



Avaya Operational Analyst

Security Guide

Release 7.3.x

July 2021

© 2021 Avaya Inc

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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 to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, <http://support.avaya.com/LicenseInfo> under the link "Avaya Terms of Use for Hosted Services" or such successor site as designated by Avaya, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/LicenseInfo),

UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" or such successor site as designated by Avaya, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in Section M(i)1 or 2 as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo/> under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya

including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com)

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE

AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company’s behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Contents	3
Preface	5
Audience	5
Related documents	5
Availability	5
Introduction	6
Assumptions	6
Authentication and group membership	6
Pre-installation configuration	7
User IDs	9
Administration and reporting User ID creation	9
Windows	9
Solaris and AIX	9
Administration and reporting groups	9
Creation	10
Maintenance	10
ADS groups support	10
How to determine the fully distinguished name of ADSgroups	10
Alternate domain name support	13
ADS groups: what to do in case of error	13
User ID policy guidelines	14
Length	14
Lockout	14
Password reuse	15
Composition (alpha/numeric)	15
Root and Administrator privileges	15
Uniqueness	15
Creation	15
Database user ID and passwords	15
Changing database passwords for SQL Server 2008 R2 64-bit and Oracle	15
Changing database passwords for DB2	16
Changing Informix password on a CMS Solaris host	16
File permissions	17
Directory access on Solaris and AIX	17
Process owners on Solaris and AIX	17

Windows access and run permissions.....	17
Running scripts on AIX	17
Log/audit file	19
Audit content	19
Location on Solaris and AIX	19
Location on Windows.....	19
Policies.....	19
Size	19
Conservation.....	19
Access	19
Installation audit.....	19
Data privacy	20
What is protected.....	20
How it is protected	20
Third party software security.....	21
Oracle.....	21
SQL Server 2008 R2 64-bit.....	21
DB2	21
Times Ten	21
Tomcat for Windows, Solaris, and AIX	21
Remote access (PC Anywhere).....	21
Additional customer responsibilities	22
OS updates	22
Third party advisories and patches	22
Virus protection	22
Firewall.....	22
OS level IP-Filtering	22
Sub-interfacing.....	24
Loopback of ports	24
Data privacy	24
Limit access to this document.....	25
Index	26

Preface

This section contains the following topics:

- [Audience](#)
- [Related documents](#)
- [Availability](#)

Audience

This guide is intended primarily for system administrator who is responsible for configuring and administering Avaya Operational Analyst.

Related documents

The following documents in the Operational Analyst Release 7.3.x documentation set are related to this Security Guide:

- Avaya Operational Analyst Release 7.3.x Installation Planning and Prerequisites
- Avaya Operational Analyst Release 7.3.x Operational Analyst Installation and Configuration
- Avaya Operational Analyst Release 7.3.x Operational Analyst Maintenance and Troubleshooting

Availability

You must keep this document under tight control.

This document describes security features of the Avaya Operation Analyst 7.3.x product and is a potential security risk if distributed to a wide audience.

Introduction

The topics discussed in this document are to be used as guidelines to the system administrators responsible for the security of the servers where Avaya OA 7.3.x is installed. This is not an exhaustive list of security measures to follow by administrators to manage their network of computers as a whole. It focuses on the security considerations related to the Avaya OA 7.3.x software.

Assumptions

This document assumes that the reader is familiar with Windows, AIX and Solaris system administration, especially user and group management. It also assumes that the reader is familiar with the OA architecture (what it does, where the components are installed).

Authentication and group membership

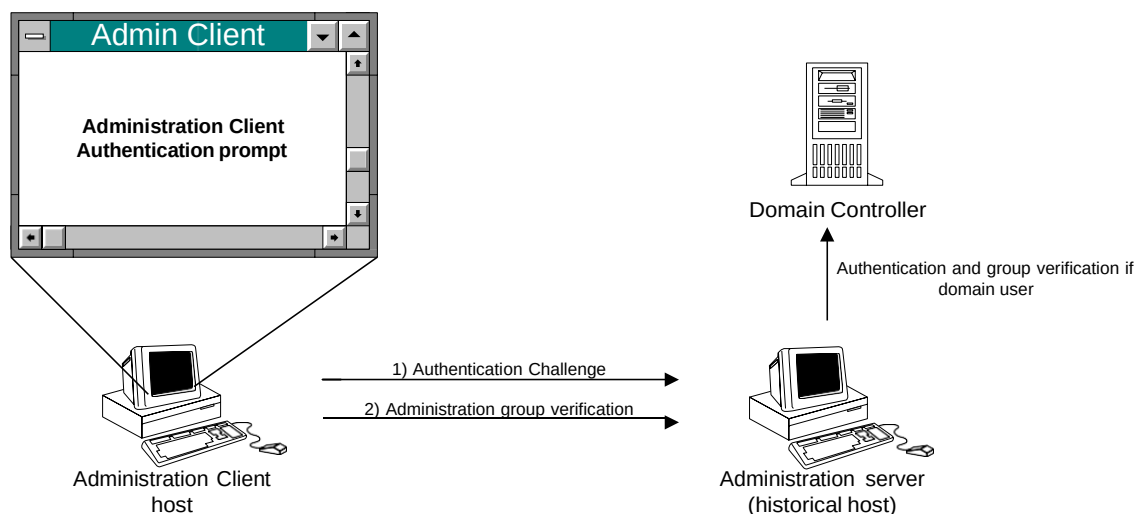
The authentication of administration users and report users is done using the underlying Operating System (OS) mechanism on Windows, AIX and Solaris. User ID, passwords and groups are managed using OS off-the-shelf tools. This capability simplifies user administration as the system administrator uses familiar tools to setup users. Also, OS security policies can be taken advantage of, such as password re-use and expiration. This also offers a single point to administer network and OA users.

