST_1	(Not displayed in the Administration application)	The IP address or hostname of the secondary server running your directory server. This value is entered during installation. Example: ldapserver_2.avaya.com If you add this property, it appears on the System Configuration page as *Secondary directory server*.
com.axeda.drm.secondary.directory-server.peoplesearch=$USER_DN_1$	Not displayed in the Administration application	Search information for locating users in the secondary directory server database. The organizations and domain classes for your directory server are entered during installation. If you add this property, it appears on the System Configuration page as *Secondary directory server people search*.
com.axeda.drm.secondary.directory-server.groupsearch=$GROUP_DN_1$	Not displayed in the Administration application	Search information for locating groups in the secondary directory server database. The groups and domain classes for your directory server are entered during installation. If you add this property, it appears on the System Configuration page as *Secondary directory server group search*.
com.axeda.drm.secondary.directory-server.adminsearch=$DS_ADMIN_DN_1$	Not displayed in the Administration application	Search information for locating administrators in the secondary directory server database. This value is entered during installation. If you add this property, it appears on the System Configuration page as *Secondary directory server admin search*.
Web server settings		
com.axeda.drm.webserver.factory=com.axeda.drm.jboss.JbossServer	WebServer factory class name	The default Web server factory is JBoss Server.
com.axeda.drm.webserver.load.startup-in-servlet = false	Not displayed in the Administration application	How to start the Web server used with the Web Application Server.
Device communications and encryption		
com.axeda.drm.device.tokenRequired=false	Not displayed in the Administration application	False (default) to not require a token from devices, or true to require a token from devices.

This line	Sets the property called	Specify
com.axeda.drm.emessage.timeout=30	eMessage timeout	The number of seconds that the Secure Access Concentrator Remote Server waits before closing the connection to the device, allowing enough time for a message being sent from the device to the Secure Access Concentrator Remote Server to complete.
com.axeda.drm.emessage.ignore.duration=0	Ignore eMessage Duration	The number of minutes after startup that the Concentrator Remote Server ignores messages from devices.
com.axeda.drm.emessage.persistent_connection=false	eMessage persistent connection	False (default) to not require a persistent HTTP connection (HTTP 1.1 only), or true if you are using HTTP 1.1 and require a persistent HTTP connection.
com.axeda.drm.emessage.device.overwrite.timezone=true	eMessage will overwrite device time zone	True (default) for the eMessage from the device (registration message) to overwrite the setting for the device's time zone (as stored in the Concentrator Remote Server database).
com.axeda.drm.device.allowUnencryptedData=true	Allow unencrypted device data	True (default) to allow the application to accept unencrypted messages from devices, or false to reject unencrypted messages.
com.axeda.drm.devcon.emessage.badData=false	Process bad quality data	False (default) to reject bad or uncertain data, or true to accept bad or uncertain data.
com.axeda.drm.device.update-missing-devices-interval = 30	Missing device update frequency	The number of seconds to wait between updating devices' *missing* states. The default is 30 seconds.
com.axeda.drm.device.default-missing-ping-multiplier=1	Default missing device ping multiplier	An integer to use in the equation that determines when the system should consider that devices are missing. The following equation is used to make this decision: missing = current-time > last-contact + ping-rate * ping-multiplier + additional-factor
com.axeda.drm.device.default-missing-additional-factor=10	Default missing device additional factor	The number of seconds to use in the equation for determining that devices are missing. The default is 10 seconds.
com.axeda.drm.device.redundant-gateways = false	Server running in redundant-gateways mode	If True, the server is set to redundant-gateways mode; if false (default), the server is not running in redundant-gateways mode. When in redundant-gateways mode, the server can support multiple gateways managing the same device.

This line	Sets the property called	Specify
com.axeda.drm.device. allowAutoCreation=true com.axeda.drm.model. allowAutoCreation=true	Allow automatic creation of devices Allow automatic creation of product families	True (default) to allow automatic addition of devices and product families to the database upon registration.
com.axeda.drm.device. disableNotificationsOn Registration=false	Disable notification on device registration	False is the default setting, which means that all newly registered devices are excluded from notifications for all users. Change to true to include all newly registered devices in notifications for all users.
com.axeda.drm. notifications.exclude DefaultGroupFrom Notifications=false	Exclude default group from notifications	True to exclude all users from device group security-based notifications who belong to the default device group only, for a specific product family. False to include all such users. False is the default setting, which means if a user is included in the default device group for a product family and in no other device group settings for that product family, that user will receive notifications for the related device.
com.axeda.drm.device. enableGatewayLocationCusto merInheritance	Not displayed in the Administration application	True for managed devices to inherit the location and organization set for their managing Gateway upon registration with SAL. False (default) to require the location and organization to be set for each device.
com.axeda.drm.resource. update.interval	Not displayed in the Administration application	Identifies the resource update interval that controls how soon a change in security is applied to active Applications sessions. By default (and if not specified), this value is set to 120000 milliseconds, or 2 minutes.
Database and database pools		
com.axeda.drm.db. dataSource=drm-data_source	Data source name	The appropriate domain name and JDBC data source. The value shown here is the default used by SAL. If you plan to change it (or have changed it) when configuring your JBoss Server, make sure that the name you used appears here. **Important:** This property MUST be set in order for the Concentrator Remote Server to start.

This line	Sets the property called	Specify
com.axeda.drm.db. maxDataInsertDelay=1	Maximum delay between data inserts in seconds	The maximum number of seconds between data inserts.
com.axeda.drm.db. maxDataInsertQueueSize= 25000	Maximum queue size for inserting data items	The maximum number of data items that can be placed in the queue before the system starts discarding the oldest data items. Avaya recommends that you do not set this value above 30000.
com.axeda.drm.db. maxAlarmInsertDelay=10	Maximum delay between alarm inserts in seconds	The maximum number of seconds between alarm inserts.
com.axeda.drm.db. maxAlarmInsertQueueSize= 25000	Maximum queue size for inserting alarms	The maximum number of alarms that can be placed in the queue before the system starts discarding the oldest alarms. This value must not exceed 30000. Avaya recommends that you ignore this parameter as the remote server does not handle alarms.
com.axeda.drm.db. maxEventInsertDelay=10	Maximum delay between event inserts in seconds	The maximum number of seconds between event inserts.
com.axeda.drm.db. maxEventInsertQueueSize= 25000	Maximum queue size for inserting events	The maximum number of events that can be placed in the queue before the system starts discarding the oldest events. Avaya recommends that you do not set this value above 30000.
com.axeda.drm.db. maxScriptInsertDelay=10	Maximum delay between script inserts in seconds	The maximum number of seconds between script message inserts.
com.axeda.drm.db. maxScriptInsertQueueSize= 25000	Maximum queue size for inserting scripts	The maximum number of script messages that can be placed in the queue before the system starts discarding the oldest script messages. Avaya recommends that you do not set this value above 30000.
com.axeda.drm.db. maxLastContactUpdateDelay= 5	Maximum delay between last contact update inserts in seconds	The maximum number of seconds to allow between contact updates.

This line	Sets the property called	Specify
com.axeda.drm.db.maxLastContactUpdateQueueSize=25000	Maximum queue size for inserting last contact updates	The maximum number of updates the queue can hold before the system starts discarding the oldest updates. Avaya recommends that you do not set this value above 30000.
com.axeda.drm.db.maxPackageStatusInsertDelay=10	Maximum delay between package status inserts in seconds	The maximum number of seconds to allow between package status updates.
com.axeda.drm.db.maxPackageStatusInsertQueueSize=25000	Maximum queue size for inserting package status	The maximum number of package status messages the queue can hold before the system starts discarding the oldest updates. Avaya recommends that you do not set this value above 30000.
com.axeda.drm.db.maxUploadChunkInsertDelay=10	Maximum delay between upload chunk updates in seconds	The maximum number of seconds to allow between upload chunk updates.
com.axeda.drm.db.maxUploadChunkInsertQueueSize=25000	Maximum queue size for upload chunk updates	The maximum number of uploaded (file/data) chunks the queue can hold before the system starts discarding the oldest updates. Avaya recommends that you do not set this value above 30000.
com.axeda.drm.db.lastContactUpdateRatio=1	Number of device messages per last contact update	The number of device messages that will cause the server to update a device's last contact time. For example, if set to 10, the server updates a device's last contact time when processing every 10th message from the device. By default this value is 1, which causes the server to update the last contact time with each message received from a device. Although increasing the value of this parameter helps improve the server's scalability, it also lengthens the amount of time required to detect that the device is missing.
com.axeda.drm.db.maxStateInsertQueueSize=25000	Maximum queue size for inserting states	The maximum number of device states that can be placed in the queue before the system starts discarding the oldest device state. Avaya recommends that you do not set this value above 30000.
com.axeda.drm.db.maxStateInsertDelay=10	Maximum delay between state inserts in seconds	The maximum number of seconds between device state inserts. The default value is 1800 seconds.