Pre-installation configuration

Prior to installing OA, user ID and groups must be defined to access OA components and databases. Reference [1] explains in detail how to create database users and reference [2] explains how to use them in the OA context. These documents explain how to create OS user ID and groups to access the administration client and the operational reports.

OA uses two groups of users to access its components: the administration group and the report group. The system administrator must add these groups. The existence of these groups is verified by the OA installation software as described in [2]. If they are not present, the OA software cannot be installed. The OA software does not predetermine the groups. The system administrator can decide to use groups that already exist or create new ones. The only restriction is that those groups must match the groups entered by the administrator in the OA installation program. The OA runtime components will know based on the installation input, which group to use for administration and which for reporting.

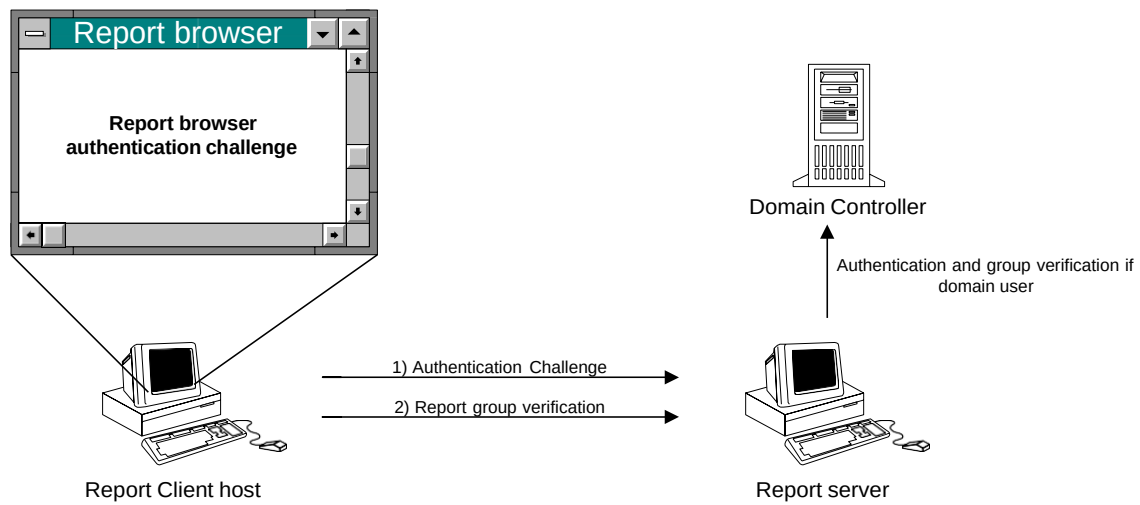
The administration group is used by the OA administration client to verify whether users have administration privileges. Note that this group is not the same as the Administrators group on Windows. Windows actually prevents us from using the Administrators group for this purpose so you must use a different group for OA administration. The diagram below shows what happens when the administration user tries to connect to the administration server.



1. The user's user ID and passwords are encrypted on the administration client host and then sent to the Administration server. They are decrypted on the server. If the configured administration group is an ADS name, the authentication is performed against the domain controller. If locally defined, it is done on the OA Administration server.
2. If the user is authenticated, the administration client requests group membership verification. The administration server verifies that the user belongs to the administration group as configured via the OA installation program. Like the authentication, the administration server will forward the request to the domain controller based on the configured ADS group name.

Similarly, the report browser will present a user ID and password challenge to the report user. The picture below represents the authentication and group membership process for reporting.

The flow of data is the same for the report users except that the group verification is performed every time that the report screen refreshes.



User IDs

Administration and reporting User ID creation

The following recommended policies should be implemented using the OS tools:

- Password aging
- Password reuse
- Password length
- Password composition (alphanumeric)

Windows

Users IDs are created using Windows tools. On Windows, the user management tool, from the Administrative tools menu, can be used to create the new user IDs. Refer to the Windows documentation for details on how to create user IDs. Once the IDs are created, they must be added to the administration group or the report group (or both), based on the role of the user.

Note: The user IDs and group IDs must be created on the same host. For example, if the group name is defined on the ADS, the user must also be defined on the ADS. If the group is defined on the local host (localhost), the user must also be defined on the local host.

Solaris and AIX

User IDs are created using Solaris and AIX tools. For example, the `useradd` command can be used. Refer to the Solaris and AIX documentation for details on how to add user IDs. Similarly to Windows, the users must be added to the groups that the system administrator defines for OA administration or reporting.

Administration and reporting groups

The OA administration group is a user group that has access to the administration client functionality. Only members of this group will be able to access the administration client. This group is also used to run the OA server processes. All processes except the authentication server (`autserver`), `initrv`, and `MOM` run as the OA administrator. The members of the OA administrators group can do the following tasks:

- Access the administration client
- Read the OA log files
- Start and stop OA components via the `pa` command
- On Windows, start and stop OA services such as Stumbras and the Avaya Business Intelligence Service

The OA reporting group is a user group that has access to OA real-time and historical reports. Only users of that group will be able to view reports.

Remarks:

- A user can be a member of both the OA administration and reporting groups
- On Windows, the Administrators group cannot be used for either the OA administrators group or the reporting group (this is a Windows limitation)

- On Windows, the groups, similarly to users, can be managed at the domain level (using the ADS) or on the local servers
- The user IDs and group IDs must be created on the same host. For example, if the group name is defined on the ADS, the user must also be defined on the ADS. If the group is defined on the local host (localhost), the user must also be defined on the local host.
- On Solaris and AIX, the groups, similarly to users, can be managed via the NIS or locally

Creation

The groups must be created before the OA system is installed. They are created using OS tools such as the Computer Management on Windows or the **groupadd** command on Solaris and AIX.

Maintenance

Users can be added or removed from these groups to allow or deny access to OA administration or reporting. The change will take effect the next time the user connects to either the OA administration client or the OA reports.

ADS groups support

Authentication and authorization has changed for the administration client and reports on Windows. Group membership is now verified against the Active Directory Service (ADS) and authentication does not require a domain name. When logging on to the administration client and reports, only enter the user ID instead of the previous <domain>\<userID> format. This change also supports locally administered groups and users (not on a domain, on the server where the OA Historical subsystem is installed).

This change only applies to Windows. It allows you to create logical Organizational Units (OU) to structure security principals. For example, instead of **"telcolab\oaadmin"**, the fully qualified name of the administration group in the Telco development lab could be:

- CN=oaadmin,CN=Users,DC=telcolab,DC=telco,DC=com

Another example would be a report group that looks like:

- CN=oarpt,DC=telcolab,DC=telco,DC=com

The following are examples of administration and report groups using an OU:

- CN=DenverAdmins,OU=Denver,DC=telcolab,DC=telco,DC=com
- CN=DenverReports,OU=Denver,DC=telcolab,DC=telco,DC=com

Note that even if these names seem to be organized in a tree structure, ADS requires that the Common Name (CN) is unique for the whole directory. In addition, a directory is also known as a "forest". If using local groups and users, the groups are specified like this in *autserver.properties*: *localhost\<GroupName>*.

How to determine the fully distinguished name of ADS groups

- **From network administrator**

The network administrator added groups and users to the ADS and should be able to provide the fully qualified name of the groups used for OA administration and reporting.

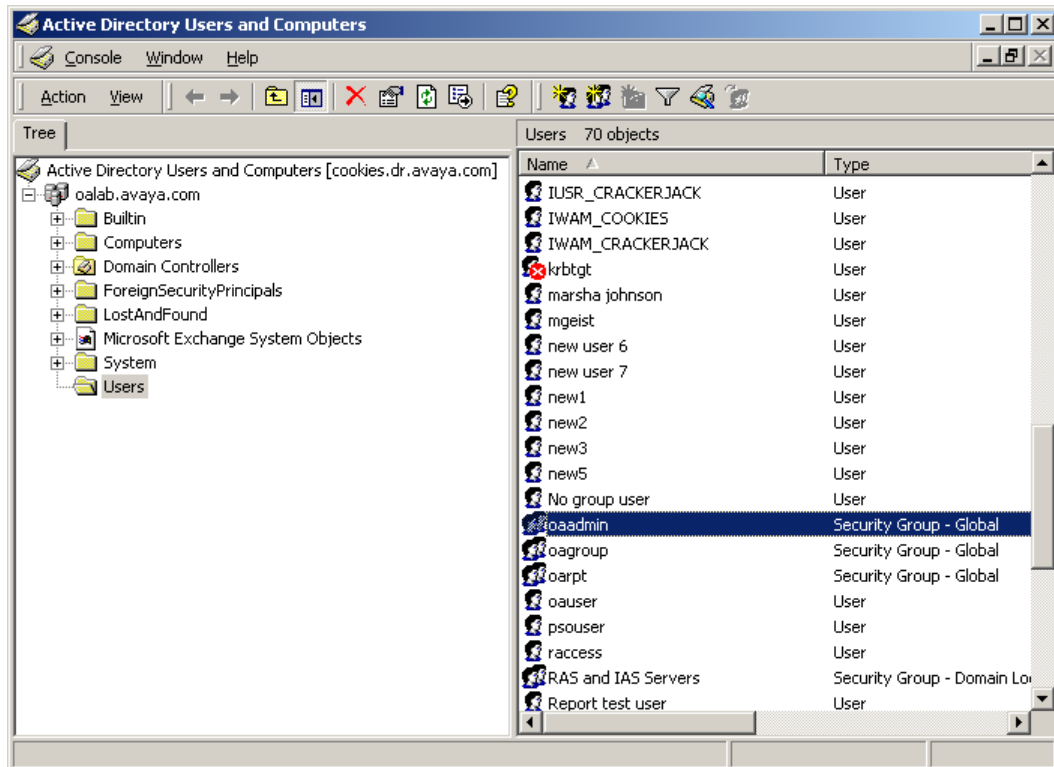
- **Guessing with user/group management tool**

The Active Directory user/group management tool is where groups and users are added and maintained. This tool can be run from the domain controller. The left panel of that tool shows a tree that allows you to

browse the list of groups and users. Typically, the root of the tree represents the fully qualified Domain Controller (DC) name. Then, browsing down to the OU or the default *User Distinguished Name (DN)*, you can determine the fully qualified name of the administration and report groups. In the picture below, the fully qualified name of the administration group is:

CN=oaadmin,CN=users,DC=oalab,DC=avaya,DC=com

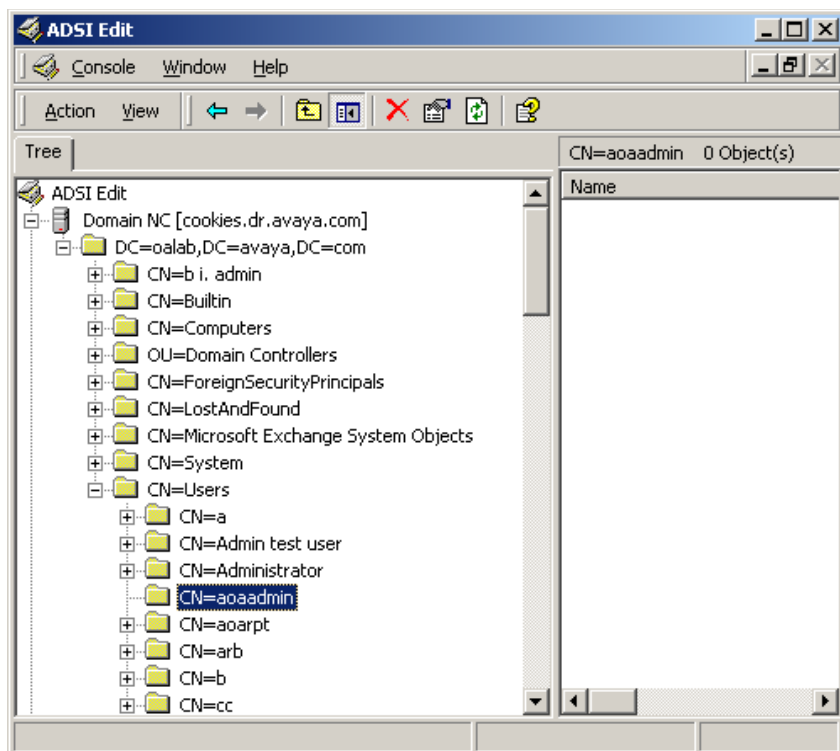
However, this method can lead to errors, as there is no guarantee that this really represents the ADS name. For example, CN=users could be defined as OU=users on some systems.



- **Using the ADS Edit tool**

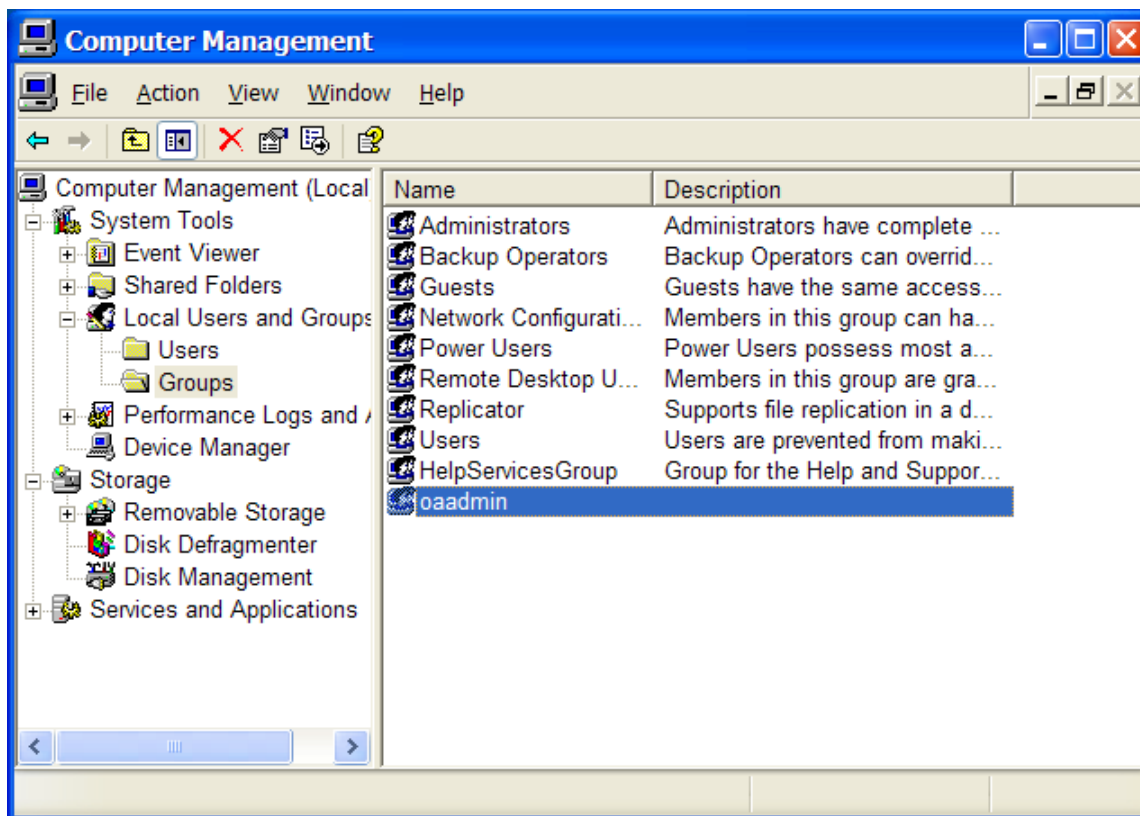
This is the most reliable way to determine the fully qualified name of OA groups. This tool is not installed by default on the domain controller. It needs to be installed from the Windows CD-ROM; the tool is part of the "Windows Support Tools". In the picture below, the ADS-style name is clearly identified at each branch of the tree. This picture confirms that the fully qualified name of the aoadmin group is:

CN=oaadmin,CN=users,DC=oalab,DC=avaya,DC=com



- **Using local users and groups**

Although the primary reason for this change is to support the ADS, support for locally defined groups and users is also provided. Local groups and users are managed using the Computer Management tool on the OA historical host. This tool can be accessed by right clicking on the **My Computer** icon and choosing **Manage**. The picture below shows that the oaadmin group is managed locally. When using that option, both users and groups must be managed locally, no mixing between domain users and local groups is allowed.