This line	Sets the property called	Specify
com.axeda.drm.db. devconSyncDelay=10	Devcon cache synchronization delay	The number of seconds between synchronizations of the device context cache with the database.
com.axeda.drm.db. deviceUpdateSyncDelay =10	Device update synchronization delay	The number of seconds between checks by the device context cache for device updates in the database.
com.axeda.drm.search. defaultMaxResults=1000	Maximum number of search results	The maximum number of rows for a set of search results to display on an application page (for a database search).
com.axeda.drm.data.failed_ insert.enable=false	Enable writing data to file should processing fail	True to save data that could not be inserted in the database to a backup file. False (default) to discard the data if the database insert fails.
com.axeda.drm.data.failed_ insert.file_prefix= *[[Replace with File Name Prefix]]*	Name of the file used to store data should a database insert fail	The name of the backup file in which to store data that cannot be inserted in the database (If the server is set to save data to a backup file). If necessary, the server creates this file. Make sure com.axeda.drm.data.failed_insert.enable is set to *true*.
com.axeda.drm.data.failed_ insert.file_extension= *[[Replace with File extension]]*	Extension of file used to store data should an insert fail	The extension (type) of the backup file in which to store data that cannot be inserted in the database (if the server is set to save data to a backup file). For example. *csv* or *txt*. If necessary, the server creates this file. Make sure com.axeda.drm.data.failed_insert.enable is set to *true*.
com.axeda.drm.data.failed_ insert.file_path= *[[Replace with File path]]*	Path of the file used to store data should an insert fail	The path of the backup file in which to store data that cannot be inserted in the database (if the server is set to save data to a backup file), If necessary, the server creates this file. Make sure com.axeda.drm.data.failed_insert.enable is set to *true*.
Service application		
com.axeda.drm.service. dateNavigationAmount=1	Service Application date navigation amount	An integer to set the number of steps backward in time that each click of the single arrow will take. The default setting is 1, so that the arrow moves back one step with each click. Thus, if data is updated once per minute, the setting of 1 here means that clicking the arrow results in the display of data going back 1 minute. If data is updated every 30 seconds, clicking the arrow results in the display of the last update.

This line	Sets the property called	Specify
`com.axeda.drm.service.dateNavigationBigAmount=10`	Service Application date navigation big amount	An integer to set the number steps backward in time that each click of the double arrow will take. The default setting is 10, so if data is updated once every minute, clicking the double arrow results in the display of data going back 10 minutes. If data is updated every 30 seconds, clicking the arrow results in the display of data going back 5 minutes.
`com.axeda.drm.service.device.overview.note.displayLength=100`	Service Application Device dashboard note display length	The number of lines for notes about devices on the home page of the Service application.
E-mail server		
`com.axeda.drm.email.server=`*`server_name.domain_name.domain_type`	E-mail server	Name of the e-mail server to use for sending e-mail messages. Specify the complete server path, for example, *usmail2.avaya.com.*
`com.axeda.drm.email.default-encoding=UTF-8`	Default e-mail encoding	Type of encoding to use as the default for e-mail messages. The default is UTF-8. Other possibilities include ASCII, UTF-16, ISO8859, and so on. A complete list is available on the Preferences page of the Applications. The type of encoding you select must be supported by your e-mail server and client applications.
Script settings		
`com.axeda.drm.script.timeout-factor=5`	Scripting timeout	A number by which to multiply the ping rate in order for the server to determine when SOAP messages to a device have timed out and the status of the script or timer should be changed. What the status is changed to depends upon which operation timed out. For example, suppose a device has a ping rate of one minute, and the default timeout factor of 5 is used. You attempt to register a timer on the device, but the device is offline. After 5 minutes, the timer will go from *waiting to register* to *register error.*
Trigger settings		
`com.axeda.drm.triggers.alarm.enable=true`	Enable alarm rules	True to enable the processing of alarm triggers (default), or false to disable processing. **Note:** Avaya recommends that you ignore this parameter as the remote server does not handle alarms.

This line	Sets the property called	Specify
com.axeda.drm.triggers. data.enable=true	Enable data rules	True to enable the processing of data triggers (default), or false to disable the processing. **Note:** If you are not going to need these triggers, set this to false to improve system performance.
com.axeda.drm.triggers. registration.enable=true	Enable registration rules	True to enable the processing of device registration events as triggers (default), or false to disable the processing. **Note:** If you are not going to need these triggers, set this to false to improve system performance.
com.axeda.drm.triggers. soap-status.enable=true	Enable SOAP status rules	True to enable the processing of SOAP status events as triggers (default), or false to disable the processing. **Note:** If you are not going to need these triggers, set this to false to improve system performance.
com.axeda.drm.triggers. file-upload.enable=true	This entry enables/disables upload rule	True to enable file uploads as triggers (default), or false to prevent file uploads from acting as triggers.
com.axeda.drm.triggers. schedule.enable=true	Enable schedule rules	True to enable schedule triggers (default); false to disable schedule triggers. **Note:** If you are not going to need these triggers, set this to false to improve system performance.
com.axeda.drm.triggers. schedule.delay=1	Schedule rules delay	The delay (in minutes) that the schedule thread waits between database queries for execution.
com.axeda.drm.triggers. schedule.newThread=true	New thread for schedule rules	True to spawn a new thread to process each trigger (default); false to use same thread for each trigger. Keep in mind that the number of threads is related to system performance. You may need to tune this setting.
com.axeda.drm.triggers. schedule.owners=drmdata_ source	Schedule rules owners	Do not change. This property identifies the data source name for scheduled business rules.
Access settings		
com.axeda.drm.access. msgtimeout=40	Access message timeout	The number of seconds the Access application waits between messages from Access Viewer or Access Remote server. If the Access application does not receive any messages within this time period (for example, if there are network problems), the session is disconnected. The default is 40 seconds.

This line	Sets the property called	Specify
		In addition, this is the period of time within which the Access Viewer and Access Remote server operators must connect to the shared session. If both Access Viewer and Remote do not connect to the session within this timeout period, the session will time out, and a new session must be requested.
`com.axeda.drm.access.sessiontimeout=10`	Access session timeout	The number of minutes an inactive session stays open, waiting for activity, before it is removed. An inactive session is one that has not been used (no Access Viewer or Access Remote server computers shared using this session ID). The default is 10 minutes (between contacts).
`com.axeda.drm.access.unattendedsessiontimeout=10`	Access unattended session timeout	The number of minutes an inactive, unattended session stays open, waiting for activity, before it is removed. An inactive session is one that has not been used (no Access Viewer or Access Remote computers shared using this session ID). The default is 10 minutes (between contacts).
`com.axeda.drm.access.sessionidlength=6`	Access session ID length	Length (in characters) of the Access Session ID. The default length is 6 characters.
`com.axeda.drm.desktop.downloadto.nix=/opt/Axeda/Desktop/Viewers`	Desktop Viewer download location on Linux client	The directory on client UNIX/Linux-based systems where the system should download automatically the viewer application for a remote session with the device. This property defines the default location for Quick Launch downloads of the appropriate viewer application for the device from the Remote Sessions module (or page) in the Device dashboard for the device (Service application). See also Configuring and Customizing Applications.

`# com.axeda.drm.access.ViewerIPMask1=255.0.0.0`
 	
`# com.axeda.drm.access.ViewerIP1=192.168.0.0`
 	
`# com.axeda.drm.access.RemoteIPMask1=255.255.0.0`
 	
`# com.axeda.drm.access.RemoteIP1=192.168.0.0`
	Not displayed in Administration application	IP addresses to compare with the xxIP address after the mask is applied. Only those addresses are allowed.
		
		Note:
		By default, these parameters are commented out (disabled). If you enable these parameters (remove the # sign), be sure to add them to the DRMConfigInfo.properties file.

Global Access Server (GAS)/remote session settings		

This line	Sets the property called	Specify
com.axeda.drm.remote. session.force-ssl=false	Force SSL for remote session	Used to force remote sessions to always use https (443). The default is false (SSL not forced); change to True to force remote sessions to use https (port 443).
com.axeda.drm.remote.server. tzOffset=0	Time Zone Offset for the internal access server	Used to set the timezone offset if the Global Access Server is in a different timezone from the Concentrator Remote Server. The Offset is defined as a number of hours ahead of or behind GMT. For example, -6:00 sets the time zone offset to six hours behind GMT (Central Standard Time).
com.axeda.drm.remote.audit. allow-remove=false	Allow the Admin to remove Remote Session Audit Information	True to allow the Administrator to delete the audit session information from the Administration application. By default, the administrator cannot delete the audit session information (false).
com.axeda.drm.remote. session.allow-end=true	Allow remote sessions to be stopped	True (the default value to allow the Administrator to stop Global Access Server remote sessions (using the Administration application). If changed to false, administrator cannot stop GAS remote sessions.
com.axeda.drm.remote. session.allow-hostedend= false	Allow hosted sessions to be stopped (Caution should be taken when setting to true)	True to allow the Administrator to stop Global Access Server remote sessions hosted by this server (using the Administration application). By default, the administrator cannot stop host GAS remote sessions (false).
com.axeda.drm.remote. server.allow-remove	Allow users to remove partner accounts	True to allow the Administrator to delete the Global Access Server from the Administration application. By default, the administrator cannot delete the GAS (false).
com.axeda.drm.remote. enterprise.allowremove= true	Allow users to remove remote Concentrator Remote Servers	True (the default value) to allow the Administrator to delete remote Concentrator Remote Servers (from the Administration application). If changed to false, the administrator cannot delete the remote Concentrator Remote Server.