- **References**

To learn more about the ADS, please see this Microsoft article:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dsportal/dsportal/directory_services_portal.asp

Alternate domain name support

The domain name is determined from the LDAP string. If ADS is setup so the domain name cannot be determined from the LDAP string, the domain name needs to be supplied before the ADS security can work correctly. The alternate domain name can be added to the `autserver.properties` file using the example below.

The string `"xxxxxxx"` is replaced by the alternate domain name.

```
# Alternate domain name enhancement. This is only used when the domain
# name cannot be determined from the LDAP string. If this property
# ALTERNATE_DOMAIN_NAME exists, the properties value for domain name
# is used. If this string does not exist, the domain name is built
# from the LDAP string.
```

```
ALTERNATE_DOMAIN_NAME=xxxxxxx
```

ADS groups: what to do in case of error

The authentication server logs are the best way to diagnose errors if you have authentication or authorization problems when connecting to the administration server or reports. This change does not affect authentication (password verification) so that will not be discussed in this document. The only thing to keep in mind is that it

is not allowed to enter a domain name when prompted on the report or administration client screen. Only the user name is allowed. Authentication will occur on the localhost if local groups are configured or on the domain controller if ADS-style group names are used in *autserver.properties*.

These are some of the errors that can be encountered at authorization (group membership verification). All of these can be diagnosed by looking at the authentication server logs in `%PABASE%\data\log\autserver`. The list below explains some of the most common problems that can arise with this new feature.

- **User not authenticated**

If the user id/password are not correct, the authentication server will not try to verify the group membership of the user. In this case, verify that the userid/password are correct on the domain controller (if using ADS-style groups) or the historical host (if using local groups).

- **Can't connect to ADS**

In order to get the list of users for the OA groups, the authentication server needs to connect to the ADS. It uses the userid/password provided by the user for security. The location of the ADS is automatically discovered by the authentication server by searching for the domain controller for the domain name configured in *autserver.properties*. The LDAP port and version numbers configured in *autserver.properties* are also used to establish the connection. If this fails, verify that the domain controller resolution was what you expected. The host name of the domain controller is logged in the *autserver* logs. If that is correct, the LDAP version or port may be wrong. Those values are configured at installation time by the person that installed the ADS on the domain controller.

- **Can't read user list for groups**

If the connection is successful but the list of users cannot be read, it is likely that the fully qualified name of the OA groups is not configured properly. Please double-check the instructions in "how to figure out the fully distinguished name of the groups" above.

- **User not in group**

Lastly, if the list of users was read properly but the group membership is still not verified, it is likely that the user is not a member of that group. Make sure that the spelling of the user is correct using the user administration tool discussed above.

User ID policy guidelines

This section lists policy guidelines that are configurable for user password management. These guidelines shall not precede policies in effect in the organization using OA unless agreed with the appropriate policy decision makers. These guidelines can be implemented using common security tools provided by the OS.

Length

Avaya recommends that passwords have a minimum of 7 characters.

Lockout

The default values for authentication retries are

- 3 logon tries before a user is locked out
- A user is locked out for 10 minutes

Those values are located in `%PABASE%\data\admin\autserver.properties` (Windows), `$PABASE/data/admin/autserver.properties` (Solaris and AIX). They can only be modified by the system administrator. The authentication server must be restarted once the file is changed. To restart the authentication server, the system administrator needs to issue the following commands on the host where the values were changed:

- pa off autserver
- pa on autserver

Password reuse

Avaya recommends that password reuse not be allowed for at least 4 aging cycles.

Composition (alpha/numeric)

Avaya recommends that passwords consist of at least one alpha and one numeric character.

Root and Administrator privileges

Avaya recommends that the user IDs used for OA administration and reporting are not given root (on Solaris or AIX) or Administrator (on Windows) rights. These privileges are not needed to manage and use the OA software except for installation.

Uniqueness

Avaya recommends that user IDs should not be shared between users so that you will be able to trace user actions, such as logon time and administrative tasks, back to the correct user.

Creation

Avaya recommends that user IDs not used for one day after creation should be disabled.

Database user ID and passwords

The section “*Creating users and setting OS parameters*” in the first reference document describes how to set up user groups, including those needed for accessing the Oracle database on either Solaris or Windows or the DB2 database on AIX.

SQL Server 2008 R2 64-bit uses internal authentication or Windows user IDs and passwords (SQL Server 2008 R2 64-bit installation option). We use the SQL Server 2008 R2 64-bit internal authentication. Please refer to *Installing Microsoft SQL Server 2008 R2 64-bit on Windows* in [1] for more details.

Changing database passwords for SQL Server 2008 R2 64-bit and Oracle

Since the database user ID in the database and in OA must match, do not change the password in the database directly. Instead, use the commands shown in this section to change the password in the database and in OA. These commands are located at %PABASE%\bin for Windows or \$PABASE/bin for Solaris.