This line	Sets the property called	Specify
`com.axeda.drm.remote.management-enterprise=false`	Not shown in Administration application	True (default value) for the Concentrator Remote Server to provide hosting solutions for GAS, version 5.3. If true, the Applications show remote access hosting functionality, and any configured Global Access Servers are managed by this Concentrator Remote Server. False if the Concentrator Remote Server does *not* support remote access/GAS hosting. (If false, the Concentrator Remote Server will treat all configured GAS servers as standalone servers.)
`com.axeda.drm.remote.activity-monitor.enabled = false`	Remote activity monitor	False (default) to disable the activity monitor for remote sessions. True to enable the monitor. The Activity Monitor tracks sessions that were created and cleans up sessions that it determines are abandoned. If true, the activity monitor for the GAS is enabled; if false, the activity monitor is disabled.
`com.axeda.drm.remote.activity-monitor.cleanup-period = 720`	Global Access Server activity monitor cleanup period	The number of hours that the Activity Monitor will wait before cleaning out inactive sessions. Identifies how frequently the activity monitor runs and cleans up (removes) unused or abandoned sessions. The default is every 720 (seconds).
`com.axeda.drm.remote.activity-monitor.monitorperiod = 60`	Remote activity monitor period	How frequently the activity monitor runs to track all remote sessions for this GAS. During this operation, the activity monitor is watching each session. If it seems that a session may be abandoned (based on the value of `com.axeda.ras.activity-monitor.min-data-threshold`), the activity monitor does not remove the session until the number of cleanup periods has been reached (as defined in `com.axeda.ras.activity-monitor.numperiods-forcleanup`). While monitoring a potentially abandoned session, the activity monitor will run at the frequency specified here. The default is every 60 (seconds).

This line	Sets the property called	Specify
`com.axeda.drm.remote.activity-monitor.min-data-threshold = 4096`	Not displayed in Administration application	The minimum amount of data that must be transmitted during a session for the activity monitor to consider the session active. If the activity monitor determines that an *active* session is transmitting fewer bytes than specified here, it will track the session and may eventually remove the session (based on the `com.axeda.ras.activitymonitor.num-periodsfor-cleanup` setting). The default is every 4096 (bytes).
`com.axeda.drm.remote.activity-monitor.numperiods-for-cleanup = 3`	Not displayed in Administration application	How frequently the activity monitor runs and tracks inactive sessions while the GAS is running. The activity monitor runs a total of *x* times before it removes a session, if applicable. (*x* being the value defined for this property). If it determines that a session is potentially inactive (based on the number of bytes transmitted in a session), the activity monitor continues to monitor the session (*x*-1) more times. If the session still appears inactive after the activity monitor has run all *x* times, the activity monitor removes the session. This property defines the number of times that the activity monitor runs. The `com.axeda.ras.activity-monitor.monitor-period` property defines the frequency with which the activity monitor runs. For example, suppose `com.axeda.ras.activitymonitor.monitor-period = 60` and `com.axeda.ras.activity-monitor.numperiodsfor-cleanup = 3` The activity monitor runs three times, or once every 60 seconds, while monitoring a potentially abandoned session. If, upon reaching the third time, the session still appears inactive (that is, has not transmitted the minimum amount of data), the activity monitor removes the session. The default is 3 (periods).
`com.axeda.drm.remote.session.allow-merge = true`	Remote session merge allowed	True (default) to allow remote sessions to merge or false to prevent remote sessions from merging.
`com.axeda.drm.remote.server.hostName= $SL_CLUSTER_IP_1$`	Global Access Server DNS name (IP) usable by all users	An IP address that all Agents can access for Remote Sessions. The Concentrator Remote Server installer will set it to the IP address for the cluster, if applicable. (Clusters are not supported for this release.)

This line	Sets the property called	Specify
com.axeda.drm.remote.server.extHostName=*$SL_CLUSTER_IP_1$*	Global Access Server external address	An IP address that can be used for Remote Sessions from computers that are not running Agents. The Concentrator Remote Server installer sets this to the IP address for the cluster, if applicable. (Clusters are not supported for this release.)
com.axeda.drm.remote.server.exclusiveHost=*IP_address*	Global Access Server name of host to be used exclusively for all remote sessions	The IP address of the host that will be used exclusively for Remote Sessions.
com.axeda.drm.remote.server.hostPort=*$SL_NODE_PORT_1$*	Server port for remote session communications	The number of the port on the Concentrator Remote Server computer to use for Remote Session communications.
com.axeda.drm.remote.server.hostSSLPort=**443**	Server port for secure remote session communications	The number of the port on the Concentrator Remote Server computer to use when SSL encryption is required for Remote Sessions.
com.axeda.drm.remote.server.notifyAlive=15	Ping rate for Global Access Servers to notify they are alive	The rate (in seconds) at which Remote Servers will notify the Concentrator Remote Server that they are *alive*.
com.axeda.drm.remote.server.startupTimeout=120	Remote session start-up timeout in seconds	The number of seconds before a session that has not started is closed. This timeout must be greater than the device Ping rate. The default is 120 seconds (2 minutes).
com.axeda.drm.remote.server.inactiveTimeout=120	Remote session inactive timeout in seconds	The number of seconds before closing a session that is inactive (either from user or device). The default is 120 seconds (2 minutes).
com.axeda.drm.remote.server.directConnectPort=17001	Standard connection port socket	The number of the port that GAS server can use to connect directly to the device when the HTTP port specified is blocked. The default is 17001.
com.axeda.drm.remote.server.directConnectSSLPort=17002	SSL connection port socket	The number of the SSL port that GAS server can use to connect directly to the device when the HTTPS port specified is blocked.The default is 17002.

This line	Sets the property called	Specify
`com.axeda.drm.remote.server.agent-directprotocol=true`	Direct protocols allowed	True (default) for the server to accept direct protocol connections. (The agent uses the "direct connect" protocol in remote sessions.) False for the server to prohibit direct protocol connections from agents and ignore the following direct connect properties: *directConnectPort* and *directConnectSSLPort*.
`com.axeda.drm.remote.server.keystore=`	Not shown in Administration application	The path on the Concentrator Remote Server for the keystore that identifies the Remote Server for SSL communications.
`com.axeda.drm.remote.server.passphrase=`	Not shown in Administration application	The passphrase that the Remote Server uses when communicating directly with the Concentrator Remote Server using SSL.
`com.axeda.drm.remote.server.keyphrase=`	Not shown in Administration application	The keyphrase that the Remote Server uses when communicating directly with the Concentrator Remote Server using SSL.
`com.axeda.drm.remote.server.ssl.algorithm=SunX509`	Name of the Key Management Algorithm	The name of the SSL algorithm for KeyStore and TrustManager. In keeping with the default selection of the JBoss Server, the default SSL algorithm to select is SunX509.
`com.axeda.drm.remote.server.ssl.protocol=SSLv3`	Name of the SSL Protocol used	The version of SSL protocol to use. SSLv3 is the default protocol to use for SSL negotiation. You should not need to change this setting.
`com.axeda.drm.remote.server.tokenLength=32`	Not shown in Administration application	The number of bytes that specify the size of the secure token used to identify and confirm the server. The length should be between 16 and 128 bytes; the default is 32 bytes.
`com.axeda.drm.remote.server.auto-register=true`	Global Access Server auto register	True to allow remote servers to register themselves with the Concentrator Remote Server; false to require that someone register them manually.
`com.axeda.drm.remote.server.sessionLogPath=$USER_INSTALL_DIR$/sessionlogs`	Global Access Server log path	The path in which to store Terminal audit sessions. If this path is empty of invalid, the audit sessions are not stored. Example: `/avaya/SAL/CRS/sessionlog`
`com.axeda.drm.remote.server.maxSessions=10`	Global Access Server max. sessions	The maximum number of sessions to allow on this server. To specify an unlimited number of sessions, type 0 here.

This line	Sets the property called	Specify
com.axeda.drm.remote. server.maxBufferSize=10	Global Access Server buffer size	The maximum amount of data (in KB) that can be buffered on the Concentrator Remote Server before further data posts are rejected. The default is 10 KB. a setting of -1 disables buffering on the Concentrator Remote Server.
com.axeda.drm.remote. server.getDeviceTimeout=30	Global Access Server device timeout	The number of seconds that an Agent getData request pauses to wait for data. If the time period is reached before data is received, the getData request is returned with a NO DATA value specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40 to 45 seconds).
com.axeda.drm.remote. server.getUserTimeout=1	Global Access Server user timeout	The number of seconds that a User getData request pauses to wait for data. If the time period is reached before data is received, the getData request is returned with a NO DATA value specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40 to 45 seconds). Set this to a small value.
com.axeda.drm.remote. server.name=	Global Access Server internal name	A user-friendly name to display for the server. The default value is *Internal*.
com.axeda.drm.remote. server.desc	Internal Global Access Server description	A user-friendly description to display for the server. The default value is *Internal Access Server*.
com.axeda.drm.remote. server.agentModel=	Not displayed in Administration application	The name of the Agent Product Family watching the remote server (Federated Concentrator Remote).
com.axeda.drm.remote. server.agentSerial=	Global Access Server agent serial	The solution element / asset id of the Agent that has been deployed on the Remote Server.
com.axeda.drm.remote. ras.webservices=false	Global Access Server Web service name	True to enable Web Services for the Global Application Server (GAS); false (default) to disable Web Services for it.
com.axeda.drm.remote. abs.webservices=false	Application bridge Web service	True to enable Web Services for the Application Bridge Server (ABS); false (default) to disable Web Services for it.
com.axeda.drm.remote. ras.use-ssl=false	Global Access Server uses SSL	True to enable SSL for the Global Access Server (GAS); false (default) to disable SSL for it.
com.axeda.drm.remote. abs.use-ssl=false	Application Bridge server use SSL	True to enable SSL for the Application Bridge Server (ABS); false (default) to disable SSL for it.

This line	Sets the property called	Specify
com.axeda.drm.remote. server.use-user-timezone = false	Global Access Server determined by user's time zone	True to use the user's time zone to determine which Global Access Server (GAS) to use; false (default) to find the GAS using the default algorithm. The default algorithm uses the time zone offset value of the GAS and the device to determine their geographical location. The algorithm then uses the geographical location, the current load, and maximum supported load to determine the GAS to use.
com.axeda.drm.remote. terminal.sessionLogPath= =$USER_INSTALL_DIR$$/ $sessionlogs	Path to store terminal audit sessions	The path where audit logs of terminal sessions will be stored on this Concentrator Remote Server.
com.axeda.drm.remote. terminal.maxSessions=10	The maximum number of terminal sessions allowed on this server.	The maximum number of terminal sessions to allow on this Concentrator Remote Server. To specify an unlimited number of sessions, type 0 here.
com.axeda.drm.remote. application.launchPage= launch/application.jsp	JSP page to use for Remote Application sessions	The location of the launch page for Remote Application sessions.
com.axeda.drm.remote. application. maxSessions=	The maximum number of application sessions allowed on this server	The maximum number of sessions to allow on this server. To specify an unlimited number of sessions, type 0 here. The default is 10 sessions.
com.axeda.drm.remote. application. maxBufferSize=-1	Remote Application maximum data buffer size	The maximum amount of data (in KB) that can be buffered on the Concentrator Remote Server before further data posts are rejected. The default setting of -1 disables buffering on the Concentrator Remote Server.
com.axeda.drm.remote. application. getDeviceTimeout=30	Remote Application timeout	The number of seconds that an Agent getData request pauses to wait for data. If the time period is reached before data is received, the getData request is returned with a NO DATA value specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40 to 45 seconds). The default is 30 seconds.

This line	Sets the property called	Specify
com.axeda.drm.remote.application.getUserTimeout=1	Remote Application user timeout	The number of seconds that a User getData request pauses to wait for data. If the time period is reached before data is received, the getData request is returned with a NO DATA value specified. This amount needs to be less than any proxy or bridge timeouts for HTTP GET requests (usually 40 to 45 seconds). Set this to a small value.
com.axeda.drm.remote.application.secureWebPorts=443	Remote Application secure Web port	The port number used by the secure Web server. To connect to this port, Web-browser sessions must be secure. The default port is 443.
com.axeda.drm.remote.gas.proxy-name = [Proxy server name or address, if server behind firewall]	Global Access Server proxy name	IP address or the host name of the proxy server that the Global Access Server will use to access the Concentrator Remote Server.
com.axeda.drm.remote.gas.proxy-port = [Proxy server port, if server behind firewall]	Global Access Server proxy port	The number of the port on the proxy server that the Global Access Server will use when accessing the Concentrator Remote Server.
com.axeda.drm.remote.gas.proxy-user = [Proxy server login name (optional)]	Not displayed in Administration application	The login name for the Global Access Server to use when accessing the proxy server.
com.axeda.drm.remote.gas.proxy-pwd = [Proxy server login password (optional)]	Not displayed in Administration application	The password for the proxy server login name.
com.axeda.drm.remote.server.validate-sslcertificate=false	Not displayed in Administration application	True for the Global Access Server (GAS) to strictly validate all SSL certificates. False (the default) for the server to accept any certificates.
com.axeda.drm.remote.server.direct-connect-foragent-versions-from = 384	Not displayed in Administration application	The version of the agent from which connections are permitted if the server is configured to accept "direct protocol" connections from agents.
com.axeda.drm.remote.gas.inactivity-period = 0	Inactivity period for GAS monitoring task	The number of minutes that the Concentrator Remote Server waits without communication from the Global Access Server (GAS) before setting the status of the GAS to Offline.
com.axeda.drm.remote.abs.inactivity-period = 0	Inactivity period for ABS monitoring task	The number of minutes that the Concentrator Remote Server waits without communication from the Application Bridge Server (ABS) before setting the status of the ABS to Offline.

This line	Sets the property called	Specify
com.axeda.drm.remote.http_ connect_timeout	Not displayed in Administration application	Sets HTTP connection timeout. The default is 60000 (seconds).
com.axeda.drm.remote.set_h ttp_timeout	Not displayed in Administration application	Forces HTTP connection timeout if true. The default is false (HTTP connection timeout not forced).
File transfers		
com.axeda.drm.xfer. basedir.download=*path*	File download base directory	The path to the download directory for the Secure Access Concentrator Remote Server.
com.axeda.drm.xfer. basedir.upload=*path*	File upload base directory	The path to the upload directory for the Concentrator Remote Server. Be sure to use forward slashes in the path, no matter which operating system is hosting your Concentrator Remote Server.
Scheduler		
com.axeda.drm. scheduler.check-pooled-frequency=60000	Scheduler check pooled frequency	The number of milliseconds that the Scheduler waits before the next scheduled execution of tasks.
com.axeda.drm. scheduler.retry-frequency= 100	Scheduler retry frequency	The number of milliseconds that the Scheduler waits between attempts to connect to the Oracle database.
com.axeda.drm. scheduler.max-threads=5	Scheduler maximum threads	The maximum number of threads for the Scheduler to use.
com.axeda.drm.scheduler. jms-enabled = false	Scheduler uses JMS	If JMS enabled (true), create com.axeda.drm.scheduler.SchedulerTopic in JBoss. By default, this property is false.
Instantiator		
com.axeda.drm. instantiator. startup-file.name= startup.xml	Instantiator start-up file	Name of the XML configuration file for the Scheduler. The Instantiator reads this file for the Scheduler.
Data sources		
com.axeda.drm. datasource.remote.port= 8800	Remote data source Port	The remote.port and remote.host parameters support the import of non-SAL data, such as external databases and @aGlance data servers.

This line	Sets the property called	Specify
# com.axeda.drm. datasource.remote.host= localhost	Not displayed in Administration application	These parameters apply to a Concentrator Remote Server installation that is integrating such external data sources only; otherwise, they are ignored. Avaya offers a stand-alone program called Adapter to gather the data and communicate with the Concentrator Remote Server through a TCP socket. The port and host properties tell the SAL system on which host and port the Adapter process is listening. For the port, type the port on which to access the remote data source. For the host, ONLY IF the remote data source is running on a separate node, un-comment the line and type the IP address of the node where the remote data source is running.
Cognos 8 report		
com.axeda.drm.cognos. report.serverurl	Not displayed in Administration application	The URL of the Cognos 8 server. For example, *http://server.avaya.com.*
com.axeda.drm.cognos. report.port =	Not displayed in Administration application	The port for the Cognos 8 server. This value is entered during installation. The default port is 9300.
com.axeda.drm.cognos. listener.port = $COGNOS_WEB_PORT_1$	Not displayed in Administration application	Port used by the proxy servlet to redirect requests from the JBoss application server to the Cognos 8 server.
com.axeda.drm.cognos.publi sh.folder = Custom Reports	Not displayed in Administration application	*When configuring Cognos 8 server to support multiple Concentrator Remote Servers:* The default directory on the Cognos 8 server to which reports, queries, and other Cognos 8 objects are saved. The Cognos user can select to save Cognos 8 objects to a different directory location. When the server is running in a Cognos 8 hosted environment, this property should match the name of the hosted customer.
com.axeda.drm.cognos. report.namespace = AxedaNameSpace	Not displayed in Administration application	*When configuring Cognos 8 server to support multiple Concentrator Remote Servers:* Configure the customer's namespace for the Cognos 8 server. This should match the name provided during SAL Installation. By default, this value is *AxedaNameSpace*. Change this value only if you are running the Cognos 8 server in a hosted environment.