Run the following command from a command window to change the password of the database user login:

- **ChangeDBPWD -s** (Windows)
- **ChangeDBPWD.sh -s** (Solaris)

Note: If you want to change the OA database user password, you must know the database administrator password.

Run the following command from a command window to change the password of the system admin user login:

- **ChangeDBSYSPWD -s** (Windows)
- **ChangeDBSYSPWD.sh -s** (Solaris)

The command asks you enter in the new password in the historical database and to confirm the password. After successfully running this command, you can use the new password to connect to the database.

On SQL Server, you can confirm that you changed the password correctly by logging into SQL Server using the Query Analyzer and the new password.

On Oracle, you can use the **sqlplus** command to verify your passwords.

Changing database passwords for DB2

Since the database user ID in the database and in OA must match, use the commands shown in this section to change the password in the database and in OA. These OA commands are located at **\$PABASE/bin**.

Run the following command from a command window to change the password of the database user login:

ChangeDBPWD.sh -s

Note: If you want to change the OA database user password, you must know the database administrator password.

You must immediately use the OS command **passwd** to change the password at the OS level for the database user ID or the system administrator user ID. Always use the **ChangeDBPWD** and **passwd** commands together to change the password at the same time.

Run the following command from a command window to change the password of the system admin user login:

- **ChangeDBSYSPWD -s** (Windows)
- **ChangeDBSYSPWD.sh -s** (Solaris and AIX)

The command asks you enter in the new password in the historical database and to confirm the password. After successfully running this command, you can use the new password to connect to the database.

To verify passwords, use the DB2 commands to verify the password change.

Changing Informix password on a CMS Solaris host

Use the CMS specific script to change the password. It behaves the same way as the Oracle script but the command is **ChangeCMSDBPWD -s**.

File permissions

This section describes the directory and file permissions of the OA components.

Note: The OA installation program must be run as root (Solaris and AIX) and Administrator (Windows).

Directory access on Solaris and AIX

The top directory structure of **\$PABASE** permissions are:

```
drwxr-xr-x    6 root      other
```

All the directories and files under that structure have the following permissions:

```
-rwxr-x---    1 biadmin  staff
```

Where **biadmin** is the user ID entered in the OA installation program by the installer and **staff** is the name of the OA administration group as entered in the OA installation program by the installer.

Process owners on Solaris and AIX

All daemon processes are run as the user entered in the OA installation program by the installer (**biadmin** in the example above) with the exception of 3 processes:

- **initshr**: runs as root. It requires those privileges because it starts MOM as described below. It does a **setgid** and **umask** so the common log files that it uses can be read and written by the other processes that do not run as root.
- **MOM**: runs as root. Started by **initshr**, it starts all the OA daemons as the user ID entered in the OA installation program by the installer except for the authentication server. It inherits the **setgid** and **umask** of the process that started it (**initshr**).
- **autserver**: runs as root. The authentication server requires privileged access to be able to make system calls to authenticate users. It inherits the **setgid** and **umask** of the process that started it (**MOM**).

The client processes such as the command-line utilities, **dcstat** or **amui**, run as the user that is currently logged on to the system. Typically, the administrator will run these commands under the user ID entered in the OA installation program by the installer (for example, **biadmin**) because root privileges are not required and should not be used.

It is important to note that members of the OA administration group have permissions to change OA files and directories. This means that a member of that group could manually edit or replace files and have processes started as root on the host. It is therefore imperative that only trusted administrators are members of the OA administration group.

Windows access and run permissions

Currently, all Windows processes are installed and run as Administrator. This is typical of Windows applications and it is also due to limitations in the installation tool that we use. Any user in the Administrators group is able to run the client-side tools (Administration client, command-line tools).

Running scripts on AIX

The AIX OS does not allow scripts to run as a different ID or group as the current user. This causes any file created by the scripts to be owned by the user that runs the scripts. For example, if logged on as root, log files

created by the **amui** or Data API Utility scripts will be created and owned by the root user. Any user other than root will not be able to run the **amui** or Data API Utility after root has run them. This is because other users do not have the access rights to open and modify log files owned by root. We recommend that OA commands be always run using the OA administration user ID, never root. In the AIX case, this recommendation must be followed to avoid running into the problem described above.

Log/audit file

Audit content

The login attempts, successes and failures are audited.

Location on Solaris and AIX

On Solaris and AIX, the central error log is used for auditing. It is located at `$PABASE/data/log/CentralError`. On a multi-server setup, the logs are located on each of the Solaris or AIX hosts.

Location on Windows

On Windows, the application event log is used for auditing. It can be viewed using the Event Viewer Windows tool. On a multi-server setup, the event logs are located on each of the Windows hosts.

Policies

On Windows, the event log policies can be configured using the Event Log Viewer. On Solaris and AIX, edit the entry for CentralErrorLog in `$PABASE/data/admin/loginfo` to change the maximum trace file size and the number of trace files that will be retained.

Size

It is recommended that all audit logs be configured to hold 90 days of typical activities.

Conservation

It is recommended that the audit logs not purge automatically until the system administrator can copy the logs. The logs should not automatically overwrite.

Access

On Solaris and AIX, all members of the OA administration group as entered in the OA installation program by the installer can read the audit logs. On Windows, any user that has read access to the host where the event log is located can view the audit log.

Installation audit

The installation audit log is included as part of the installation log, near the end. If there are no problems, no warnings will be seen.

The default location is `C:\Program Files\Avaya\BI` on Windows, `/export/home/biadmin` on Solaris, and `/home/biadmin` on AIX.

Data privacy

What is protected

Only the passwords have been determined to be critical information targeted for encryption. The database user password and database system administrator password are encrypted.

How it is protected

The OA installation program encrypts the database passwords at install time. They are decrypted by the OA servers and are never sent across hosts once decrypted. They are also encrypted using the **ChangeDBPWD** tool described in section *0 Database user ID and passwords*.

The user ID passwords are stored and encrypted by the operating system as they are managed using OS tools. When entered at the authentication challenge screen of the Administration client, the password is encrypted on the client host using the Java Cryptography Extension (JCE) and decrypted by the administration server. This prevents the password from being sent in the clear over the communication lines.

Third party software security

Oracle

Oracle uses the internal Oracle security infrastructure. The OA software and interactive users must have a valid user ID and password to access the data. As described in section *0 Data privacy*, the password is encrypted so our processes can access the data without asking the end user for a password.

SQL Server 2008 R2 64-bit

SQL Server 2008 R2 64-bit uses the internal SQL Server 2008 R2 64-bit security infrastructure for authentication. The OA software and interactive users must have a valid user ID and password to access the data. As described in section *0 Data privacy*, the password is encrypted so our processes can access the data without asking the end user for a password.

DB2

DB2 uses the internal AIX security infrastructure for authentication. The OA software and interactive users must have a valid user ID and password to access the data. As described in section *0 Data privacy*, the password is encrypted so our processes can access the data without asking the end user for a password.

Times Ten

Data stored in the Times Ten real time database is not encrypted or protected by a password. The system administrator is responsible for ensuring that the right users have access to the interactive tool.

Tomcat for Windows, Solaris, and AIX

Tomcat on Windows, Solaris, and AIX is configured to anonymously pass through requests to access reports, and OA reporting uses the autserver to authenticate the user.

The effect is that Tomcat uses security of the respective operating system.

To prevent version-specific attacks and banner collection, the Tomcat version may be hidden from the default error pages.

To do this, create directory `\lib\org\apache\catalina\util` in tomcat base directory and put the `ServerInfo.properties` file in it with following content

```
server.info = AVAYA OA
server.number = 0.0.0.0
server.built =
```

"AVAYA IC" may be replaced with any desired server name to be displayed on default error pages

Remote access (PC Anywhere)

The remote access software used by the service group is capable of session encryption. Please refer to the PCAnywhere documentation for details on how to set it up to match the privacy needs of your environment.

Additional customer responsibilities

OS updates

The customer is responsible for updating the operating system with security patches.

Third party advisories and patches

The customer is responsible for keeping third party software secure by finding out and apply security advisory and patches.

Virus protection

The customer is responsible for installing, running and keeping up to date virus protection software.

Firewall

For non-secure environments the customer is responsible for protecting access to its network using firewall components or using a VPN. However for environments where this is not possible the following options should be considered.

OS level IP-Filtering

Sample OS level IP-Filtering configuration

Windows IP-Filtering:

1. Click Start, point to Settings, click Control Panel, and then double-click Network and Dial-up Connections.
2. Right-click the interface on which you want to configure inbound access control, and then click **Properties**.
3. In the **Components checked are used by this connection box**, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Advanced**.
5. Click the **Options** tab.
6. Click **TCP/IP filtering**, and then click **Properties**.
7. Select the **Enable TCP/IP Filtering (All adapters)** check box. When you select this check box, you enable filtering for all adapters, but you configure the filters on a per-adapter basis. The same filters do not apply to all adapters.
8. There are three columns with the following labels:
 - TCP Ports
 - UDP Ports
 - IP Protocols

In each column, you must select either of the following options:

- **Permit All**. If you want to permit all packets for TCP or UDP traffic, leave **Permit All** activated.

- **Permit Only.** If you want to allow only selected TCP or UDP traffic, click **Permit Only**, click **Add**, and then type the appropriate port in the **Add Filter** dialog box.

If you want to block all UDP or TCP traffic, click **Permit Only**, but do not add any port numbers in the **UDP Ports** or **TCP Port** column. You cannot block UDP or TCP traffic by selecting **Permit Only** for **IP Protocols** and excluding IP protocols 6 and 17. Note that you cannot block ICMP messages, even if you select **Permit Only** in the **IP Protocols** column and you do not include IP protocol 1.

Note: TCP/IP Filtering can filter only inbound traffic. This feature does not affect outbound traffic or response ports that are created to accept responses from outbound requests. Use IPSec Policies or packet filtering if you require more control over outbound access.