This line	Sets the property called	Specify
com.axeda.drm.cognos. hosting.environment	Not displayed in Administration application	Identifies if Cognos 8 is running in a hosted environment. If running in a hosted environment, then the Applications user will not have access to Cognos 8 administration links on the Administration application - Report Administration page (various Report Admin Tools). If false (default value), the server is running in a nonhosted environment and, therefore, the Cognos 8 administration tools and links are available. Change this to true to hide the Cognos Administration links because the server is running in a hosted environment.
com.axeda.drm.cognos. ping.session	Not displayed in Administration application	Cognos 8 session timeout value, in minutes. The default is 10 (minutes).
Character handling		
com.axeda.drm.character. filter.filter_non_ascii_ characters=false	Filter non-ascii characters from device data	True to enable the filtering of non-ASCII characters or false to disable filtering.
com.axeda.drm.character. filter.substitute_ character=?	Filter substitute character	The character that replaces non-ASCII characters when filtering is enabled.
Software Configuration Management (Software Application)		
com.axeda.drm.scm. upload-manager.root= c:/servicelink/scm/uploads	Software Management upload root directory	The root directory for the files that will be uploaded by devices. The files are stored in subdirectories by device ID. This directory must exist before you start the server or use the Software Management application. This property is set when you run the Concentrator Remote Server Installer. If the Software Management this directory is located on another server, all managed servers must reference that directory via Samba UNC or NFS mount points. (NFS mount points is the recommended method.)
com.axeda.drm.scm. package-files.root= c:/servicelink/scm/ downloads/package	Software Management package root directory	The location where package files that the user has uploaded to the server to be part of a package should be stored. This directory must exist before you start the server or use the Software Management application. This property is set when you run the Concentrator Remote Server Installer. If this Software Management directory is located on another server, all managed servers must reference that directory via Samba UNC or NFS mount points. (NFS mount points is the recommended method.)

This line	Sets the property called	Specify
com.axeda.drm.scm.named-instruction-files.root=c:/servicelink/scm/downloads/named_instruction/	Software Management named Instruction file root directory	The location where files that the user has uploaded to the server to be part of a named instruction set should be stored. This directory must exist before you start the server or use the Software Management application. This property is set when you run the Concentrator Remote Server Installer. If this Software Management directory is located on another server, all managed servers must reference that directory via Samba UNC or NFS mount points. (NFS mount points is the recommended method.)
com.axeda.drm.scm.temp-directory=c:/servicelink/scm/downloads/temp	Software Management temporary directory	The path to temporary space in which the Software Management application can store files that are uploaded to the Concentrator Remote Server for the purpose of being downloaded to devices. This directory must exist before you start the server or use the Software Management application. This property is set when you run the Concentrator Remote Server Installer. In a clustered environment, all managed servers must reference that directory via Samba UNC or NFS mount points. (NFS mount points is the recommended method.) For file uploads, file content will be written to this location. (Clusters are not supported for this release.)
com.axeda.drm.scm.timeout-ping-multiplier=4	Software Management timeout ping multiplier	The number of ping intervals the server waits before timing out a *Pending* software package deployment. These deployed packages are in a Pending state, meaning they are still on the Concentrator Remote Server and have not yet deployed to the device. The expectation is that, if a device is missing and you deploy a package to it, you do *not* want that package be sent when the device comes back online a day later. For example, if a device pings the server every hour, and the timeout ping multiplier is 4, then a package will be timed out if it remains pending for four hours. Set this value to -1 if the package should never expire.
com.axeda.drm.scm.upload.keep-history=true	Software Management upload keeping history	True to keep old copies of the same files (as defined by the full name, path, and hint) or false to overwrite existing files.

This line	Sets the property called	Specify
com.axeda.drm.scm. upload.keep-history. override=snapshot	Software Management upload keeping history override	A comma-separated list of file hints that are exceptions to the keep-history rule set with the keep-history property. The default setting is snapshot. For example, if keep-history is true, then this list determines files that will *not* be kept when a file of the same name arrives. To keep all copies of all files except for the dependency files from the agents, you would set these properties as follows: upload.keep-history = true upload.keep-history.override = DependencyRegistry, MyCustomHint
com.axeda.drm.scm. upload.url=http:// host_name.server_name. domain_type/upload	Software Management upload URL	The URL at which the Concentrator Remote Server accepts files uploaded by the Agents. This property is set when you run the Concentrator Remote Server Installer. The default setting is http://server.avaya.com:7002/upload.
com.axeda.drm.scm. upload.retry-count=3	Software Management upload retry count	The number of times that an Agent should try the upload operation.
com.axeda.drm.scm. upload.retry-min-delay= 1000	Software Management upload retry minimum delay	The minimum amount of time (in milliseconds) that the Agents should wait before retrying an upload.
com.axeda.drm.scm. upload.retry-max-delay= 10000	Software Management upload retry maximum delay	The maximum amount of time (in milliseconds) that the Agents should wait before retrying an upload.
com.axeda.drm.scm. upload.chunk-delay=0	Software Management upload chunk delay	The number of milliseconds for the Agents to wait before sending the next chunk of a file.
com.axeda.drm.scm. upload.chunk-size=1048576	Software Management upload chunk size	The number of bytes from a portion of a file to include in a single request.
com.axeda.drm.scm.upload.c hunk-timeout.threshold = 60	Software Management upload chunk timeout threshold (seconds)	The time elapsed, in seconds, since the last upload chunk after which the associated package will be marked as timed out.

This line	Sets the property called	Specify
com.axeda.drm.scm.upload.chunktimeout.threshold.cancelpaused = 60	Software Management upload chunk timeout threshold for canceling paused transfers (minutes)	Time elapsed in minutes since the last upload chunk after which the associated paused package will be canceled (minutes).
com.axeda.drm.scm.upload.sessionlength=43200	Software Management upload session length	The number of seconds that a file should be available for upload.
com.axeda.drm.scm.upload.compression-highthreshold=2147483648	Software Management high compression threshold for uploads	The size of a file (in bytes) to be uploaded that will result in content compression being disabled automatically. The default setting is 2 GB. You cannot specify a value larger than 2 GB. This setting overrides the file transfer options selected for a Software Management package or in an upload action configured in the Agent project when the file to be transferred exceeds this threshold.
com.axeda.drm.scm.download.url=http://*host_name.server_name.server_type*/download	Software Management download URL	The URL for the directory in which you want to store files downloaded from the server to an Agent. This property is set when you run the Concentrator Remote Server Installer. The default setting is http://server.avaya.com:7002/download.
com.axeda.drm.scm.download.retry-count=3	Software Management download retry count	The number of times that an Agent should try the download operation.
com.axeda.drm.scm.download.retry-min-delay=1000	Software Management download retry minimum delay	The minimum amount of time (in milliseconds) that the Agent should wait before retrying a download.
com.axeda.drm.scm.download.retry-max-delay=10000	Software Management download retry maximum delay	The maximum amount of time (in milliseconds) that the Agent should wait before retrying a download.
com.axeda.drm.scm.download.chunk-delay=0	Software Management download chunk delay	The number of milliseconds for the Agent to wait before requesting the next chunk of a file.

This line	Sets the property called	Specify
com.axeda.drm.scm. download.chunk-size=65336	Software Management download chunk size	The number of bytes from a portion of a file to include in a single request.
com.axeda.drm.scm. download.sessionlength= 43200	Software Management download session length	The number of seconds that a file should be available for download.
com.axeda.drm.scm. download.compression- highthreshold= 2147483648	Software Management high compression threshold for downloads	The size of a file (in bytes) to be downloaded that will result in content compression being disabled automatically. The default setting is 2 GB. You cannot specify a value larger than 2 GB. This setting overrides the file transfer options selected for a Software Management package or in a download action configured in the Agent project when the file to be transferred exceeds this threshold.
com.axeda.drm.scm. validate-ip-address=false	Software Management validate IP	True to validate the IP addresses of devices when transferring files, or false (default) to transfer files without validating the IP addresses.
Snapshot status configuration		
com.axeda.drm.entity. snapshot.SnapShotStatus. levels=4	Snapshot status levels	The number of status levels to configure. Each status is identified by four values, followed by a number. The priority of the level is identified by the number at the end of the tag (0 is lowest priority). If a snapshot entry has no status, it is assigned the status identified by level 0 (the default).
com.axeda.drm.entity. snapshot.SnapShotStatus. name_*X*=	Snapshot status 0 Snapshot status 1 Snapshot status 2 Snapshot status 3	The string in the snapshot XML file that will identify the level. The following levels are defined in the file: • name_0 = ok • name_1= info • name_2 = warning • name_3 = error
com.axeda.drm.entity. snapshot.SnapShotStatus. image_*X*=	Snapshot status image 0 Snapshot status image 1 Snapshot status image 2 Snapshot status	The image to display when an entry has the level specified by the name. The following images are defined in the file: • image_0 = snapshot_status_ok.gif • image_1 = snapshot_status_info.gif • image_2 = snapshot_status_warning.gif • image_3 = snapshot_status_error.gif

This line	Sets the property called	Specify
	image 3	
eMessage error handling instruction		
com.axeda.drm.entity. device.communication. MessageContext.interval= 120	Device communication maintenance ping rate	The number of seconds that the Agent will wait between sending maintenance pings to the Concentrator Remote Server.
com.axeda.drm.entity. device.communication. MessageContext.url=	Device communication maintenance ping agent url	The URL where you want the Agents to send their maintenance pings (when the Concentrator Remote Server has placed them in the maintenance mode).
com.axeda.drm.entity. device.communication. MaintenancePingContext. url=Remote Server url	Device communication maintenance ping redirect Concentrator	The URL of the Concentrator Remote Server to which the Agent maintenance pings are being redirected.
com.axeda.drm.entity. device.communication. MaintenancePingContext. owner=drm-data_source	Device communication maintenance ping owner	The JNDI name of the data source as configured on the Concentrator Remote Server to which Agent maintenance pings are being redirected.
com.axeda.drm.devcon. maintenanceping. MaintenancePingManager. delay=1	Device communication maintenance ping delay	The number of minutes to wait between maintenance pings.
com.axeda.drm.devcon. maintenanceping. MaintenancePingManager. enable=true	Device communication maintenance enable flag	True to enable the maintenance ping manager or false to disable it.
eMessage processing notification e-mail		
com.axeda.drm.devcon. notification. DevconNotificationManager. interval = 2	Device communication notification interval in minutes	The number of minutes to wait before sending an e-mail message to the server administrator. Leaving the parameter blank or specifying a negative number disables the property completely. The e-mail address used is that defined in com.axeda.drm.administrator.email
com.axeda.drm.devcon. notification. DevconNotificationManager. displaySource = true	Device communication notification display source	True (default) to enable notifications sent to the server administrator to identify the source of the errors (for example, an XML posting from a specific agent); false (or blank) to prevent notifications from showing the source of the error.
com.axeda.drm.devcon. notification. DevconNotificationManager. maxEmailLength=10000	Device communication notification maximum e-	The maximum number of bytes for an e-mail message. The default value (10000) limits the size of e-mail messages to 10K. To allow unlimited length messages, use a setting of -1.

This line	Sets the property called	Specify
	mail length	
Lightweight Ping servlet		
`com.axeda.drm.devcon.lwping.enabled=true`	Lightweight Ping servlet enabled	True (the default) to enable the ping servlet; false to disable the ping servlet.
`com.axeda.drm.devcon.lwping.servlet.secure=`	Lightweight Ping servlet uses HTTPS	True to make the ping servlet accessible through HTTPS. False to use HTTP. If unspecified, the Agents use the communication protocol defined for the main message servlet.
`com.axeda.drm.devcon.lwping.servlet.host=`	Lightweight Ping servlet host	The IP address or hostname of the ping servlet. If unspecified, the Agents use the same IP/hostname defined for the main message servlet.
`com.axeda.drm.devcon.lwping.servlet.port=`	Lightweight Ping servlet port	The port number of the ping servlet. If unspecified, the Agents use the port defined for the main message servlet.
`com.axeda.drm.devcon.lwping.servlet.path=/lwPing`	Lightweight Ping servlet port path	The path of the ping servlet on the server. The default is /lwPing.
Forced ping		
`com.axeda.drm.devcon.forced-ping-interval=3600`	Forced ping interval (in seconds)	The maximum amount of time allowed for a managed device to be silent (that is, not sending messages). Normally, when a managed device has no data to send, the Agent managing that device sends a brief ping message based on a configured ping rate. However, if a managed device is deleted on the Concentrator Remote Server and the agent sends no data for that device, the device becomes hidden such that it exists, from the agent's perspective, but is not visible in the Concentrator Remote Server. **Note:** To make a hidden device reappear, the agent must send an explicit message (a forced ping) on behalf of the device, so that the Concentrator Remote Server can re-register it.
Parent server		
`com.axeda.drm.parent-server.post-rate=30`	Server to Server post rate	The rate, in seconds, at which to send out the queue of messages to the parent server. This defines how often the child server takes the list of messages that have queued up and sends them up using HTTP to the parent server.
`com.axeda.drm.parentserver.ssl.verifyhostnames`	Server to Server verify	True to force this Concentrator Remote Server to reject certificates if the hostname in the

This line	Sets the property called	Specify
`= true`	host name	certificate does not match the parent server name; false for the Concentrator Remote Server not to check certificates against the hostname.
`com.axeda.drm.parentserver.ssl.strictcertificate-verification = true`	Server to Server validate SSL certificate	True for this Concentrator Remote Server to validate strictly all SSL certificates; false for the server to accept any certificates
Enhanced select lists		
Enhanced select lists enable you to select from very large data sets in a practical way. They also retain an MRU list, making each select list more efficient to use. When an enhanced select list is in enhanced mode, it means that you can access any items that are not displayed in the first max-lines-displayed items shown in a popup window.		
`com.axeda.drm.enhancedselect – list.mru-size=9`	MRU size	The number of items to store in an MRU list.
`com.axeda.drm.enhancedselect – list.max-linesdisplayed=11`	MRU maximum lines	The maximum number of lines to display when a select list is in enhanced mode.
`com.axeda.drm.enhancedselect – list.popupthreshold=35`	MRU popup threshold	The number of lines that cause the system to shorten the list to the value specified for maxlines-displayed. When the number of items in the select list is greater than or equal to this value, the system shortens the list to max-linesdisplayed and the list uses enhanced mode.
Numeric data value		
`com.axeda.drm.data. numeric.truncate-trailing-zeroes=false`	Truncate trailing zeros for Numeric Data	True to truncate trailing zeroes after the decimal point for numeric data, or false to preserve all trailing zeroes for numeric data.
Service application tree		
`com.axeda.drm.webapp. service.tree. status-aggregator= com.axeda.drm.webapp. service.browse. MostSevereStatusAggregator`	Service Application tree status aggregator	The device status condition that *bubbles up* through the hierarchy for quick viewing. By default, this is the *most severe* status. Do not change this value without the assistance of Avaya Technical Support.
`com.axeda.drm.webapp. service.tree. max-children=50`	Service Application tree maximum children	The maximum number of nodes that the Service application displays in its tree.
Global default chart		
`com.axeda.drm.charting. global-default-chart= History Chart`	Default chart	The chart that you want to display as the default chart for data. Other settings include: • Default History Chart • Default Live Chart • Default History Comparison Chart • Default Bar Comparison Chart

This line	Sets the property called	Specify
Cache parameters		
`com.axeda.drm.cache.expiry-invalidator.interval=60`	Cache expiration frequency (seconds)	The number of seconds that the expiry invalidator waits between runs of its invalidator. The default is 60 seconds (1 minute).
`com.axeda.drm.cache.devices=50000`	Not displayed in Administration application	The number of devices to keep in the device cache. The default is 50000 devices.
`com.axeda.drm.cache.dataitems=10000`	Not displayed in Administration application	The number of data items to keep in the dataitem cache. The default is 10000 data items.
Undefined information		
WAAG timeout		
`com.axeda.drm.waag.timeout=30`	Not displayed in Administration application	The number of seconds that WAAG waits between updates of the display.
AES Max Ciphers pool		
`com.axeda.drm.aes_ciphers_pool.max=15`	Not displayed in Administration application	The maximum number of ciphers available from the cipher pool.
`com.axeda.drm.aes_ciphers_pool.min=0`	Not displayed in Administration application	The minimum number of ciphers available from the cipher pool.
Data export configuration		
`com.axeda.drm.dataexport.date-format=`	Date format	A date format for the system to use, using Java date format strings. By default the data export uses the date format specified by the user's locale. If the user has not specified a locale, the server's default locale is used. For details on date format strings, see the JavaDoc for `java.text.SimpleDateFormat`
Recent action statuses		
`com.axeda.drm.services.agent.status.days-topersist=3`	Days to persist statuses in database	The number of days that the server should maintain device command statuses in the database. Statuses older than this number of days will be deleted automatically from the database. The default number of days is 3.