Unix IP-Filtering

1. First check with your OS vendor documentation to see if the IP-Filtering package is installed. If not, install it following the OS vendor documentation.
3. IP-Filter, if installed as a package, puts its binaries and man pages under /opt/ipf and the configuration files under /etc/opt/ipf. Once you have installed IP-Filter, there is very little you need to do to set up NAT.
4. To start using NAT, create a NAT configuration file, called /etc/opt/ipf/ipnat.conf. A sample file is shown below:

```
#
# Use the internal FTP proxy for outgoing FTP
#
map dp0 10.5.3.0/24 -> 0.0.0.0/32 proxy port ftp ftp/tcp
#
# Map anything going though dpn onto
# the dpn address
#
map dp0 10.5.3.0/24 -> 0.0.0.0/32 portmap tcp/udp 40000:60000
map dp0 10.5.3.0/24 -> 0.0.0.0/32
```

To enable packet filtering and assuming that you simply want all your outgoing connections to work and any attempts at incoming connections to be blocked, set up a simple set of IP-Filter rules for that purpose in file /etc/opt/ipf/ipf.conf, as shown in sample below:

```
# Block any packets which are too short to be real.
block in log quick all with short
# Block any packets with source routing set
block in log quick all with opt lsrr
block in log quick all with opt ssrr
# Allow traffic on le0 and lo0 to pass unimpeded
pass in on le0 all
pass out on le0 all
pass in on lo0 all
pass out on lo0 all
# Deny reserved addresses
block in log quick on dp0 from 10.0.0.0/8 to any
```

```
block in log quick on dp0 from 192.168.0.0/16 to any
block in log quick on dp0 from 172.16.0.0/12 to any
# Allow pings out
pass out log on dp0 proto icmp all keep state
```

Sub-interfacing

Sub-interfacing can also be considered for security. The following are sample configurations:

Windows based systems

1. Click **Start**, point to Settings, click **Control Panel**, and then double-click **Network and Dial-up Connections**.
5. Right-click the interface on which you want to configure inbound access control, and then click **Properties**.
6. In the Components checked are used by this connection box, click **Internet Protocol (TCP/IP)** and then click **Properties**.
7. In the Internet Protocol (TCP/IP) Properties dialog box, click **Advanced**.
8. Add second IP address
9. Modify System32\drivers\etc or update your DNS server to make this new IP address accessible by other OA servers.

Unix based systems

If you need multiple IP addresses on one interface, proceed as follows:

- `modprobe ip_alias` Verify the `ip_alias` module compiled.
- `ifconfig eth0 192.168.0.1` Define the first IP address
- `ifconfig eth0:0 192.168.0.42` Define the second IP address
- `ifconfig eth0:1 192.168.0.100` Define the third IP address

Add routes:

- `route add -net 192.168.0.0 dev eth0`
- `route add -host 192.168.0.1 dev eth0`
- `route add -host 192.168.0.42 dev eth0:0`
- `route add -host 192.168.0.100 dev eth0:1`

Note: entries of this nature can be put into `ip_alias` configuration file depending on your OS vendor.

Loopback of ports

If OA is on single server configuration, the setting of localhost 127.0.0.1 in the `/etc/hosts` file and using localhost as server name in the “Administration Client” can prevent an attack.

Data privacy

As described in the *Data privacy section*, only password information is encrypted over the network and on file. Historical database access is only allowed upon successful authentication. Data transferred between processes and across hosts is not protected. Any OA data that is considered sensitive by the customer is the

customer's responsibility to protect. VPN technology may be the right solution if data requires protection across hosts or via Internet communications.

Limit access to this document

The sensitive nature of this document dictates that it should not be made available to external parties or outside the system administrator group. It is recommended that this document is not copied from the CD and that printed copies are kept in a secured area.

Index

A

Active Directory Service support.....	10
Active Directory user/group management tool	11
administration group	9
ADS support	
determine fully distinguished ADS group name	10
ADS-style name	11
alternate domain name support	13
audience	5
audit log activities	19
audit log purging	19
authentication and authorization problems	13
authentication server logs	13
location.....	14

C

changing database password	
for DB2	16
for Oracle.....	15
for SQL Server 2008 R2.....	15
changing Informix password	
on CMS Solaris host	16
common authentication and authorization errors	
unable to connect to ADS	14
unable to read user list for groups	14
user not authenticated	14
user not in a group	14
creating an administration or a reporting group	10
customer responsibilities	
firewall protection	23
virus protection	23
customer responsibilities	23

D

data privacy	21
How data is protected?	21
what is protected?	21
determine fully distinguished ADS group name	
from network administrator.....	10
using ADSEdit tool	11
using local users and groups.....	12
using user/group management tool.....	11
diagnosing errors due to authentication and authorization problems	13
directory access	
on AIX	17
on Solaris	17
directory and file permissions.....	17
Distinguished Name	11

E

error logs	
location	19
location on Windows	19
on AIX.....	19
on Solaris.....	19
event log policies	
on AIX.....	19
on Solaris.....	19
on Windows	19

F

firewall protection	
OS level IP-Filtering	23
on Unix	24
on Windows.....	23
TCP/IP filtering	24
forest	10

G

group lds.....	9
----------------	---

I

installation audit log	19
location	
on AIX	20
on Solaris	20
on Windows.....	20

L

LDAP	13
log auditing.....	19
loopbacking ports	25

M

maintaining groups.....	10
-------------------------	----

O

OA database user password	16
---------------------------------	----

P

policy guidelines	
user ID	14
preface	5
process owners	

on AIX	17
on Solaris	17
processes	
autserver	17
initsrv	17
MOM	17

R

reporting group.....	9
----------------------	---

S

security	
sub interfacing	25
third party software	22
Security	
administration	9
assumptions	6
authentication	6
creating user ID	9
group membership	6
groups	

administration group	9
ADS support	10
creating a group	10
maintenance	10
reporting group	9
introduction	6
pre-installation configuration	7
security guide	
availability	5
related documents	5

T

third party software customer responsibilities	23
third party software security	
DB2	22
Oracle	22
PC Anywhere	22
SQL Server 2008 R2 64-bit	22
Times Ten	22
Tomcat	22