This line	Sets the property called	Specify
Automatic acknowledgement of alarms		
`com.axeda.drm.services.archive.days-before-acknowledge-alarms=-1`	Days before alarms are acknowledged	The number of days after which all alarms will be acknowledged automatically. A number less than 1 (the default, -1) indicates that alarms are not to be acknowledged automatically.
User Manager		
`com.axeda.drm.services.users.sent-email = true`	Not displayed in Administration application	True (default) to send a welcome e-mail message to a user that has just been created, or false to not send such an e-mail message.
Web services		
`com.axeda.drm.webservices.session.timeout = 60`	Not displayed in Administration application	The number of seconds before an inactive Web service session is timed out. The default value is 60 seconds.
SDK		
`com.axeda.drm.sdk.startupfile = custom-startup.xml`	These properties are not displayed in Administration application	The name of the XML file that contains your custom startup or scheduled tasks.
`com.axeda.drm.sdk.actionsfile = custom-actions.xml`		The name of the XML file that contains your custom action definitions.
`com.axeda.drm.sdk.rulesfile = custom-rules.xml`		The name of the XML file that contains your custom rule definitions.
Enable/disable Windows Update functionality		
`com.axeda.drm.enable.update_window=false`	Not displayed in Administration application	True to enable the Windows Update functionality; false (default) to prevent Windows from automatically updating the computer. **Note**: Avaya recommends that you ignore this parameter as the remote server does not handle alarms.
Max. items to display for submenu items		
`com.axeda.drm.webapp.service.menu.max-submenu-items = 10`	Not displayed in Administration application	The maximum number of items to display on a submenu in the Service application. The default maximum number is 10.
Enable/Disable Soundex on Device Search Soundex and wildcard searching is supported for the following fields Service application and dashboards: Device (Solution Element / Asset Id), Functional Location, Account, and Device Name.		
`com.axeda.drm.soundex.enabled=false`	Enable Soundex Feature	False (default) to disable Soundex functionality for searching for and displaying data; true to enable the server to implement Soundex functionality when searching the database.
Device updates		
`com.axeda.drm.transport-servicelink.export.root =`	Device Updates export root	The server directory to which the server saves the tar .gz file intended for export to a specified

This line	Sets the property called	Specify
`$USER_INSTALL_DIR$/scm/export`		device during an Transport - Export session. This file contains all queued server commands and eMessages, as well as any pending actions or download instructions for the device. The file for export is stored in a new subdirectory named for the export session. In a clustered environment, all managed servers must reference this directory via Samba UNC or NFS mount points. (NFS mount points is the recommended method.) (Clustering is not supported for this release.)
`com.axeda.drm.transport-servicelink.import.root = $USER_INSTALL_DIR$/scm/import`	Device Updates import root	The server directory to which the server will save files imported from a specified device during an Transport - Import session. The server store the imported file to a new subdirectory named for the import session. In a clustered environment, all managed servers must reference this directory via Samba UNC or NFS mount points. (NFS mount points is the recommended method.) (Clustering is not supported for this release.)
Smart suggest Many combo boxes in the Service, Case, and Preventative Maintenance Applications implement Smart Suggest, which provides automatic completion functionality. When a single character is typed in the Device search combo box, for example, the server will retrieve a predefined number of device names that match that character (the top x device names available). While the user is typing additional characters, the system will retrieve more device names that match the updated character set, but only based on a predefined interval (in milliseconds).		
`com.axeda.drm.smartsuggest.interval=1000`	Smart Suggest Interval	The interval at which the server searches the database using the currently specified search values. As the user types characters, the server updates the list of returned strings at a frequency defined by this setting. The default value, 1000 milliseconds, causes the server to query the database every 1000 milliseconds (1 second) using the currently specified search characters.
`com.axeda.drm.smartsuggest.maxlistsize =10`	Smart Suggest max list size	The number of records that the server shows in the list of returned strings. The default value is 10 records.
Agent version default name		
`com.axeda.drm.agentversion = Pre3.8`	Default Agent version	The version of the Agent to display in the Device dashboard of the Applications UI. If the agent version value is not available in the Concentrator Remote Server system, the server displays the agent version defined in this

This line	Sets the property called	Specify
		property. By default, the value is set to Pre 3.8.
Huge file upload		
com.axeda.drm.file.upload.applet.ping.interval	Not displayed in Administration application	Ping interval time is used when network is down. After every specified interval (default is 30 seconds), the user's browser will ping the Concentrator Remote Server to check the availability of the network. The default value is 30000 milliseconds (30 seconds). When setting this value, make sure it is less than the SAL server session-timeout value defined in the web.xml (drm/WEB-INF/web.xml).
com.axeda.drm.file.upload.applet.ping.count	Not displayed in Administration application	Defines the total time period used by the pinging process when checking for the network connection. The default count is 36. This count value is related to session-timeout value set in the web.xml file, Guidelines to set this value When setting this value, make sure the multiplied value of the Ping interval (com.axeda.drm.file.upload.applet.ping.interval) and the Ping count is LESS than the session-timeout value (defined in the web.xml file). In other words, *Ping Interval * Ping count < Secure Access Link session timeout*>. If the resulting product is not less than the value of the SAL session timeout property, then the server will set the automatically as follows: *Ping count = Secure Access Link session-timeout /Ping interval*
com.axeda.drm.file.upload.applet.chunk.size	Not displayed in Administration application	Identifies the size of data chunk that will be sent to the server in every request. The default is 5242880, or 5 MB, where 5*1024*1024 = 5242880. The minimum size is 1 MB Minimum size is 1 MB (1*1024*1024 = 1048576). The maximum size is 20 MB (20*1024*1024 = 20971520).
Access enhancements		
com.axeda.drm.remote.session.use-internal-access=false	Not displayed in Administration application	Defines whether or not to use the internal access server for starting the remote application session. By default (false), the internal server is not used. Change to true to use the internal server.

This line	Sets the property called	Specify
com.axeda.drm.remote.session.use-internal-access.show=false	Not displayed in Administration application	Defines whether or not the server will display the Use Internal Access check box in the Start Remote Application Session window displayed when the user selects to start a remote session.
Device Dashboard File Comparison utility		
com.axeda.drm.file.compare.maximum.size	Not displayed in Administration application	Identifies the maximum size of a file for comparison using the Text File Comparison utility (Service application - Device dashboard - Uploaded Files module. This value is in MB (Megabytes). The default value is 3 MB.
Audit Log settings (Syslog Server settings)		
com.axeda.drm.audit.auditor.multiple-auditor-types=	Additional Auditor types actively running in the system	Registers the types of auditors to use along with the JDBC Auditor when dispatching audit messages. The supported values for this property are: • AUDITOR_SYSLOG_SERVER (support for both Syslog and JDBC Auditors) • <blank> (support for JDBC Auditor only) **Note:** Configuration properties for the syslog server, such as host and port number, syslog facility id, and message format template can be specified in the log4j.appender.SYSLOG definition of the log4j.properties file. This file is located in the config directory of the SAL installation; by default, /avaya/SAL/CRS/config.

This line	Sets the property called	Specify
`com.axeda.drm.audit.auditor.filter-categories=`	Audit Categories allowed for auditing (no value means all Audit Categories are allowed)	Registers the types of audit categories that will be dispatched to the defined auditors. If no types are defined, or if the property is missing altogether, no filtering will be performed and, therefore, *all* messages will be dispatched. (For this release, the audit category filtering is supported for Syslog server auditors only.) The following categories are supported for auditing: • dashboard • data-export • data-management • device-communication • file-upload • maintenance • network • notification • partner-access • report • scm-file-transfer • scm-package-management • transport-servicelink • update-window You can specify multiple categories in a commaseparated list. For example, the setting `com.axeda.drm.audit.auditor.filter-categories=data- export, file-upload, notification` will cause the Concentrator Remote Server to dispatch all data export, file upload, and notification audit messages to the specified Syslog server. (In addition, all audit messages of all types will be dispatched to the JDBC auditor.)

Appendix D: Site Preparation Utility

This appendix introduces Site Preparation Utility, an applet provided with the Concentrator Remote Server to aid in troubleshooting Agent to Concentrator Remote Server connections and communications. Complete information for using Site Preparation Utility is provided in the online help supplied with the applet.

Overview provides an introduction to Site Preparation Utility.

Running Site Preparation Utility explains how a remote user will start and run Site Preparation Utility.

How the Utility Works explains how Site Preparation Utility communicates with defined servers, tests the connections, and relays that information back tot the user. Also explains any problems that may occur during communications and the Log file created with configuration and communications information.

Overview

The Site Preparation Utility is a signed applet provided by Secure Access Concentrator Remote Server. Groups of users, technicians, and support personnel can use this utility to assist with troubleshooting connection and communications issues between Agent and other components of the SAL system, including Concentrator Remote Server, registered Secure Access Global Servers, and configured proxy servers. As long as the local computer has a network connection and can browse the Internet, it can use Site Preparation Utility. This utility works with Agent software, version 3.8.x or later, Concentrator Remote Server, JRE version 1.5 or later.

Remote users access the applet, and select or define the configurations they want to test. The applet accesses the local system resources and tests the selected settings and component connections. It captures the pertinent information from that computer and displays it in the UI. A user can save this information to file for later review, or send it to a support technician, who can load that file in his or her local browser to troubleshoot issues with that remote user's computer or connections. Remote users must have access to that Concentrator Remote Server as well as Applications log in privileges to that server.

For information on using the Site Preparation Utility, see the online help documentation available from the Site Preparation Help menu.

Server support for the Site Preparation Utility

By default, the Concentrator Remote Server installation application installs the Site Preparation Utility to the directory *sitepreputility* at the following server installation location:

- for Linux: into the drm.war, in the servicelink.ear (*<JBoss_HOME>/server/<SAL Install>/deploy*)

Session timeouts

The *<session-timeout>* value defined in the *web.xml* file for the Concentrator Remote Server controls when the user's Site Preparation Utility session times out. By default, this value is set at 10 minutes. When the user has not used the Site Preparation Utility for the amount of time defined by the *<session-timeout>* value, the Concentrator Remote Server closes the applet's session. Note that this timeout will occur even if the user is actively running diagnostics.

Configuring users for the Site Preparation Utility

Only individuals with privileges within Applications can run Site Preparation Utility. These individuals need login privileges only. They do not need the ability to perform operations within the Applications. These users need to be defined in the directory service used by the SAL server.

Running the Site Preparation Utility

After restarting, you should determine that the Site Preparation Utility was installed correctly. To do so, you need to have a valid login account for the Applications.

To verify the installation, open a Web browser and browse to the following Concentrator Remote Server URL:

<http/https>://<concentrator_remote_server_ip_address>:<port>/drm/sitepreparationutility

Replace *<http/https>* with either http or https (depending upon Concentrator Remote Server setup), and *<concentrator_remote_server_ip_address>:<port>* with the IP address and listening port for the Concentrator Remote Server.

The Site Preparation applet will load in your browser and appear similar to the following:

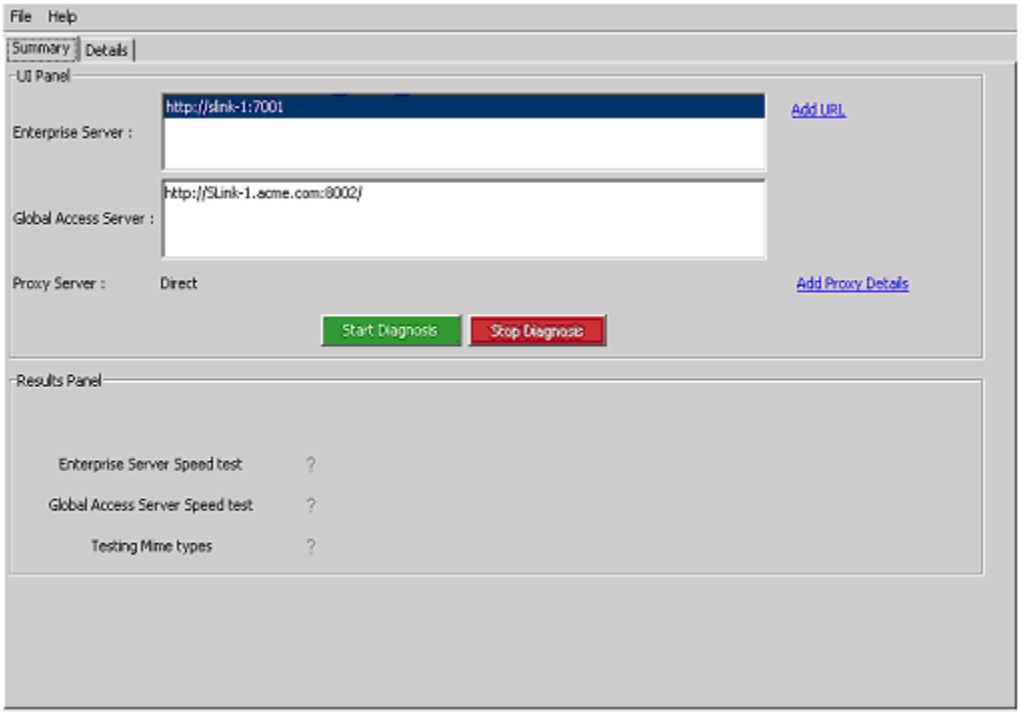


Figure E-1: Example Site Preparation Utility UI

Note:

The Web browser must be running JRE version 1.5 or later for the Site Preparation Utility. If the browser is running with an earlier JRE of version (that is, earlier than version 1.5), a message similar to the following appears:

```
Your browser's Java plug-in is not compatible with this application.
Please install the latest version from the Sun Web site.
```

If the Web browser is not configured with any JRE or the configured JRE is earlier than version 1.4, a message similar to the following appears:

```
Your browser's Java plug-in was not found or in not compatible with
this application. Please install the latest version from the Sun Web
site.
```

You need to upgrade your Java Plug-in (or Java Runtime Environment) version to a supported version.

How the utility works

To run the Site Preparation Utility, a user with login privileges to the Applications types the URL to the utility as directed in Running the Site Preparation Utility. After logging in, the utility appears in the browser window.

When the utility appears, you can see that the Concentrator Remote Server that is running the Site Preparation Utility is defined for testing by default. You can remove this server and add another, as needed. You select the connections to test, specifying an Concentrator Remote Server connection, one or more Global Access Server connections, and proxy server configurations. As you add URLs for Concentrator Remote Servers, the utility tries to connect to them. If a server is not running or the utility cannot connect to it, the utility displays an error similar to the following:

```
Could not connect to the server.
Please enter a valid URL or check your network connection.
```

After specifying the Concentrator Remote Servers you want to test, select the Start Diagnostics button. The utility calls the poptimize servlet of the selected Concentrator Remote Server to perform the speed test. The utility establishes a HTTP or HTTPS connection to the poptimize servlet by sending and receiving data from the Concentrator Remote Server. The results of the tests are displayed in the browser window. If you need to send the results to a support technician, you can save the test results to a file.

Proxy server support

The Site Preparation Utility supports the Basic and Digest authentication schemes for testing. An error message similar to the following appears if you attempt to test an unsupported proxy server authentication scheme (that is, those configured with the NTLM scheme):

```
You have selected to test an NTLM proxy server.
Site Preparation Utility does not support the NTLM authentication scheme.
Please select to test either a Basic or Digest proxy server, or leave at
Direct.
```

The utility log file

When launched, the Site Preparation Utility creates the log file, *sitepreparationutility.log*.

- If you run the utility using Internet Explorer as the browser, the file is created on the browser desktop.
- If you run the utility using Mozilla Firefox as the browser, the file is created in the directory, *C:\Program Files\Mozilla Firefox* (for supported Windows platforms; this will be different for Linux).

The *sitepreparationutility.log* file identifies the start date and time of tests as well as the progress and results of those tests. In addition, connection timeouts and other issues are saved in this file for reference.

Glossary

2FA	2 Factor Authentication. A system wherein two different authentication factors (piece of information and process) are used in conjunction to authenticate or verify the identity of a person or other entity requesting access under security constraints. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance. Two-factor authentication typically is a signing-on process where a person proves his or her identity with two of the three methods: something you know (for example, password or PIN), something you have (for example, smartcard or token), or something you are (for example, fingerprint or iris scan).
API	Application Program Interface. A source code interface that an operating system or library provides to support requests for services to be made of it by computer programs.
CAS	Converged Application Server. A combination of the Avaya Ubiquity SIP Servlet Container and a J2EE Container for the development of SIP-based applications. The J2EE container is RedHat JBoss. (Previously known as SDP.)
CLI	Command Line Interface. A computer program that reads lines of text entered by a user and interprets them in the context of a given operating system or programming language.
GSD	Global Services Delivery.
GPSS	Global Product Support Solutions.
INADS	Initialization and Administration System. Used by Avaya Services personnel located at the Technical Service Center (TSC) to initialize, administer and troubleshoot customer communications systems remotely. The INADS alarm format identifies the device from which the alarm was generated.
IP INADS	An INADS alarm string that is transported from an alarming system or proxy over TCP/IP to an INADS receiver. Typical receivers of IP INADS include the SSG, SIG and SPIRIT Agent.
IPINADS CMS	IP INADS alarms from CMS.
IPS	Internet Proxy Server.
J2EE	Java Platform, Enterprise Edition. A widely used platform for server programming in the Java programming language offering additional libraries which provide functionality to deploy fault-tolerant, distributed, multi-tier Java software, based largely on modular components running on an application server.
JBoss	The JBoss application server is a range of application servers and software that implement Java Enterprise Edition-related standards. JBoss is a product of RedHat.
JEE Cluster	JEE Cluster. A group of loosely coupled Java-based servers that work together closely so that in many respects they can be viewed as a single server.
MSP	Maintenance Service Provider.
NMS	Network Management System. A management system, usually an SNMP management application that provides management capabilities for networked hosts and other managed elements. Examples of NMS include HP OpenView, IBM Tivoli and Netcool.

Panther	Management interface of the CAS. Panther fulfils the OAMP requirements for the CAS platform. Panther provides capabilities that applications making use of the CAS can take advantage of to produce a consistent management interface across all Avaya and 3rd-party products that use the CAS.
SDP	Service Delivery Platform. A combination of the Avaya Ubiquity SIP Servlet Container and a J2EE Container for the development of SIP-based applications. The J2EE container is RedHat JBoss. Now known as CAS.
SEAR	Secure Enhanced Alarm Receiver. The original name of the SPIRIT Agent Alarm Component that supports the functions of alarm management.
SIP AS	Session initiation protocol (SIP) application server (AS). a Java SIP servlet container implemented by Ubiquity, an Avaya company.
SNMP	Simple Network Management Protocol. Exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.
SNMP INADS	An INADS alarm string which is transported within an SNMP trap.
SOA	Service-Oriented Architecture. An evolution of distributed computing and modular programming. SOAs build applications out of software services. Architecture relies on a business process expert to link and sequence services in a process known as orchestration, to meet a new or existing business systems requirement.
SPIRIT	Former project name for Secure Access Link. Acronym meaning **S**erviceability through **P**roduct **I**ntegrated **R**emote **I**ntelligent Agents and **T**ransport
SSO	Single Sign-On. A system to minimize the number of times a user must log into multiple applications.